SafePaaS™

Enhancing Workday Security:
Utilizing Access Governance Solutions for Stronger Defenses



Workday is used by more than 10,000 customers globally for financial management and HR needs. This number includes over 50% of the Fortune 500 and more than 25% of the Global 2000.

Securing your Workday system is paramount, especially when these systems store sensitive data such as Personally Identifiable Information (PII) and financial data. Protecting confidential information requires your organization to implement robust security measures to ensure only authorized users have access to such data.

As your organization increasingly relies on digital platforms for managing operations and housing critical data, understanding Workday's functionality becomes imperative. Safeguarding against potential threats like financial misstatements or control failures is essential.

This eBook explores the significance of securely managing sensitive data in Workday. It discusses actionable measures your organization can take to fortify its defenses and ensure maximum security for your data, and Workday applications.

Understanding Workday's Security Hierarchy

Workday's Security Hierarchy manages data access through roles (security groups), business process actions and domains, and access levels that determine if users can view or modify data.

Tenant Level
At the top of Workday's security hierarchy is the tenant level, which represents the entire organizational environment within Workday. Security configurations at this level apply universally to all users and data across the organization and encompass global policies and configurations.

Organization Level
Workday allows organizations to segment their operations into different organizations within a single tenant. Organizations mirror organizational structures such as business units, regions, or subsidiaries, each with tailored security settings. Workday typically calls these organizational hierarchies.

Position
In Workday, Positions define specific job roles within a Supervisory Organization, including attributes like worker type, time type (full-time or part-time), job family, and availability date. A position can exist whether it is filled or unfilled, serving as the foundation for workforce planning and management. Positions also incorporate role-based security, allowing one or multiple security groups to be assigned, and allowing organizations to ensure that employees in those positions have the appropriate system access based on their responsibilities.

Security Groups / Roles
Security Groups in Workday define access rights for specific job functions, including the specific business process actions and domains users have access to. While predefined security groups cater to common roles like finance manager or procurement specialist, it is recommended that organizations design custom security groups to address security requirements.

Domain Security Policies
Define access to specific data and actions within the system, such as HR information, financial data, or organizational structures. These policies determine what security groups can view or modify data directly within the user interface and interact with data via web service operations.

Business Process Security Policies
Control security group access to and participation in specific business process workflows, like hiring payroll, or accounting journals. These policies ensure that only authorized users can initiate, approve, or take action within a business process, helping to maintain workflow integrity and compliance.

Access Levels
Business process action levels and domain access levels govern user actions and data access based on assigned security groups. These policies dictate the level of access and specific actions users have to records and pages within a Workday tenant.



SafePaaS™

© SafePaaS 2024

Strengthening Workday Security with Access Governance Solutions

Given Workday systems' wealth of sensitive data, from social security numbers to bank account details, it's no surprise that they are a prime target for bad actors.

An access governance solution allows users to define and enforce access policies accurately, monitor the activities of privileged users, provide centralized control and visibility over user access rights, and streamline processes such as automated role/security group assignments, access certifications, and policy enforcement. Combined with continuous monitoring capabilities, this solution enables proactive identification and response to security threats in real-time, effectively reducing the likelihood and impact of security breaches.



SafePaaS™

© SafePaaS 2024

Consequences of Inadequate Access Governance

Inadequate access governance within Workday systems can have severe repercussions. Security breaches can result in the unauthorized disclosure, alteration, or theft of sensitive data, leading to financial loss, reputational damage, and legal liabilities. Non-compliance with regulatory requirements such as SOX, GDPR and HIPAA can result in hefty fines and penalties, further exacerbating the consequences of inadequate security measures.

Moreover, the lack of proper access governance can undermine investor trust and confidence in your organization's ability to protect sensitive data. This can harm stock price and productivity, ultimately impacting your organization's bottom line.

Two examples, Equifax and Target, suffered security breaches due to inadequate access governance. Equifax's breach exposed the personal information of over 147 million people, costing between $200 million to $300 million. Target's breach exposed the personal information of over 40 million customers, costing approximately $162 million. The financial and reputational damage from these breaches highlights the importance of proper access governance.



