Saviynt | workday

SOLUTION GUIDE

Saviynt for Workday

A Comprehensive Solution for Continuous Compliance, SoD and ILM Management

Workday is a consolidated suite of cloud applications used by organizations for in-depth human capital management and financial management solutions, student applications, and other business-critical tasks. Each application contains multiple modules, and each module requires a unique and complex security model. Achieving compliance, enforcing security policies, and preventing fraud in this situation becomes challenging without automation and deep integration with the application security model.

As a certified Workday partner, Saviynt is the trusted cloud identity governance provider of an automated, simplified, and centralized governance and compliance platform for movers, joiners and leavers. One-click integration with Workday and built-in templates provide rapid onboarding for multiple scenarios. Saviynt identifies risky user access using intelligent analytics to drive higher effectiveness of certification. In addition, Saviynt provides an intuitive and intelligent access request system to ensure all access to Workday is reviewed and approved prior to being provisioned.

Protecting Sensitive Data and Meeting Compliance Needs

Access to sensitive HR data (PII), over-privileged access, not applying principles of least privilege, and segregation of duty (SoD) conflicts expose critical data and transactions. Anytime data is stored or managed, the organization must ensure appropriate access is assigned to users to the right data at the right time.

Understanding Workday Security

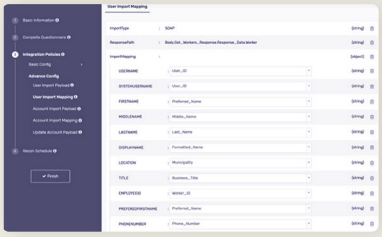
Workday's multi-layered security model is defined using organization, business process, domain, job, role, and or user. Each business activity in Workday requires access to the specific business process, security permissions and domain permissions.

Also, there are several distinct types of security groups in Workday; some configurable to the user and or role and some based on inheritance. Different security groups can be configured, and permissions managed using the user, user role, job, organization data, or position leading to a complex matrix to design or assess security.

Saviynt Application Risk and Governance Solution

Machine-learning analytics consume any entitlement hierarchy to analyze risk across all technology platforms, any application and multiple applications. Application GRC analyzes access hierarchy and maps out complex inherited relationships between domains, business processes, security groups, positions, roles, actions, and policies. Risk-aware insight identifies and manages risk while providing much-needed visibility into Workday access.

Certified



Key Solution Benefits

SoD Management

- Out-of-the-box rulesets customized for Workday
- SoD rules for business process and domain security policies
- Visibility into actual SoD and key control violators
- Cross-cloud and cross-application SoD evaluation
- Investigation workbench
- Detective and preventive control enablers
- Contribute to Online Controls Exchange

Saviynt automates and enables organizations to satisfy compliance requirements by offering a comprehensive, cutting edge capability in all areas of Application GRC including SoD Analysis, Role Engineering and Management, Emergency Access Management, Compliant Provisioning, Access Certification and Transaction Monitoring.

Identify and Monitor Risk in Real Time

Using the intuitive workbench, internal security teams and auditors can readily determine and remediate SoD violations. Mitigating controls to accept or manage risks are provided in the built-in library.

A comprehensive SoD ruleset designed for Workday is built into App GRC. The ruleset comes with risks or toxic combinations of fine-grained Workday entitlements and incorporates items such as roles, business processes, security policies, domain security policies, and organization hierarchies.

Unified Compliance Framework

Many organizations struggle to build a library of controls that automate compliance processes due to a lack of resources or time and difficulty in gaining expertise in all the applications. Using Saviynt security teams are empowered utilize 200+ security controls mapped to industry domains and applications such as Workday to ease their workload. Users are also able to contribute organization-specific security controls to the online control exchange.

Privileged Access Management

One of the critical benefits of Saviynt is that companies can manage emergency access/account procedures to provide temporary time-bound, privileged access to an existing user, or temporary access to a privileged account. Emergency access activity is monitored, reviewed, documented, attested, and signed off, simplifying the auditors' preparation and reporting. Saviynt provides visibility into all activities transacted by these privileged IDS to assure organizations and auditors that all transactions are secure and appropriate for the privileged user.

Saviynt's cloud-architected Identity Governance provides a simple, fast and cost-effective solution for enterprises to manage security of their critical applications. Saviynt has a major focus on ERP applications such as SAP, Oracle, Workday etc. with global customers relying on its solution for their security and compliances needs.

Key Solution Benefits (continued)

Role Design and Management

- Automated security group management
- User and Role security group provisioning
- Role impact simulation and assessment
- Attribute based Access Rules (ABAC) combined with Roles

Access Request and Compliant Provisioning

- Risk-aware access request and review process
- Automated joiner, mover, and leaver access policies
- Automatic audit of credentials and revocations in Workday
- Easy shopping cart-based approach
- Access certifications based on usage and behavior analytics
- Flexible enterprise-grade workflow designer
- Preventive SoD and security policy violations
- Automated provisioning to target systems

Continuous Compliance

- Actionable, real-time risk dashboards
- Interactive drag and drop Link Analysis
- Controls reporting mapped to SOX, PCI, FedRAMP, HIPAA, etc.

Next Steps

- Find out why Saviynt was named a Leader in the Gartner 2019 Magic Quadrant for Identity Governance and Administration (IGA)
- Try a Demo of the Saviynt IGA Platform

ABOUT SAVIYNT

Saviynt empowers enterprises to secure their digital transformation, safeguard critical assets, and meet regulatory compliance. With a vision to provide a secure and compliant future for all enterprises, Saviynt's cutting-edge solutions have been recognized as industry leaders. For more information, please visit www.saviynt.com.

Saviynt

Headquarters, 1301 E
El Segundo Bl, Suite D, El Segundo, CA
90245, United States

310. 641. 1664 | info@saviynt.com
www.saviynt.com