Workday Security

Workday Security

Introduction

Today's technology leaders are charged with securing and protecting the customer, employee, and intellectual property data of their companies in an environment of increasingly complex security threats. As cloud computing has become more widely accepted, a number of information security concerns have been raised. This paper will help guide you when assessing a prospective cloud vendor and provide an overview of Workday's security in each area.

Regulatory Compliance and Certifications

Customers are responsible for complying with local, state, national, and foreign laws, including those related to data privacy and transmission of personal data, even when a service provider holds and processes their data on their behalf. Workday maintains a formal and comprehensive security program designed to ensure the security and integrity of customer data, protect against security threats or data breaches, and prevent unauthorized access to the data of its customers. The specifics of Workday's security program are detailed in its third-party security audits and international certifications.

External Audits (SOC 1 and SOC 2 Reports)

Workday's operations, policies, and procedures are audited regularly to maintain standards expected of service providers. Workday publishes a Service Organization Controls 1 (SOC 1) Type II report. The SOC 1, which is the successor to the SAS 70, is issued in accordance with Statement on Standards for Attestation Engagements No. 16 (SSAE 16) and the International Standard on Assurance Engagements No. 3402 (ISAE 3402). This dual-standard report gives companies around the world confidence when conducting business with SOC 1 audited companies such as Workday. The scope of the SOC 1 is limited to Workday's production systems. The intended audience for this report is a customer or prospect who is required to have an understanding of internal controls over outsourced critical business tasks that have an impact on customer's financial statements (Sarbanes-Oxley compliance). The SOC 1 audit is conducted every six months by an independent third-party auditor. The report is available to customers or prospects upon completion.

Workday also publishes a Service Organization Controls 2 (SOC 2) Type II report. The SOC 2 addresses the Security, Confidentiality, Availability, and Privacy principles of the Trust Services Principles and Criteria. The scope of the SOC 2 covers any Workday system that contains Customer Data. The intended audience for this report is a customer or prospect who is interested in understanding Workday's internal control around the Trust Services Criteria and how Workday's systems interacts with subservice organizations. The SOC 2 audit is conducted once per year by an independent third-party auditor This report is available to its customers or prospects upon completion.

Both the SOC 1 and the SOC 2 validate Workday's physical and environmental safeguards for production data centers, backup and recovery procedures, software development processes, and logical security controls.

ISO 27001 and 27018 Certifications

ISO 27001 is an information security standard originally published in 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). In September 2013, ISO 27001:2013 was published, which supersedes the original 2005 standard. ISO 27001 is a globally recognized, standards-based approach to security that outlines requirements for an organization's Information Security Management System (ISMS).

ISO 27018 is a complementary standard published by ISO/IEC in 2014, which contains guidelines applicable to cloud service providers that process personal data.

Workday is proud to say we have achieved certification against ISO 27001 in September 2010 and ISO 27018 in October 2015. Certification is achieved following an independent assessment of Workday's conformity to the ISO standard. ISO recertification occurs every three years, but to maintain certification, a business must go through annual surveillance audits. These ISO certifications affirm Workday's commitment to privacy and security and demonstrate that our controls are operating effectively. Workday's ISO certificates and ISMS Statement of Applicability are available for customer review.

Cross Border Data Transfers

In October 1998, the European Commission's Directive on Data Protection went into effect, prohibiting the transfer of personal data to non-European Union countries that do not meet the European Union (EU) adequate standard for privacy protection. To help U.S. companies meet this requisite, the U.S. Department of Commerce in consultation with the European Commission's Directive on Data Protection and the Federal Data Protection and Information Commission of Switzerland developed the Safe Harbor privacy framework on the transfer of personal data from European Union member countries and Switzerland to the United States.

Workday annually self-certifies to the Safe Harbor framework. This framework allowed U.S. companies that commit to the Safe Harbor Privacy Principles to meet the "adequacy " standard for privacy protection established by the European Commission, and import data from the European Economic Area (EEA). Workday's Safe Harbor certification covers the transfer of Customer Data, EU personal data that is used for marketing purposes, employee data, as well as professional services data from the EEA and Switzerland.

Despite the recent decision by the European Court of Justice to invalidate the Safe Harbor program, Workday continues to annually self-certify to the Safe Harbor framework. To address the adequacy requirement for customers with operations in the European Union, we have incorporated the European Commission's approved standard contractual clauses, also referred to as the "Model Contract", into our Data Protection Agreement. The Model Contract creates a contractual mechanism to meet the adequacy requirement to allow for transfer of personal data from the EEA to a third country.

