OBSIDIAN

SOLUTION BRIEF

Workday Security with Obsidian

The Industry's First Continuous Security Solution for Workday

As the leading SaaS solution for financial management, human resources, and planning, Workday is entrusted with some of the most sensitive information in your organization. This includes employee details, accounting, payroll, contracts, vendor relationships, and more. While protecting this data from insider threats and attackers is a top business priority, security teams often lack the visibility and access needed for effective threat mitigation and proactive risk reduction.

Security teams need to effectively partner with and support application owners to protect Workday without impeding the teams that rely on it. To accomplish this, they need clear, continuous insights into user activity, privileged access, and application configurations within Workday and across interconnected, business-critical applications. When suspicious behavior indicates a potential threat, security teams need the context and tools to respond immediately. And with core applications integrated so closely, vulnerabilities in one platform can become entry points into another, making remediation even more convoluted.

As the first truly comprehensive SaaS security and compliance solution of its kind, Obsidian enables your security team to harden your security posture and quickly mitigate threats to core business applications like Workday.

Obsidian Capabilities at a Glance

- Immediate, out-of-the-box value, with no agents to deploy or custom rules to write
- Anomalous behavior detection to identify and mitigate threats within Workday
- Privilege and access right-sizing based on individual and peer group analysis
- Inventory of Workday configurations with hardening recommendations and details on the resulting user impact
- Monitoring of third-party services and applications connected to Workday
- Downstream integration with SIEM and SOAR solutions to consume Obsidian alerts and data

This means Obsidian not only maps Workday's complex permission and configuration model to recommend immediate security improvements, but also monitors activity in the application and across connected platforms to identify the earliest indicators of malicious activity.

Obsidian for Workday

Obsidian has deep expertise in Workday and its data schemas. After you connect both platforms in just a few clicks, Obsidian immediately begins retrieving and contextualizing data from Workday, resolving user accounts to identities, adding threat intel, and populating our proprietary knowledge graph. This becomes the baseline for our highly accurate, machine learning-driven threat detection model.

At the same time, Obsidian identifies opportunities to improve your Workday security posture and shows the impact any change will have on users. Obsidian brings together threat mitigation and risk reduction in a single, easily consumable interface that can fit seamlessly into your workflow with downstream integration options for your SIEM or SOAR. Our solution saves your security team the time typically needed to continually monitor a complex platform like Workday and enables them to focus on delivering important security outcomes.

Mitigate Threats Early

In order to mitigate threats in Workday, you need to analyze the state and activity data within your SaaS environment. Existing proxy-based security solutions are effective at controlling the flow of data into and out of your applications, but are unable to see inside. Obsidian populates a knowledge graph by regularly collecting information on user activity and state data within Workday and across your other core SaaS applications. This provides a comprehensive baseline to identify anomalous behavior against.

While proxy-based security solutions control the flow of data into and out of your applications, Obsidian is able to detect bad actors within your SaaS environment early on. Our detailed, cross-application activity logs enable security teams to quickly assess the exact scope of a breach and understand the users, applications, and data that may have been impacted. Our solution makes it easy to identify potentially malicious activity, determine if persistence has been established, and mitigate threats before data can be exfiltrated. We also streamline reporting after responding to an incident and ease the burden of gathering data for compliance purposes.

Obsidian comes out-of-the-box with a variety of rules for Workday to detect account compromises and insider threats. To address your organization's unique security and compliance needs, our platform allows your security team to set up custom alerts to automatically monitor for specific behaviors in your environment. Because Workday integrates into a variety of third-party applications and services, Obsidian's holistic approach to threat detection protects the application no matter where the threat originates.

Harden Your Workday Configurations

Workday offers a range of granular security settings, but navigating these controls, determining their impact on the organization, and continually ensuring that preferred settings are unchanged is incredibly demanding for security teams. It's common for configuration settings to be left in default, which can expose you to unnecessary risk.

Obsidian brings configurations from various consoles across your business-critical applications into one place, providing security teams with a clear view of their application settings. We rank them against industry best practices, highlighting the most critical unoptimized controls for immediate evaluation. If configurations drift from your organization's preferred settings, Obsidian flags them to ensure constant compliance.

Because Obsidian understands identity, activity, privilege, and access within and across your SaaS environment, we're able to detail the exact impact of configuration changes in your applications. This gives your security team the context and confidence needed to effectively collaborate with application owners to balance the needs of your users with security best practices.

Manage Privilege and Access in Workday

Permissions and access in Workday can be difficult to determine and even harder to continually monitor. In order to maintain security best practices and minimize the impact of a potential breach, your security team needs to know exactly who has privileged access, who is not actively using that privilege, and who has unnecessary administrative access. They should also be aware of other risk factors like lingering access for terminated employees or outside contractors and third-party read or write access to Workday.

Obsidian untangles Workday's complex permission model to give your security team unprecedented visibility into the scope of privilege and access for your users in Workday and other core SaaS applications. A single clear interface provides a full inventory of each person's role while highlighting opportunities to right-size unused accounts or unnecessary privilege based on individual and peer data. Our contextual understanding of user activity allows security teams to make these reductions confidently, knowing they won't impede the users who need their elevated privileges to be productive.

File access is another critical consideration for security teams, since Workday houses a massive amount of sensitive data on employees, vendors, finances, and more. Obsidian notifies security personnel about abnormal access behaviors including unusually high download volumes, sensitive file access by atypical individuals, and intellectual property theft by employees with upcoming termination dates.

Conclusion

As a business-critical SaaS application entrusted with sensitive data, Workday needs to be brought within your security scope. Obsidian fills the gap in SaaS security and compliance, complementing your existing stack to proactively reduce risk and rapidly mitigate threats. Our insights and recommendations enable security teams to understand what's happening inside Workday and partner effectively with application owners. Connect additional SaaS applications for a richer view of user activity and privilege. As the first truly comprehensive SaaS security solution of its kind, Obsidian equips your security team with the contextual knowledge they need to focus on delivering real security outcomes for your organization.

Get started with a live demo

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