workday.

Whitepaper

Trusting Workday with Your Data Security Needs

Table of Contents

A Consistent Security Model	3
A Commitment to the Topmost Security Standards	4
Technology that Safeguards Your Data	4
Data Encryption	5
Auditing	5
Logical Security	5
Physical and Network Security	7
A Commitment to Transparency	9
Safeguarding Your Data and Earning Your Trust	10

Across the globe, organizations must safeguard their customer, employee, and proprietary data against escalating security challenges. Concurrently, data privacy laws are continuously evolving, rendering compliance more complex. In such a climate, it is imperative to select a software partner renowned for robust data security and privacy practices.

At Workday, building and earning trust is the foundation of everything we do. More than 50% of the Fortune 500 have selected Workday as a trusted partner, and thousands of companies entrust us with their most confidential data pertaining to their people and finances, elevating security to our topmost priority. As such, Workday security practices are integrally woven into our foundation rather than bolted on as an afterthought. We commit to continuous auditing to keep pace with the dynamic security landscape. We develop our software and services to meet the security needs of our most risk-averse and heavily regulated customers, to the benefit of all our customers. Our processes are designed to prioritize security and privacy in our operations and product development. And our organizational culture is built to uphold and reinforce the highest levels of security throughout the organization. In this paper, we discuss rigorous data security practices at Workday.

More than 50% of the Fortune 500 have selected Workday as a trusted partner.

A consistent security model.

The Workday security model is foundational to how we continuously safeguard our customers' data. The Workday Human Capital Management (HCM) and Finance applications are built on a shared technology platform using a cloud-based architecture. This allows us to utilize the latest technology improvements, enhancing everything from user experience to our underlying infrastructure platform.

Importantly, this unified setup supports a consistent security model across all Workday Enterprise Products, offering key benefits to our customers. First, our consistent security model streamlines administration, making it easier for the right people and entities to have the right access to data. Specifically, Workday Enterprise Products use the same access model across user interfaces, APIs, and integrations. This shared access model helps lower risks related to administrative "backdoor" access that can cause problems in older, legacy applications. When everyone uses the same secure access point, there are fewer chances for security breaches, data leaks, and other issues. Additionally, all our customers use the same version of Workday Enterprise Products, meaning any security improvements we make are immediately available to everyone.

In line with our approach to data management, we extend the highest level of security to all data, irrespective of the level of sensitivity assigned by the customer. We consider every piece of customer data as sensitive and encrypt it while in transit and at rest. Our applications come with embedded audit functionalities, enabling Workday customers to execute comprehensive, always-active audit coverage. This approach stands in contrast to numerous other solutions that typically incorporate audit features as secondary add-ons. Our security model is essential to how we protect our customers' data and enables us to deploy security at scale.

We equip our customers' compliance and legal teams with a wealth of resources through the Workday Community portal, assisting them in meeting their privacy and compliance needs.

A commitment to the topmost security standards.

Workday security strategies and practices are grounded in globally recognized standards from the National Institute of Standards and Technology (NIST) and the Center for Internet Security (CIS), affirming our commitment to world-class security. The NIST Cybersecurity Framework offers a comprehensive risk management approach encompassing both risk prevention and response, alongside guidance for risk measurement and benchmarking. The CIS Controls consist of 18 prioritized steps for defending against cyberattacks. Together, these methodologies affirm our commitment to maintaining peak levels of data security across the entire Workday suite of solutions.

Our array of international certifications and third-party audits serves as a testament to our dedication to data security, privacy, and our resilience against data breaches, security threats, and unauthorized access to our customers' data. Workday undergoes annual SOC 1 Type II and SOC 2 Type II audits, and complies with global security and privacy protocols, including EU-US Data Privacy Framework, Asia-Pacific Economic Cross-Border Privacy Rules, and GDPR. Moreover, Workday is certified with global security and privacy standards such as ISO 27001, ISO 27017, ISO 27018, and ISO 27701. Workday is typically at the forefront among cloud service providers in embracing new security and privacy standards; for example, Workday was the first company to demonstrate adherence to the EU Cloud Code of Conduct (CCoC).

We equip our customers' compliance and legal teams with a wealth of resources through the Workday Community portal, assisting them in meeting their privacy and compliance needs.

Technology that safeguards your data.

From architecture to applications, our technology puts your data security first. It provides configurable tools to meet the security needs of all our customers, even the most risk averse.

Data encryption: We leverage state-of-the-art encryption technologies to secure customer data, regardless of whether it's at rest or in transit. Workday utilizes the Advanced Encryption Standard (AES) algorithm with a key size of 256 bits for encryption while data is at rest. We employ Transport Layer Security (TLS) to safeguard user access over the internet, which secures network traffic between a user's device and a server, preventing tampering, forgery, and unauthorized interception.

For file-based integrations, encryption of the files can be achieved through Pretty Good Privacy (PGP). This method ensures file security during transmission. For web services integrations with the Workday API, we support WS-Security.