More information about the U.S. Department of Commerce's Safe Harbor program can be found at http://www.export.gov/safeharbor/. More information on the Standard Contractual Clauses can be found at http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm.

Additional information on Workday's commitment to safeguarding the privacy of our customer's data and details of our privacy program can be found in the Workday Data Privacy Overview paper.

Physical Security

Workday co-locates its production systems in state-of-the-art data centers designed to host mission-critical computer systems with fully redundant subsystems and compartmentalized security zones. Workday's data centers adhere to the strictest physical security measures:

- Requires multiple layers of authentication before access is granted to the server area
- Critical areas require two-factor biometric authentication
- Camera surveillance systems at critical internal and external entry points
- Security personnel monitor 24/7
- Unauthorized access attempts are logged and monitored by data center security

All physical access to the data centers is highly restricted and stringently regulated. Workday data operations uses security best practices such as "least access" hardened servers and regularly scheduled maintenance windows.

Data Segregation

Workday is a multi-tenant Software-as-a-Service (SaaS) application. Multi-tenancy is a key feature of Workday that enables multiple customers to share one physical instance of the Workday system while isolating each customer tenant's application data.

Workday accomplishes this through the Workday Object Management Server (OMS). Every user ID is associated with exactly one tenant, which is then used to access the Workday application. All instances of application objects (such as Organization, Worker, etc.) are tenant-based, so every time a new object is created, that object is also irrevocably linked to the user's tenant. The Workday system maintains these links automatically, and restricts access to every object based on the user ID. The Workday system restricts access to objects based on the user ID and tenant. When a user requests data, the system automatically applies a tenancy filter to ensure it retrieves only information corresponding to the user's tenant.

Encryption of Data at Rest (Database Security)

Workday encrypts every attribute of customer data within the application before it is stored in the database. This is a fundamental design characteristic of the Workday technology. Workday relies on the Advanced Encryption Standard (AES) algorithm with a key size of 256-bits. Workday can achieve this encryption because it is an in-memory object-oriented application as opposed to a disk-based RDBMS application. Specifically, Workday's metadata is interpreted by the Workday OMS and stored in memory. All data inserts, updates, and deletes are committed to a persistent store on a MySQL database. This unique architecture means Workday operates with only a few dozen database tables. By contrast, a RDBMS-based application requires tens of thousands of tables, making complete database encryption impractical due to its detrimental impact on performance. complete database encryption impractical due to its detrimental impact on performance.

Encryption of Data in Transit (Network Security)

Users access Workday via the Internet protected by Transport Layer Security (TLS). This secures network traffic from passive eavesdropping, active tampering, or forgery of messages.

Workday has also implemented proactive security procedures such as perimeter defense and network intrusion prevention systems. Vulnerability assessments and penetration testing of the Workday network infrastructure are also evaluated and conducted on a regular basis by both internal Workday resources and external third-party vendors.

Data Backups

Workday's master production database is replicated in real-time to a slave database maintained at an offsite data center. A full backup is taken from this slave database each day and stored at the offsite data center facility. Workday's database backup policy requires database backups and transaction logs to be implemented so that a database may be recovered with the loss of as few committed transactions as is commercially practicable. Transaction logs are retained until there are two backups of the data after the last entry in the transaction log. Database backups of systems that implement interfaces must be available as long as necessary to support the interfacing systems. This period will vary by system.

Backups of the database and transaction logs are encrypted for any database which contains customer data.

Cloud Data and Disaster Recovery

Workday warrants its service to its standard Service Level Agreement (SLA). The SLA includes a Disaster Recovery (DR) plan for the Workday Production Service with a Recovery Time Objective (RTO) of 12 hours and a Recovery Point Objective (RPO) of one hour. The Recovery Time Objective is measured from the time the Workday Production Service becomes unavailable until it is available again. The Recovery Point Objective is measured from the time that the first transaction is lost until the Workday Production Service became unavailable.

To ensure Workday maintains these SLA commitments, Workday maintains a DR environment with a complete replication of the production environment. In the event of an unscheduled outage where the outage is estimated to be greater than a predefined duration, Workday executes its DR plan. The MySQL database is replicated to the DR data center, new OMS instances are started in the DR data center, and customers are redirected to the DR data center. The DR Plan is tested at least every six months.