SafePaaS™

© SafePaaS 2024

Strategies for Mitigating Risks in Workday

1. Define Segregation of Duties and access policies, roles, and responsibilities.

Establishing clear policies, roles, and responsibilities is crucial for effective organizational governance and security, streamlining decision-making processes, promoting accountability, and ensuring alignment. Segregation of Duties (SoD) principles in access control and risk management help prevent conflicts of interest and fraud by dividing critical tasks among multiple users or teams. Clear guidelines for business process and domain access, effective communication, and regular policy review and updates are essential for maintaining security and compliance. Involving stakeholders from different departments in policy development ensures alignment with business objectives. Clarity in roles and responsibilities and regular training sessions are crucial for effective access control.

- Identify the data and systems that require access controls and assign ownership and accountability for them.
- Provide clear guidelines for granting, modifying, and revoking access permissions.
- Ensure that policies are communicated, understood, and enforced across the organization.
- Regularly review and update policies to reflect changes in business needs and regulatory requirements.

Best practices

- Involve stakeholders from different departments in policy development to ensure the policy aligns with business needs.
- Clearly define roles and responsibilities to avoid confusion and overlap.
- Provide training and awareness sessions to educate users on access control policies.

SafePaaS™

© SafePaaS 2024

2. Establish Access Controls

Establishing access controls is a key component of any security strategy because it allows you to limit who can access data and resources and under what circumstances.

- Grant access based on the principle of least privilege, which means granting users only the business process actions and domains they need to perform their job functions.
- Implement segregation of duties to ensure no single user can access all critical systems or data.
- Monitor privileged user activity to detect and respond to real-time security incidents.

Common pitfalls

- Granting excessive access rights to users leads to data breaches.
- Failing to monitor user activity or detect security incidents in real-time.
- Not implementing encryption or other security measures leads to data loss or theft.

3. Identity Access Request Management

Managing identity access requests effectively is critical to ensuring access is granted only when necessary and appropriate for specific roles and job functions. A well-defined identity access request process helps mitigate the risk of unauthorized access and ensures compliance with access control policies.

- Implement a formal process for requesting, reviewing, and approving identity access requests.
- Ensure that all access requests are evaluated against SoD policies and access control guidelines.
- Automate the access request process to reduce errors and streamline approvals.
- Track and document all access requests, approvals, and denials for audit purposes.

Best practices

- Involve relevant stakeholders in the approval process to ensure access aligns with business needs.
- Regularly review and refine the access request process to adapt to changing business requirements and risks.
- Implement automated workflows to ensure consistent and timely processing of access requests.

SafePaaS™

© SafePaaS 2024

4. Conduct Identity Access Reviews

Regularly reviewing identity access is critical to ensure access is necessary and appropriate for their job responsibilities. This involves evaluating the identity´s access level to data and systems within your organization. It is important to determine whether any changes need to be made to minimize the risk of unauthorized access or security breaches. Keeping accurate records of these reviews and documenting changes to identity access rights is also crucial. This helps ensure your organization complies with regulations and standards like SOX, GDPR, and HIPPA.

- Remove or modify access that is no longer required or violates access control policies.
- Regularly review identity activity logs to detect and respond to suspicious or unauthorized activity.
- Conduct access reviews for high-risk identities or privileged identities more frequently.

Best practices

- Automate access reviews using access governance solutions to save time and resources.
- Involve business stakeholders in access reviews to ensure access permissions align with business needs.
- Document access review processes and outcomes for audit purposes.
- Create a governance committee to review security changes, especially for interconnected systems like Workday (HCM, recruiting, payroll, financials), to avoid granting excessive access to another group's data.

SafePaaS™

© SafePaaS 2024

5. Monitor Privileged Access Activity

As organizations rely more on technology and data, the potential for security breaches and data theft increases. So, it is critical to have a system that monitors privileged users' activities to ensure the safety and security of your data and resources. This is important because privileged users, such as system administrators, have access to sensitive data and can potentially misuse their access to steal data or cause harm to the organization. Monitoring their activities can help you detect any suspicious behavior and prevent security breaches before they occur.