The Workday Key Management Service (KMS) manages the entire lifecycle of cryptographic keys used for encrypting and decrypting customer data stored at rest. Customers can also implement Bring-Your-Own-Key (BYOK) capability to retain full control of their root encryption keys.

Auditing: Workday lets you monitor all your business transactions and easily see your historical data and configuration changes. We provide a detailed audit trail, recording each system operation from data modifications to user identities and timestamps. Our "effective dating" method traces transactions over time, thereby ensuring data integrity and accountability. We also uphold a system of non-destructive updates, safeguarding data from being overwritten or lost. Furthermore, our user activity logs provide a deep dive into individual actions within the system. Every change is documented, allowing a full history review. Lastly, to optimize auditing capabilities, we offer REST APIs for smooth integration of the audit trail with customer Security Information Event Management (SIEM) systems, empowering a swift response to potential security incidents. The audit trail, user activity logs, and sign-on reports are favorites among Workday customers and auditors alike.

Logical security: The state-of-the-art security model at Workday ensures robust protection for customer data, incorporating cutting-edge technology in authentication, single-sign-on support, Workday native login, and configurable security.

- **Authentication.** Workday authenticates all users or systems accessing the platform. Customers can create end-to-end user identities or integrate them into Workday from external systems. Workday supports Security Assertion Markup Language (SAML) for single sign-on, facilitating uninterrupted access to multiple applications after a single login. And Workday supports the use of x509 certificate authentication for both user and web services integrations.
- **Single sign-on.** Workday seamlessly integrates with internal customer web portals via support for OpenID Connect and SAML, creating an effortless single-sign-on experience. For those utilizing Microsoft Azure AD, Workday provides an Azure Active Directory connector, granting secure access to both cloud and on-premise applications.

> "At Sun Life, the strength of our ongoing partnership with Workday really comes down to trust.
>
> Senior Vice President
> for Global Talent,
> Sun Life

- **Workday native login.** Our native login for Workday Enterprise Products only stores the password in the form of a secure hash as opposed to the password itself. Unsuccessful login attempts and successful login/logout activities are logged for audit purposes. Inactive user sessions are automatically timed out after a specified time, which is customer configurable by user. Customer configurable password rules include length, complexity, expiration, and forgotten password challenge questions.

- **Configurable security.** Workday role-based access control allows security administrators to manage and regulate user data actions and control data accessibility. Tools such as roles, security groups, and business process configurations help enforce and manage your company's security policies.

- **Step-up authentication.** Workday step-up authentication secures against unauthorized access by identifying critical items within Workday, requiring a secondary authentication factor that users must enter to access those items.

- **Multifactor authentication.** Workday provides and recommends customers use Multifactor authentication (MFA). Workday allows customers to supply any authenticator application backed by the Time-Based One-Time Passcode (TOTP) algorithm. With this setup, customers can easily integrate MFA providers with the Workday native login. Workday also allows end users of customers to receive a one-time passcode delivered via an email-to-SMS gateway mechanism. Lastly, Workday supports challenge questions as an additional mechanism to prove a user's identity.

- **Trusted devices.** Workday provides the ability for customers and their end users to enroll devices as trusted for access to their Workday tenant. End users will be notified of unrecognized devices attempting to access their account. They will have the ability to remove devices they no longer trust. For administrators, a list of trusted devices is provided for monitoring purposes. End users must consent to tracking of the trusted device with a browser cookie.

- **Access controls.** Access to Workday can be blocked from deny-listed IP ranges or restricted by allow-listed IP ranges through authentication policies. Workday supports the ability to enforce step-up authentication, which can require a user to re-authenticate by a specific method to access restricted items within the tenant.

- **Context-sensitive and context-free access support.** Workday offers context-sensitive and context-free role-based security, thereby providing granular control over access to resources based on their organizational association and role-based privileges.

- **System-to-system access.** System-to-system access in Workday is facilitated via public web service or Reports-as-a-Service (RaaS), ensuring tight control over data results through the Integration System Security Group.

  By integrating these elements, Workday offers advanced logical security measures that ensure the protection of customer data, providing peace of mind for businesses and their users.

Physical and network security.

To keep your data safe, Workday has specified operating policies, procedures, and processes for data centers, networks, and applications.

- **Data centers.** Workday applications are hosted in state-of-the-art data centers with fully redundant subsystems and compartmentalized security zones. The data centers adhere to the strictest physical and environmental security measures. The facilities require multiple levels of authentication to access critical infrastructure.

  Camera surveillance systems are located at critical internal and external entry points, while security personnel monitor the data centers 24/7. The data centers have implemented redundant environmental safeguards and backup power management systems including fire suppression, power management, heating, ventilation, and air-conditioning, set up in a minimum N+1 redundancy.

