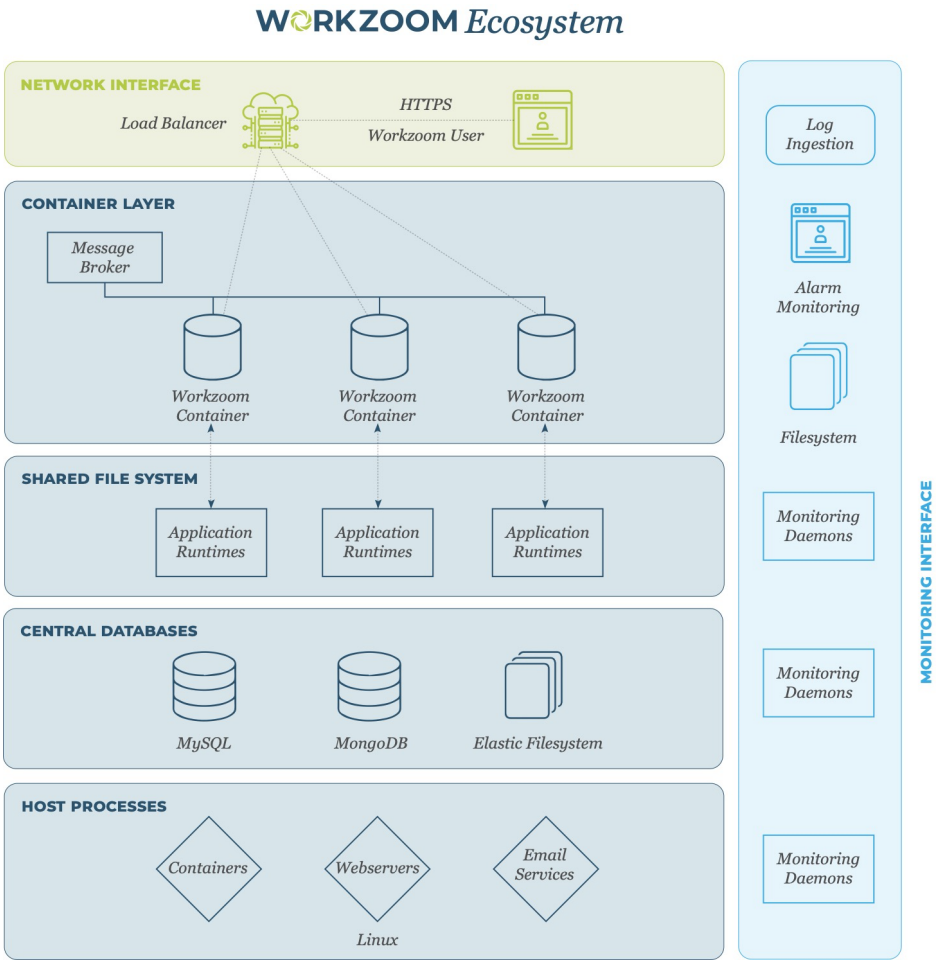
System Architecture

Workzoom is a highly scalable, cloud-based solution that runs on Linux servers provided by best-in-class hosting partners. Workzoom is a multi-tier, multi-threaded application built on our own unique, proprietary technology platform written in Java and running on Tomcat web servers. All persistent data is stored in a MySQL database while other content and media files are stored in an associated MongoDB Document Repository. Each Workzoom client has their own database schema and document repository instance which facilitates backup and recovery and ensures the highest level of data security. Application software, web resources, meta-data and common content are held outside the databases and are shared by all clients. Refreshable memory and file caches are used to achieve top performance. Workzoom is available around the clock (excluding scheduled maintenance) on servers with the highest possible uptime guarantees.



Cloud Data Storage

AWS Data Centers

Workzoom clients are hosted on Amazon Web Services (AWS) in data centers across Canada and the US. This ensures the highest system performance for clients, provides a more robust business continuity and disaster recovery regime, and complies with international data security requirements.

Cloud servers are located in fully guarded premises with physical access management and stringent security protocols. Access is restricted to authorized staff and intrusion prevention and detection systems are in place.

All data centers are Tier IV facilities with the following certifications:

- ✓ CSA
- ✓ SOC1, SOC 2, SOC 3
- ✓ ISO 9001 / ISO 27001 / ISO 27017 / ISO 27018
- ✓ PCI DSS Level 1
- ✓ PIPEDA
- ✓ FIPS
- ✓ FedRAMP
- ✓ NIST
- ✓ HITRUST CSF

Workzoom is powered by intelligent clustering infrastructure that utilizes auto scaling and self-healing capabilities to ensure maximum availability, resiliency, and speed. while maintaining strict control over client data via a central database.

Workzoom utilizes Amazon Web Services' global network infrastructure with Global Accelerators and Edge Computing to ensure absolute minimal latency by routing Workzoom traffic to endpoints nearest to the client.

