Workday Security: A Technology Perspective

The Workday data centers employ state-of-the-art measures to maintain physical security and uninterrupted service for Workday customers. Workday also employs additional security measures to protect data during transfer across the network and encrypts the Workday database for a unique level of data security.

The data center

Workday strictly regulates and limits all access to on-demand servers and network at its production and remote backup facilities. Workday also ensures that robust backup procedures are in place to foster uninterrupted service for all its customers.

Physical security

Workday co-locates its production systems in a state-of-the-art data center that adheres to the strictest physical security measures:

- Monitored 24 hours a day, seven days a week
- Access restricted to Workday-approved individuals and access is recorded and regularly audited
- Multiple methods of identification required to gain access to the data center
- Workday servers are in a private, secured area within the data center
- Consoles are not used in the data center

Backup and recovery

Workday achieves better than 99% uptime, excluding scheduled maintenance. All servers are diskless and boot from the NAS (networked attached storage), so Workday can quickly configure a new server to take any role. The Workday NAS implements RAID5+1 so that even a failure of multiple disk drives would not cause the NAS to fail. Error logs on servers and disk arrays are continually monitored for any signs of problems, and pre-emptive action is taken when necessary.

Encrypted backup files are transmitted over secure connections to a redundant server storage device in a secondary data center. Access to this server storage device is restricted to the NAS device from the primary data center. Both data center facilities employ advanced measures to ensure physical integrity, including redundant power and cooling systems (multi-homed with UPS and diesel power), and advanced fire and flood prevention.

Workday security key features:

Application Perspective
- Non-destructive data updates with no performance penalty
- Dynamic, role-based access eliminates need for dual-security maintenance
- Single unified security model

Compliance Perspective
- Continuous audit trail
- Supports Sarbanes-Oxley 404 compliance

Technology Perspective
- Non-relational data model prevents SQL injection attacks
- All communications outside the data center are encrypted
- WS-Security support for Web services
SAS-70 audit includes data center controls
During Workday’s SAS-70 Type II audit, a third party auditor validates that physical and environmental safeguards are in place at the data center. The auditor also reviews Workday’s backup and recovery procedures. Workday houses development and customer implementation systems in another data center, which also serves as Workday’s disaster recovery site. Workday regularly conducts tests of the disaster recovery plan.

Communications and networking security
Workday uses industry-standard measures to protect the integrity of all communications with its online services, its production network, and across its network.

Workday expends considerable effort to ensure that access to online services data is uniformly secure. All communication with Workday’s Business Services must use Secure Socket Layer version 3 (SSL 3) or Transport Layer Security (TLS), the successor to SSL. These protocols enable communication across a network in a way designed to prevent eavesdropping, tampering, and message forgery. Workday requires SSL between the user’s browser and Workday servers, thus ensuring that, as users access Workday’s Business Services via the Internet, their communications will be secure. All user interface server-to-browser communications use secure session keys to prevent “session hijacking.” Workday requires all Web services requests to use WS-Security. WS-Security specifies extensions to SOAP messaging, and defines a standard way to represent security information in a Web services message. All Web services must run over SSL as well.

Access to the Workday production-hosted network is strictly controlled using the “least access” strategy, and this access is limited to the Workday on-demand operations team. Workday performs network vulnerability assessments and penetration testing on a regular basis using third-party vendors. Exceptions are remedied as appropriate. Workday servers are hardened based on the latest best-practices specifications. Infrastructure patches are installed during regularly scheduled maintenance windows per our maintenance policy, and the maintenance schedule is published in advance. All patches are reviewed and signed off before being applied to production.

Database security
It is not enough to secure access to data via the online services and to ensure the integrity of the hardware. The database itself must also be protected. As a result, Workday encrypts every data value in the Workday database—the only solution on the market capable of this approach.

Most relational databases place all their data values in separate columns, unencrypted. Encrypting every data value would require encrypting each column separately. But it’s not unusual for a database that supports an enterprise-class application to contain tens of thousands of tables, and for a single key table (such as the Job table) to contain more than one hundred columns. Encrypting each column separately therefore represents a daunting task that will significantly degrade overall performance. The alternative—attempting to analyze a 10,000-table database to decide which values to encrypt— is highly impractical and imprecise, but nevertheless is frequently the general course of action. For instance, DBAs may decide to encrypt the Social Security number column and the salary column but neglect to encrypt the Federal Taxes Paid YTD column, which is a proxy for salary. It rapidly becomes apparent that it is extremely difficult and resource-intensive to secure the data held in the database.
Workday is able to encrypt every attribute value in the application before it is stored in the database. This is a fundamental design characteristic of the Workday technology. Workday is built on an object model, meaning there are only a handful of tables and only one security model to maintain.

This first-of-its-kind approach towards database security is a significant improvement over current standard practice. All of the supporting database artifacts (the physical file on disk, the transaction logs, the backups) have only encrypted values in them. Even the DBA cannot read the actual data, as illustrated below:

**DBA's view of an unencrypted database vs. an encrypted database**

Workday relies on the Advanced Encryption Standard (AES) algorithm with a key size of 256 bits. The U.S. National Security Agency has authorized the use of AES with at least 192 bits for U.S. Government Top Secret information. An ancillary benefit to Workday’s approach is that data backups are automatically encrypted as well.

**Multi-tenancy**

Multi-tenancy is a key feature of Workday, as it is with many hosted applications. Multi-tenancy enables multiple customers to share one physical instance of the Workday system without ever seeing each other’s application data. Workday accomplishes this through the Workday Object Management Server™ (OMS).

Each OMS can support multiple “tenants” (customers). Every user ID is associated with exactly one tenant, which is then used to access the Workday application. Almost all instances of application objects (such as Organization, Worker, etc.) are tenant-based, so every time a person creates a new object, that object is also irrevocably linked to this tenant. In other words, every user is uniquely associated with a specific tenant, and every new organization or worker or project—every object—that this user creates is also uniquely associated with this same tenant. The Workday system stores these links automatically and restricts access to any object based on the user ID. When a user requests data, the system automatically applies a tenancy filter to ensure it retrieves only information corresponding to the user’s tenant. This is how Workday can offer virtually error-free security at this level. The reason customers can share exactly the same instance of the Workday application is because the metadata objects (for instance, classes, methods, elements, or initial steps) are non-tenant-based, unlike the application objects.
More about the Object Management Server

Workday built its OMS on an open-source technology stack, using service-oriented architecture (SOA) principles. The technologies include the Linux operating system, MySQL database, Java, and Apache Tomcat for the application server. The OMS is the runtime component of Workday applications. It contains the application business logic and supports Workday’s secure transactional processing model. The OMS uses XML to communicate with a browser-based user interface and with Web services and Web services clients. At a high level, here’s how it works:

When the OMS receives an XML request—either from a Web services message or from the user interface server—it validates both the security and the content of the XML. The OMS processes the content (which could include updating certain business objects), then commits any changes to the persistence layer. Finally it creates a response in XML form, which it then returns to the requestor.

All XML, regardless of its origin, is validated by the OMS, meaning there’s no assumption that XML from the user interface server is valid. To further prevent anyone from entering invalid data, the user interface also applies validation rules as data is entered. This enables the application to exert strict, automatic control over what data the user can access or update. User A can change or view data for his organization only; he gets no access to User B’s organization. From a security standpoint, there are several advantages to this model. First, information is accessible only through XML, and only via the OMS. This essentially thwarts many common malicious attacks, such as SQL injection attacks. Also, there’s no need for a second security model for database-level access; having to maintain only one security model sharply reduces the likelihood that a human error will create a security flaw.