- Implement monitoring and auditing mechanisms to detect and prevent unauthorized privileged identity activity.
- Implement controls to prevent privileged users from accessing critical systems or data outside their job functions.
- Monitor privileged user activity logs to detect and respond to suspicious or unauthorized activity.

Best practices

- Implement real-time monitoring and alerting mechanisms to detect and respond to privileged user activity in real-time.
- Review privileged user access rights regularly to ensure they are still necessary and appropriate.

Common pitfalls

- Failure to monitor privileged user activity leads to unauthorized access or security incidents.
- Granting excessive privileged user access permissions leads to data breaches.
- Not revoking access rights on high-priority terminations, such as someone on a trading platform needing to be promptly deactivated upon termination processing to ensure disconnection from downstream systems for that user.

Access governance solutions are becoming increasingly necessary to enhance the security of Workday systems. This is because threats targeting sensitive and financial data are rising, and organizations must prioritize security to protect their valuable assets. By implementing access governance solutions, you can define and enforce access policies, monitor privileged user activities, and maintain centralized control over user access rights. Failing to establish adequate access governance can lead to severe consequences. Therefore, it is important to stick to these best practices to strengthen your Workday security and improve your ability to protect yourself against security threats.

SafePaaS™

© SafePaaS 2024

SafePaaS Use Cases for Workday

Segregation of Duties, Sensitive Access, and Privileged Access Policies

- Identity Access Governance: Manages access rights to enforce segregation of duties and control privileged access.
- ERP Application Governance: Segregation of duties and Sensitive Access Analysis and built-in Remediation with Comprehensive pre-built rulesets, dashboards to easily detect anomalies and robust reporting capabilities

Identity Access Request Management

- Identity Access Governance: Automates identity access request management to ensure appropriate access rights.
- API Governance: Manages API access provisioning.

Lifecycle Management

- Identity Access Governance: Manages user and identity access throughout their lifecycle based on policies.
- IT Governance: Ensures IT resources are used according to policies.

Integrated Fulfillment

- Integration with ITSM - Integrate Workday with ITSM systems such as ServiceNow to prevent fine-grained access violations in identity access request management.

Periodic Access Review

- Identity Access Governance: Automate the access review process in Workday with automated workflows to reduce the cost of SOX compliance and mitigate cybersecurity risks.
- Closed-loop User Access Change Management: Integrate ITSM for timely risk remediation.

SafePaaS™

© SafePaaS 2024

Identity Orchestration and Lifecycle Management

- Identity Governance: Orchestrates identity lifecycle from creation to deactivation.
- Integrate with IAM: Integrate Workday with IAM systems for compliant identity life cycle management.

Role / Security Group Management

- Simulation and Entitlement Management: Automate role design and simulate security before violations get introduced into your Workday system.

Privileged Access Management

- Control Privileged Access Management: Manages privileged access to Workday
- IT Governance: Ensures privileged access to Workday is controlled and audited.

Advanced Analytics

- Identify security risks in access requests approved in the provisioning systems vs. the access granted in Workday.
- Use analytics to interpret data and discover unknown business risks or opportunities as they occur or, even better, anticipate the next one.



SafePaaS™

© SafePaaS 2024

Safeguarding Your Workday Environment

SafePaaS addresses security challenges in Workday tenants by identifying and mitigating risks such as segregation of duty conflicts, unauthorized configuration changes, and false positives in analysis. The platform's advanced audit solution helps identify compliance-related risks while continuous monitoring and automated testing maintain an audit-ready system. By implementing proactive risk management strategies, SafePaaS enhances Workday security, ensuring resilience against evolving threats and compliance with regulatory standards.

By leveraging SafePaaS's access governance capabilities, organizations can effectively manage the complexities of securing their Workday system, ensuring a secure and compliant environment that builds trust with stakeholders and customers.

To learn more about how SafePaaS can help you enhance Workday security please contact:

Emma Kelly
Senior Marketing Manager
emma.kelly@safepaas.com

3300, Dallas Parkway, Suite 200, Plano, Texas, 75093 USA

SafePaaS™

© SafePaaS 2024