Private Data Cloud Storage (optional)

Clients that require physical data isolation, can subscribe to our Private Data Cloud service. This service provides a private database instance that utilizes data at rest encryption with separate keys stored within a key management server. No data from other clients resides on the server. No other clients have access to the private data cloud. The private network is closed to all outside connections not originating from an authorized Workzoom VPN connection and a VPC Peering Connection is used to facilitate secure communications between the private data cloud and the Workzoom application servers. Workzoom authorized personnel maintain the private data cloud and utilize industry standard monitoring tools to check hardware for data integrity, resource consumption, and network failure. Real-time replication and application availability is monitored 24/7.

Data Replication, Back-ups and Recovery

Workzoom uses real-time replication for client data, across different availability zones with a minimum distance of 100 km to mitigate environmental and/or infrastructure-related failures. Encrypted back-ups are also taken daily (more frequent back-up options are available based on client requirements) and stored securely off-site at a minimum distance of 100 km from the primary server locations. The last 5 backups are also retained on-site.

In the event of an incident or server failure, clients are switched to the replication environment and in the worst case, data is recovered from the last daily backups. Because Workzoom application servers use intelligent clustering infrastructure that covers a multitude of availability zones at all times, no application downtime will occur in the event of an incident at a single data centre. However, in the event of a major incident, the maximum data exposure is 24 hours and recovery time would normally be between 5 minutes and 8 hours, depending on the size and volume of restoration required.

Security Framework

Workzoom actively mitigates the risk of cyber security incidents (including Advanced Persistent Threat attacks) by following strict security guidelines that include:

- ✓ **Minimizing attack surfaces**
  Workzoom servers reside in VPCs that utilize security groups to close all external TCP and UDP ports beyond HTTPS. All communication between Workzoom services is limited to within the secure VPC.

- ✓ **Following the Principle of Least Privilege**
  Root access on Workzoom servers is disabled and elevated user privileges are strictly limited. All use of sudo-level commands are logged and monitored using industry standard tools.

- ✓ **Separation of Privileges**
  Privilege separation is used on Workzoom servers via server hardening with SELinux. Process isolation ensures that users and applications are only able to operate in areas and directories that are absolutely necessary to their function (e.g. data backup tools are only granted read-only privileges, and only to relevant databases).

Vulnerability Management Program

Workzoom employs a comprehensive vulnerability management program that involves the following key elements:

- ✓ Vulnerability Scanning
- ✓ Penetration Testing
- ✓ Hardware, Software and Application Firewalls

- ✓ Comprehensive monitoring, logging, auditing and event management
- ✓ Virus, Trojan and malware protection

Vulnerability management best practices continuously improve. Workzoom evolves to stay current with the latest advancements.

Encryption

Stringent login authentication is in place. Passwords are encrypted with the "PBKDF2WithHmacSHA1" algorithm which includes salted password hashing with key stretching. This method ensures best of class protection against dictionary, rainbow table and brute force attacks.

All data in motion and in transit is encrypted using 128-bit+ TLS 1.2 over TCP/IP using a 2048-bit certificate and strong cipher suites.

Data at rest is encrypted using the Advanced Encryption Standard (AES 256).

Browser Security

As a cloud-based application, browser security is paramount. To ensure that only the most secure connections are made, only browser / operating system combinations that support transport layer security **(TLS 1.2)** are approved. Based on Workzoom's security configurations, servers will refuse to even acknowledge a connection request from non-supported browser / OS combinations to ensure all traffic across our network infrastructure is secure.

User Security & Access Management

Workzoom provides the following types of security:

- ✓ who can log into the system with start/end dates
- ✓ what "subjects" a user can access
- ✓ what tasks users can perform
- ✓ what data users can view, add, update, remove, etc.

Workzoom is primarily role-based. Because of Workzoom's HR focus, those accessing the system have pre-defined roles and responsibilities that are built into their job/position definition. These features extend to security so a person's role defines what information they have access to. That being said, Workzoom's security features are flexible enough that if an individual user or group requires an exception it can be applied down to the field level if necessary.

Workzoom has a default password policy in place within the application which can also be configured to meet the specific requirements of clients when necessary. Clients can define the following parameters within the password policy:

- ✓ Number of log-in attempts before lock-out

- ✓ Password duration
- ✓ Username and password format and length
- ✓ Password reset process

Workzoom also supports federated authentication using SAML (Security Assertion Mark-up Language) protocol and integrates with Azure AD. Other integrations are also available with single sign-on / identity management services using the SAML 2.0 standard such as OneLogin and Okta.

User Activity Logging

All logins and session activities are logged. For every log-in, action or change to the system, the application logs the user, the process, timestamp, IP address, original value and new value. Logging procedures are compliant with Sarbanes-Oxley requirements.