- **Network security.** Network security is a cornerstone of the Workday comprehensive security architecture. We employ an array of sophisticated tools to protect our network and your data from threats. Intrusion Detection Prevention Systems (IDPS) and other tools are in place to monitor network activity, identifying and mitigating potential threats to ensure system integrity and availability.

  Content filtering is another key component of our strategy, scrutinizing and controlling the data that travels through our network to prevent data leaks and exposure to harmful content. We use advanced firewall technologies to monitor and control incoming and outgoing network traffic based on predetermined security rules, thereby monitoring and controlling sessions east-west and north-south.

  Workday also utilizes Web Application Firewalls (WAFs) to identify and block attacks targeted at exploiting web application vulnerabilities. To protect against Distributed Denial-of-Service (DDoS) attacks, we deploy DDoS services, filtering out malicious traffic to maintain service availability under all circumstances. The combination of these measures ensures a robust network security framework, securing the Workday environment from evolving threats.

- **Security monitoring and response.** Workday Cybersecurity Operations Center (CSOC) leverages comprehensive monitoring tools and stringent processes to safeguard our infrastructure from potential threats. Operated by a globally positioned team, our CSOC adheres to a follow-the-sun model, ensuring continuous, 24/7 surveillance. The CSOC team routinely scrutinizes data patterns, identifying anomalies that could suggest a potential vulnerability. If the SIEM system spots any unusual activities within our systems, an alert is immediately triggered to the CSOC. This initiates a thorough investigation, encompassing in-depth examination, detailed analysis, and timely resolution of potential security issues.

  We also designate security personnel to evaluate alerts from security vendors and industry organizations. They identify critical updates that may impact our systems. If a security vulnerability is identified that demands action, an internal tracking ticket is issued to the appropriate team. All updates are installed in a time frame commensurate with the risk associated with the vulnerability, and all changes adhere strictly to our Change Management process.

- **Disaster recovery and backups.** 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 1 hour. To meet these SLA commitments, Workday maintains a comprehensive Disaster Recovery Plan. Workday utilizes advanced database replication mechanisms involving the creation of standby replicas that mirror the production databases, thus maintaining continuous data availability and facilitating seamless business operations across various platforms.

  To ensure the plan's effectiveness, we conduct semiannual tests. These trials assess both the recovery plan's reliability and the integrity of backup systems and data. The testing process contributes to keeping our recovery plans and documentation up-to-date and reliable.

  Moreover, Workday implements a robust backup protocol for database and persistent data stores. Our primary production database and persistent data stores are securely replicated at an offsite data center, with regular backups. This strategy ensures minimal loss of committed transactions, thereby maintaining operational continuity. Dedicated teams constantly oversee the backup schedule, ensuring swift issue resolution. This vigilant approach to disaster recovery and data backup ensures a superior level of data resilience and availability for our customers.

- **Multitenancy.** Workday is a multitenant Software-as-a-Service (SaaS) application. Multitenancy 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 Workday account is associated with exactly one tenant, which is then used to access the Workday application. All instances of application objects (such as Organization and Worker) 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 Workday account and tenant. When a user requests data, the system automatically assigns the request to one and only one tenant to ensure that it retrieves only information corresponding to the user's tenant.

- **Application security.** Our application development, testing, and deployment process is rooted in a firm commitment to product security. Our Product and Technology teams follow a framework called Secure Software Development Life Cycle (SSDLC), and with DevSecOps, everyone in the development and operation of the product takes accountability. During the development process, we conduct an in-depth security risk assessment and review of Workday features. This includes analyzing security risks, examining both static and dynamic source code, training our developers so that they understand the best practices for secure coding, and penetration testing to help identify problems before the product goes to customers. Prior to release, a third-party security firm will assess web and mobile applications to spot potential vulnerabilities.

A commitment to transparency.

To help our customers facilitate their audit, compliance, and internal governance needs, we readily share various security-related documentation on Workday Community that many SaaS providers keep strictly internal. Examples include SOC audit reports, disaster recovery processes, business continuity plans (BCP), penetration testing results, current and past security advisories, and common security questionnaires. Our customers commend this level of transparency they don't see elsewhere. This is just one example of the Workday commitment to transparency and how we seek to build trusting partnerships with our customers.

Safeguarding your data and earning your trust.

As data security and regulatory requirements evolve, Workday leverages our core values of innovation, customer service, and integrity to deliver meaningful value to customers. We innovate on our platform and in our applications to meet the needs of even the most risk-averse organizations. We strive for the highest levels of customer and user satisfaction, and are deeply committed to our customers' success. And to earn the trust of everyone we work with, we set clear expectations, establish accountability, measure results, and own our outcomes.

Workday serves more than 10,000 customers globally. To learn more about why leading businesses around the world trust Workday with their sensitive data, visit: workday.com/trust

workday.

+1-925-951-9000 +1-877-WORKDAY (+1-877-967-5329) Fax: +1-925-951-9001 workday.com

20230929-trusting-workday-with-your-data-security-needs-enus