WorkBase

Security And Privacy Whitepaper

July 2020

Overview

The confidentiality and integrity of our service is a top priority for Workbase. We have designed our products, processes, systems, and behaviors to meet or exceed our customers' expectations. We're committed to being transparent about our security practices and helping you understand our approach.

Security and privacy governance is led by the Chief Technology Officer at Workbase. All employees are required to understand and follow internal policies and standards. Our policies are reviewed quarterly with all employees. All new employees undergo mandatory security training with the CTO. Topics include device security, acceptable use, preventing spyware/malware, physical security, data privacy, account management, and incident reporting.

Application Security

Development Lifecycle

Standard best-practices are used throughout our software development cycle from design to implementation, testing, and deployment. All code is checked into permanent version-controlled repositories. Code changes are always subject to peer review and continuous integration testing to screen for potential security issues. Further, the code base is split into several separate repositories, with access only granted to those employees who are actively working on them.

All changes released into production are logged and archived, and alerts are sent to the engineering team automatically. Each release is tested in a sandboxed staging area prior to general release. Access to source code repositories requires strong credentials and two-factor authentication. The development lifecycle is based on git-flow and is held as close to the 12 Factor App Framework as possible.

Secure By Design

The Workbase platform is tiered into logical segments that separate business logic from underlying data storage. Each segment, from front-end, back-end, data pipeline and data storage, has its own security layer built-in. Additionally, both internal and customer secrets are stored and handled separately in a key vault. All activity with the key vault is logged and audited.

We leverage modern browser protections, such as Content Security Policy (CSP) and security HTTP headers to prevent Cross-Site Scripting (XSS), Clickjacking and other code injection attacks resulting from the execution of malicious content in the trusted web page context.

Authentication And Access Control

Workbase allows users to log in with Google accounts using OAuth 2.0. Workbase does not receive or store user passwords when using OAuth. We implement the most secure version of the OAuth 2.0 authorization code to mitigate attacks that could leak the user's access token. Both access tokens and refresh tokens are encrypted at rest using AES-128 encryption.

We can also integrate with any SSO provider that supports OpenID Connect or SAML 2.0 as an authentication method. This includes but is not limited to Okta, OneLogin, Azure, Ping Identity, ADFS, etc.

The above authentication flows have been tested against common attacks including but not limited to Cross-Site Request Forgery (CSRF) and misconfigurations of the redirect URL by an independent security testing company.

Vulnerability Management

Workbase works with third-party independent vendors to perform automated vulnerability tests and security status reports on the production environment. We also tap into the broader security community via a private bug bounty program and offer incentives for stakeholders to responsibly disclose software bugs and centralize reporting streams. This involvement of the external community provides an independent scrutiny of Workbase applications to help keep users safe. Engineers are always on call to immediately address any discovered threats to our network.

Data Security

Encryption
All data at rest in Workbase's production network is encrypted using 256-bit Advanced Encryption Standard (AES). Workbase leverages GCP Secrets Management Service (SMS) to manage encryption keys. Keys are never stored on disk, but are delivered at process start time and retained only in memory while in use. To ensure the security of our database, encryption keys are rotated regularly.

User Access
Data access policies are enforced at both the application level and at the database level. All access to services data is logged and designed to deny by default security posture. Users are granted short-living encrypted security tokens (JWTs). Role based access is also included down to an individual top-level data object level, with 4 user roles: Admin, Editor, Writer, Reader.

Employee Access
No customer data persists on employee devices or servers located in our offices. We apply the principle of least privilege in all operations to ensure confidentiality and integrity of customer data. All access to systems and customer data within the production network is limited to those employees with a specific business need. A best effort is made to troubleshoot issues without accessing customer data; however, if such access is necessary, actions taken by the authorized employee are logged.

Unauthorized Access
Workbase logs all logins, views and writes to an audit log, including time, user and IP address. Unauthorized requests to access the data fields are monitored and alerts to the CTO and security staff.

Audit Trails
All actions taken to make changes to the infrastructure or to access customer data for specific business needs are logged for auditing purposes.

Network Security

Encryption
Workbase uses SSL/TLS during data transfer, creating a secure tunnel protected by 128-bit or higher Advanced Encryption Standard (AES) encryption. SSL/TLS is further used to encrypt the traffic between our servers and databases within the same datacenter.

Isolation
Workbase divides its systems into separate networks using logically isolated networks in Google Cloud Platform data centers. Systems supporting testing and development activities are hosted in a separate network from systems supporting Workbase's production website. Customer data only exists and is only permitted to exist in Workbase's production network.

Network access to Workbase's production environments from open, public networks (the Internet) is significantly restricted. Only network protocols essential for making Workbase's service work are open at Workbase's perimeter. All network access between production hosts is restricted using security groups to only allow authorized services to interact in the production network.

Our infrastructure and applications are monitored using standard health checks and log watchers. This helps detect systems that are malfunctioning as well as potential intrusions.

Operational Security

Passwords Management
Every employee is provided with a secure password manager account and is required to use it to generate, store, and enter unique and complex passwords. We require an industry-standard best-practices Password Policy.

Access To Systems
All access to the production servers and data is protected using network isolation and strong authentication mechanisms. A combination of strong passwords, passphrase-protected SSH keys, a Virtual Private Network (VPN), and two-factor authentication is used to shield mission critical systems.

Hardware And Devices
We require employees to set all devices used for work to have strong passwords, full disk encryption and automatic lock when idle.

Datacenter Security
Workbase is hosted in Google Cloud Platform (GCP) data centers, which are highly scalable, secure, and reliable. GCP complies with leading security policies and frameworks, including SSAE 16, SOC framework, ISO 27001 and PCI DSS. More information can be found at https://cloud.google.com/security/compliance.

Disaster Recovery and Business Continuity
Workbase customer data is regularly backed up each day to guard against data loss scenarios. All backups are encrypted both in transit and at rest using strong industry encryption techniques. All backups are also geographically distributed to maintain redundancy in the event of a natural disaster or a location-specific failure.

Workbase uses third-party monitoring services to track availability, with engineers on call to address any outages.

Workbase is set up to operate from geographically distributed locations. By leveraging cloud resources, Workbase's infrastructure and customer support teams can support your business at any time.

Privacy

Customers retain control of their data and only provisioned users and specific Workbase employees have access. There is a standard 30-day data offboarding period after the end of any contracts. Data is available for direct download or secure transfer. Data is deleted from Workbase systems 30 days after the end of any contracts.

Workbase maintains a full privacy policy here https://getworkbase.io/privacy.