Unified Security Model

Unlike legacy ERP systems, Workday operates on a unified security model. This includes user access, system integration, reporting, mobile device, and IT access. Everyone must log in and be authorized through the Workday security model. By contrast, in legacy ERP systems there is typically an applications layer of security which IT and DBA personnel can bypass to access the data directly at the database level. This is not possible with Workday. Workday is an object-oriented in-memory system with an encrypted persistent data store. This ensures all access and changes are tracked and audited. This uniquely robust security model, combined with Workday's automatic ability to effective date and audit all data updates, lowers the time and costs associated with governance and compliance and reduces overall security risk.

Logical Security

Workday security access is role based supporting LDAP Delegated Authentication, SAML for Single Sign-On and x509 certificate authentication for both user and web services integrations.

Delegated Authentication

Workday supports delegated authentication via a customer's on-premise LDAP server such as Microsoft Active Directory. This allows the customer's security team to disable a user account centrally from the LDAP server without the need to

login to Workday. Workday can also automatically update the LDAP server with new active user accounts via new hires or deactivated accounts such as employee separations and employees on leave of absence.

Single Sign-On Support

LDAP allows for a unified username/password, SAML takes the next step and enables an enterprise single sign-on (SSO) environment. While LDAP Delegated Authentication makes it possible for users to have the same username and password for both their internal applications and Workday, it still requires the user to log in twice. SAML takes the next step and allows for a seamless, single sign-on experience between the customer's internal web portal and Workday. Specifically, users log in to their company's internal web portal using their enterprise username/password and are then presented with a link to Workday, which automatically gives them access without having to log in a second time.

Workday Native Login

For customers who wish to use Workday's native login, Workday only stores their Workday password in the form of a secure hash as opposed to the password itself. Unsuccessful login attempts are logged as well as successful login/logout activity for audit purposes. Inactive user sessions are automatically timed out after a specified time, which is customer configurable by user or role. Customer configurable password rules include length, complexity, expiration, and forgotten password challenge questions.

Authorization

The Workday application enforces group policy-based security for authorization. The application prevents customer end users from directly accessing the production database. Workday's security groups combined with Workday predefined security policies grant or restrict user access to functionality, business processes, reports, and data.

Customer-configurable security groups are based on users, roles, jobs, organizations, or business sites and can be combined into new security groups that logically include and exclude other groups. System-to-system access is defined by integration system security groups. Customers can thereby tailor these groups and policies to meet their needs, providing as finely grained access as required to support complex configurations including global implementations.

Context-Sensitive and Context-Free Access Support

Workday allows for both context-sensitive and context-free role-based security. A context-sensitive role-based security group is associated with an organization type such as a Supervisory organization, Cost Center organization, or a Company organization. Workday security is 'sensitive' to only accessing secured items in the same organization type. For example, a manager initiates the Hire Employee business process to hire a new worker into their organization called U.S. Sales Division. One step in that business process is performed by the HR Partner role. This business process is context sensitive so Workday security only looks for a worker in the HR Partner role who supports the U.S. Sales Division Supervisory organization. Context-free access means there is no restriction by organization type and membership is defined by role only such as Any Managers or Any HR Partners.

Workday does not attempt to match the worker's organization to the organization of the secured item. Customers can leverage Workday's powerful, flexible organization structures and security groups to control access to various types of data, business processes, and transactions in accordance with their unique requirements.

System-to-System Access

In Workday, system-to-system access is via public web service or Reports-as-a-Service (RaaS). Regardless of method, the data results are controlled by Integration System Security Groups. These security groups offer either context-sensitive or context-free access. For example, you can set up an integration that exports data only for workers who are members of a specific paygroup, while a separate integration can return all supervisory organizations. Data results can also be further filtered by element or row. For example, the public web service filters by element so the Workday integration that returns worker data may filter out some data for that worker (e.g., compensation or personal data). RaaS integrations filter by row based on the security of the underlying Report Data Source, which can also be configured to filter its results contextually.

About Workday

Workday is a leader in enterprise-class, Software-as-a-Service (SaaS) solutions for managing global businesses, combining a lower cost of ownership with an innovative approach to business applications. Founded by PeopleSoft veterans Dave Duffield and Aneel Bhusri, Workday delivers unified Human Capital Management, Payroll, and Financial Management solutions designed for today's organizations and the way people work. Delivered in the cloud leveraging a modern technology platform, Workday offers a fresh alternative to legacy ERP. More than 310 customers, spanning medium-sized organizations to Fortune 50 businesses, have selected Workday. Visit us at www.workday.com.

Workday, Inc. | 6230 Stoneridge Mall Road | Pleasanton, CA 94588 | United States
1.925.951.9000 | 1.877.WORKDAY (1.877.967.5329) | Fax: 1.925.951.9001 | www.workday.com