Workzoom Staff Data Access

Access to client data is restricted to individuals who support the client. All Workzoom personnel sign a non-disclosure agreement and code of ethics and are subject to background and criminal record checks as part of the new-hire process.

All Workzoom servers are isolated on their own VPC. Access to Workzoom servers is only available to a very limited number of authorized personnel. Access is only possible using a VPN tunnel with TLS1.2 ciphers and SHA256 key exchange. All data within the VPN tunnel is encrypted with AES-256 to prevent intruders from piggybacking on communications or packet sniffing. Additionally, all access to web consoles and administrator accounts are protected with Multi-Factor Authentication (MFA) using rotating access tokens. All VPN connection data is logged, and alerts are generated for failed authentication attempts.

All data will be securely removed from the Cloud and internal computers at the end of the engagement.

System Maintenance and Release Cycle

Thanks to our unique system architecture, Workzoom rarely requires more than a few minutes of downtime for maintenance. Most maintenance is conducted in the background. Each week, a server restart is conducted which takes approximately five minutes. On average, every two months there is a new Workzoom release which is done in the background and activated after the regular server restart. Quarterly updates are done in off-hours over a weekend with very little downtime. Upgrades to new major releases are planned events providing clients a window of opportunity suiting their business to upgrade.

Clients who subscribe to a secondary “Sandbox” environment can be provided an advanced copy of an upcoming release for their own testing purposes. Moving to a new release can be timed to

ensure it does not impact critical business functions (such as an active payroll run). However, all clients must be on the most current or previous release.

System patching for OS level and third-party application vulnerabilities deemed high-risk are tested and performed within a timeframe appropriate for the assessed risk. All updates are first tested on internal development and sandbox servers before being applied to production environments.

Client Penetration Tests & Vulnerability Assessments

Clients may conduct penetration tests and vulnerability assessments or engage a third-party to conduct them on their behalf with Workzoom's prior approval. We require 14 days advance notice of any testing, a detailed outline of the testing procedures and schedule, a signed non-disclosure agreement from all parties involved, and a copy of un-redacted results related to Workzoom technologies within 7 days of testing completion. We reserve the right to restrict testing in any manner including the timing, methodology and supplier performing the testing.

Incident Response

Advanced monitoring systems are in place at the hardware, database, and application level. Hardware is monitored for data integrity, resource consumption, and network failure. Real-time replication and application availability is monitored 24/7 with alerts being sent to technical personnel immediately. Client and system-level logging is also used for incident detection and prevention. There are strict guidelines in place for escalation in incident reporting and technical investigation.

In the event of a security or privacy incident, the procedure is:

1. The Workzoom Information Security Team and senior management are immediately informed.
2. A Critical Incident Report is started.
3. The Information Security Team does an assessment to determine the scope and severity of the incident.
4. Depending on the scope and severity, a communication is prepared and emailed to all clients affected.
5. The Information Security Team immediately takes action to contain the incident, restore availability and prevent it from reoccurring.
6. A post-incident review is done to determine the root cause and identify risk mitigation factors for the future.
7. If there is any data loss, clients are contacted individually to put data recovery plans in place.

Vulnerability Response Standards

The prevention, detection, mitigation and resolution of potential vulnerabilities in our systems is a top priority. Below are the standards we adhere to upon the identification of a potential vulnerability.

Common Vulnerability Scoring System

We use the Common Vulnerability Scoring System (CVSS) version 3.1 to rate potential vulnerabilities and security issues that may impact software in use. CVSS is an open framework for communicating the characteristics and severity of software vulnerabilities and is broadly used and accepted. More information can be found at https://www.first.org/cvss.

Vulnerabilities to the Workzoom Technology Platform

In the event that a possible vulnerability in the Workzoom Technology Platform is identified, we will confirm the vulnerability and score it using the CVSS methodology.

Other Vulnerabilities

Workzoom uses certain technical software supplied from other sources in order to host the application in the cloud (e.g. CentOS). Occasionally a vulnerability in this software may be identified that impacts the safe and secure delivery of services to our clients. For this type of vulnerability, CVSS Base Scores and fixes are provided by the software author.

CVSS Base Score and Resulting Service Level Standards

If a vulnerability in the Workzoom platform is identified, the table below outlines response and resolution time standards that will be applied from the date we become aware of the vulnerability.

If a vulnerability to other software impacting Workzoom systems is identified, the table below outlines response and resolution time standards that will be applied from the date the software author issues a confirmed fix. We will also use commercially reasonable means to rectify the vulnerability independently if a vendor fix is not immediately available.

CVSS Base Score	Response Time	Resolution Time
9.0+ (Critical)	4 hours or less	80% resolved within 1 business day
7.0 - 8.9 (High)	1 business day or less	80% resolved within 5 business days
4.0 - 6.9 (Medium)	5 business days or less	80% resolved within 25 business days
0.1 - 3.9 (Low)		
0 (None)		