Workday Account Takeover Protection

Analyze human behavior to gain greater visibility into Workday risks.

Workday houses your most sensitive data

HR platforms house everything from benefits and health information to banking details and social security numbers, presenting a high-value target for attackers to compromise.

Attackers target Workday with sophisticated tactics

Threat groups are attempting to compromise Workday with session hijacking, credential stuffing, and other sophisticated tactics with the goal of changing financial data, steal PII, or execute ransomware attacks

Complex Workday environments hinder security visibility

Security teams often do not own Workday security. While Workday provides native security tools, there is no easy way to detect a compromised user attempting to access the platform.

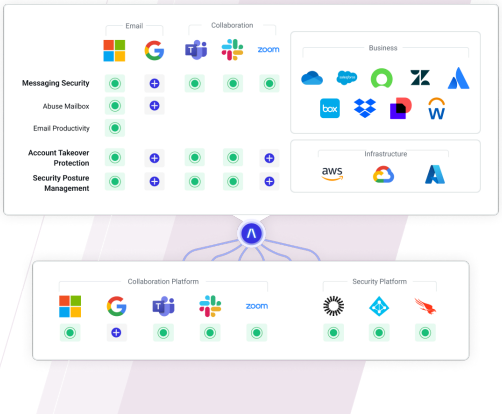
Extend Abnormal Protection Across All Platforms

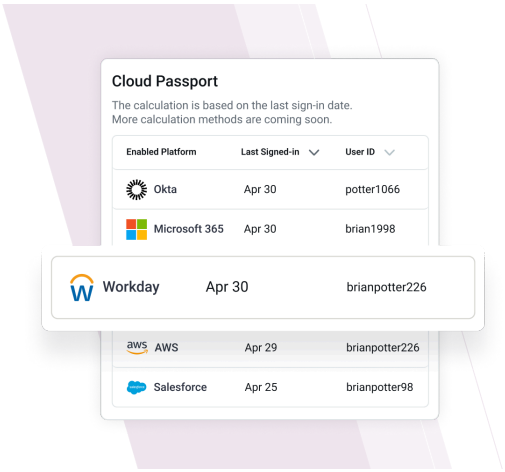
Cloud phishing breaches—that is, breaches affecting your cloud apps and services that result from the exploitation of human vulnerability through advanced phishing and social engineering tactics—are a primary concern for Security teams. As an HR and payroll platform, Workday requires greater protection than most applications when it comes to stopping breaches. The key to protecting Workday is consistent visibility and security automation that analyzes activity across your entire cloud environment through an extensible AI platform. Abnormal provides this platform, providing higher fidelity threat detection not only in Workday but across all of your most important cloud services.

How Abnormal Secures Workday

Simple API Integration

Connect directly to Workday with Abnormal's cloud-native API architecture—automatically ingesting and normalizing sign-in signals related to every human in your organization that accesses the Workday platform.



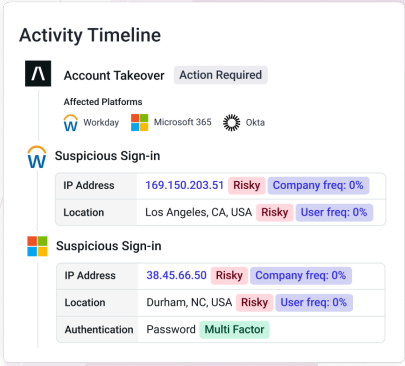


Continuous Monitoring of Human Behavior in Workday

Build dynamic behavioral profiles of every human accessing Workday, develop a behavioral baseline, and automatically detect and analyze any deviations from that baseline.

AI Account Takeover and Response

When a behavioral deviation is deemed a likely account takeover, Abnormal Human Behavior AI automatically triggers the creation of a contextual Case populated with Workday activity. Each Case is scored based on detection confidence and continually enriched with new activity across all platforms integrated with Abnormal.



Try Abnormal Today

See how Abnormal can keep attacks out of your cloud email and connected platforms. Integrate in minutes via API.

abnormalsecurity.com/risk →

Abnormal