OBSIDIAN

SOLUTION BRIEF

WORKDAY SECURITY WITH OBSIDIAN

The Industry's First Continuous Security Solution for Workday

Capabilities at a Glance

- Delivered as SaaS, deployed in minutes with no agents and nothing to install
- Inventory of all Workday users and their privileges
- Normalized activity data for easier triage, investigation and threat hunting
- Visibility into activity related to tasks, reports, data sources, web service operations, and business processes
- Visibility into activity by third party integrations
- Ability to correlate HCM events with security data for detection, hunting, and IR
- Built-in detections for risks and threats
- Security hygiene alerts, including inactive accounts and weak authentication practices
- Downstream integration with SIEM and SOAR solutions to consume Obsidian alerts and data

As the leading SaaS solution for financial management and human capital management, Workday holds some of the most sensitive information in your organization. This includes employee details, accounting, payroll, contracts, vendor relationships, and more. Protecting this data from insiders and attackers is a top business priority, yet in most organizations the security teams often don't have the access needed for security monitoring, threat detection, incident response, and remediation.

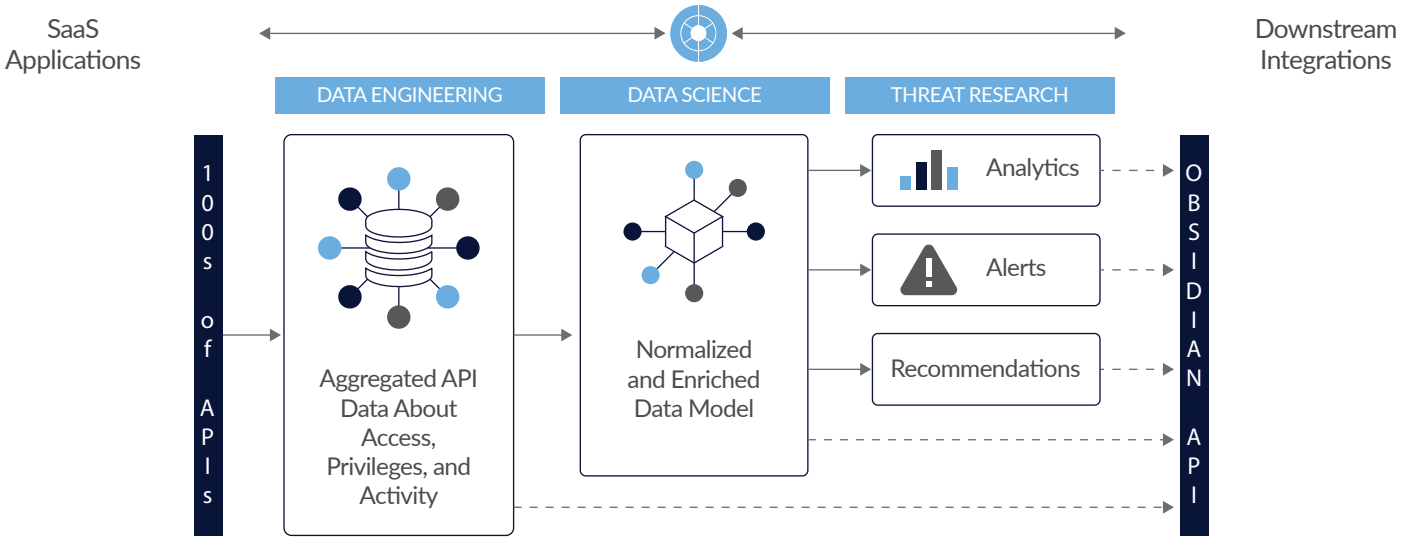
While Workday takes responsibility for the security of the application itself, customers are still responsible for identity and access management, configuration management, and activity monitoring. Administrators have to manage access and privileges so that legitimate users have the right level of access to the resources they need. Configuration drift can increase the risk of compromise and data loss. Security teams also need to be able to detect and respond to insider threats, account compromise, data exposure, and inappropriate access.

An effective SaaS security solution unifies visibility, monitoring, and protection across multiple applications. The data in Workday, including employee status, start and end dates, and team changes, can also provide highly relevant context for an identity-centric security model. The security solution must be capable of analyzing Workday events in the context of other activities.

Obsidian for Workday

Obsidian delivers a simple yet powerful security solution for SaaS applications based on a new approach called cloud detection and response (CDR). With Obsidian, security teams can continuously monitor user activity, protect against data breaches, and detect and respond to insider threats and account compromise. Obsidian arms security teams with the data they need to ensure that the right people have the right level of access to Workday and they are doing the right things with that access.

To do this, Obsidian connects with Workday and other SaaS applications over APIs to aggregate data about accounts, privileges, and activity. The platform normalizes and analyzes the data using built-in policies and machine learning to detect account compromise, insider threats, access misuse, data leaks, excessive privileges, and configuration changes. Security teams have unified access to activity data across Workday and other SaaS applications to investigate and respond to incidents.



Use Cases

Problem: Lack of Visibility

Security teams are not able to monitor Workday because they don't have access to the live environment. Furthermore, entitlements and activity data are buried deep across multiple applications, creating visibility silos.

Solution

Fix the visibility gap by arming security with the data they need. Give security teams a unified view of activity across Workday and other SaaS applications to monitor and investigate suspicious behavior, and respond to incidents without getting in the way of regular SaaS users and admins.

Problem: High Risk Employees

Employees with upcoming termination dates can pose a higher risk for IP theft.

Solution

Get visibility into users with upcoming termination dates. Obsidian lets you quickly view recent activity of these users to find any access activity of concern. Alerts and analytics related to employee termination raise security awareness to heightened risk situations.

Problem: Lingering Access

Employees who have left the company may still have lingering access to SaaS applications (not just Workday). In some cases, these employees may access services after termination. This is a serious security issue.

Solution

Get alerts and analytics around former employees and contractors who have lingering accounts in SaaS applications and/or have accessed the apps after they are no longer with the company.

Problem: Data Protection

Sensitive data about employees and vendors is stored in Workday. Insider threats are a real concern. A data breach can cause a loss of trust and trigger severe penalties under regulations such as GDPR and CCPA.

Solution

Identify risks associated with data access in Workday. Obsidian generates alerts when a user has an unusually high volume of downloads, or reveals other signs of suspicious data access activity. Who is accessing data or downloading reports that they should not?

Problem: Financial Data

Organizations sometimes store financial data in Workday Financial Management. This increases the impact of a data exposure or breach.

Solution

Get continuous visibility into access related to sensitive financial data and reports. With Obsidian's saved searches and user-generated alerts, you can quickly detect suspicious or inappropriate access.

Problem: Weak Authentication

Weak authentication practices create gaps in protection from account takeover attempts.

Solution

Use Obsidian's alerts and analytics around authentication and access to identify weak or inappropriate security practices; e.g., users accessing Workday via basic authentication. Obsidian provides visibility into accounts frequently targeted by brute force attacks that are at a high risk for takeover access.

Problem: Excessive Admin Privileges

Admin sprawl is rampant. Who has privileged access? Does an employee have admin access that they should not have, or are not actively using?

Solution

Get an inventory of user access and privileges. Monitor for privilege elevation and admin sprawl. Obsidian maps privileged roles to show privileges associated with any user.

GET STARTED WITH A LIVE DEMO

https://www.obsidiansecurity.com/demo