





Secure Your Identity Perimeter and Protect Your Business from Malicious Threats

 **ENTRA ID RISK ASSESSMENT**

Identity providers (IdPs) like Entra ID are essential for secure access. They act as gateways to all the applications in your environment, managing identities and securing data. This makes your IdP the first line of defense. Adopting an ideal identity perimeter is challenging with today's growing SaaS reliance and IT teams struggle to enforce access to SaaS applications running through the IdP.

With local access being enabled, shadow SaaS integrating into federated applications, and unknown and unfederated applications being deployed outside of security or IT's purview every day, security teams need a way to identify every app and integration in their environment, centralize them behind their IdP, then build a robust security framework around it.

IdP vulnerabilities create business vulnerabilities

-  **SaaS is the new frontline**
81% of organizations have sensitive data exposed across hundreds of SaaS apps, making it a prime target for threat actors.
-  **99% of compromises start at the IdP**
Over the past two years, we have observed that attackers primarily target the IdP due to its potential for granting access to numerous downstream applications.
-  **Shadow SaaS hides risk**
55% of shadow SaaS integrate with core apps like Salesforce, O365 and Workday—and the number of these unfederated apps grows by 25% every 60 days.
-  **75% of the 3rd party integrations go unused**
This creates a security vulnerability similar to the Midnight Blizzard attack earlier this year—especially since these apps are often over-permissioned and have access to sensitive data.

Why Obsidian?

Obsidian's platform changes the game by bringing together SSPM and ITDR to deliver end-to-end SaaS security. Detected threats continuously inform and refine security rules, delivering automated defenses that adapt as your organization grows. Using real-world SaaS breach insights to feed an AI-powered dynamic feedback loop, Obsidian ensures full visibility and proactive protection.

To learn more about Obsidian Security, visit ObsidianSecurity.com

Common IdP posture violations

Admin account sprawl and overpermissioning

Super or global admins should be limited to a small number of accounts.

Failing NIST 800-53 1A-2 and NIST AAL2 guidelines with weak MFA enrollment

Regulators advise all accounts with network access require MFA. However, with the rise of social engineering and attacker-in-the-middle (AiTM) attacks, all admins and users should have a phishing-resistant authenticator.




Authentication complexities and policy enforcement

Flexible configuration capabilities Entra ID allow admins to create conflicting rules for users, creating vulnerabilities due to weak authentication methods.

Request your complementary IdP risk assessment

Obsidian allows you to get a complete inventory of your entire SaaS environment and IdP configurations, uncovering weaknesses and vulnerabilities in your identity infrastructure and mapping those directly to security frameworks like NIST 800-53, SOC 2, PCI DSS, and ISO/IEC 27001.

What you get:

-  **Uncover and minimize risks to your IdP**
Obsidian integrates directly into your IdP, collecting and normalizing retroactive activity data to detect vulnerabilities and providing simple remediation steps to reduce risk.
-  **Quick time-to-value**
Get your findings in 14 days to understand how to improve your security posture and compliance across your identity perimeter in a comprehensive report.
-  **White-gloved guidance from our security experts**
Together, we'll review your report to create a plan for adopting your ideal identity perimeter to reduce risk and prevent attacks.