TeamTablet™ 55 / Flex

Cloud security

Overview

TeamTablet™ 55/Flex has four major components: Video meetings, Whiteboard, Wireless screensharing and Cloud administration. The relevant data for TeamTablet™ 55/Flex is for usage of FlatFrog Board (built-in whiteboard) and the cloud administration service. FlatFrog does not manage any data for video platforms or local wireless screensharing. For example, if you are using a Teams Rooms compliant appliance then the TeamTablet™ 55/Flex only shares the video feed as would any display or monitor. Same applies for wireless screensharing.

When you use FlatFrog Board to collaborate with remote participants, we provide access to any boards you may create on our cloud-based servers. We fully understand that cybersecurity is a key requirement for your business success. FlatFrog is committed to our central security principle to ensure that data remains confidential and secure.

Cloud infrastructure

FlatFrog Board (whiteboard) cloud servers and storage currently resides on **Google Cloud Platform (GCP) which is a SOC2 Type 2 and ISO27001 compliant platform**, located in Belgium, Europe.

GCP offers a comprehensive suite of cloud security tools that can help you protect your software service from evolving threats.

GCP's security solutions are built on a foundation of **security by design**, ensuring that security is embedded into every aspect of the platform. This includes:

Secure-by-default infrastructure: GCP's infrastructure is designed with security in mind, from the physical data centers to the software-defined network.

Layered security: GCP employs multiple layers of security, including identity and access management, data encryption, and threat detection and prevention.

Centralized management: GCP's security tools are centrally managed, providing a unified view of your security posture across your entire cloud environment.

The GCP products that we use include Google Kubernetes Engine, Google Cloud Storage and Google Cloud SQL.

We utilize GCP's audit logs, monitoring, and alerts to promptly detect incidents. Access to GCP is limited to a group of employees based on their roles. FlatFrog has an **onboarding and offboarding process for these personnel** to grant access to relevant parts of GCP. Personnel use multi-factor authentication.

Servers

Our servers run in a Kubernetes cluster that is **auto updated** and managed to make sure the most recent security improvements are used. All endpoints are protected with **TLS v1.2** and recommended cipher suites. We continuously monitor our endpoint protection on Qualys' SSL Labs to make sure they keep A+ score.

To safeguard sensitive information, we employ a centralized secrets management system that provides a secure and controlled environment for storing and accessing secrets. This system eliminates the risk of storing secrets on local servers or in code repositories, where they are vulnerable to unauthorized access. Access to the secrets management system is strictly limited to a select group of IT operations engineers, ensuring that only authorized personnel can handle sensitive information.

Data

Encryption

Your board content and related data is encrypted with **AES-256 at rest** and stored on Google Cloud Storage and Google Cloud SQL. In addition, all data **in transit** between internal cloud servers is encrypted. This data is not accessible on public endpoints and can only be accessed by a small number of FlatFrog personnel for service purposes.

Access

Multi-factor authentication (MFA) is used for all user accounts and administrative accounts. Least privilege access is enforced granting personnel only the permissions they need to perform their jobs.

FlatFrog implements stringent technical safeguards and robust internal policies that strictly limit employees' access to user boards and sensitive information. To safeguard user privacy and security only a **highly restricted** group of engineers engaged in developing core FlatFrog Board services possesses access to the environment where user data resides. Accessing users' boards is strictly confined to troubleshooting purposes and only occurs with **explicit** authorization from the affected users themselves. Upon an employee's departure from the company, their access privileges are promptly revoked to further reinforce the platform's unwavering commitment to user data confidentiality.

Regular **security awareness training** is provided to our personnel for educating them on data privacy regulations, password hygiene, phishing scams, and social engineering tactics.

This product adheres to the **General Data Protection Regulation (GDPR)**, ensuring that your personal data is protected and handled with transparency. We clearly inform you about the types of data we collect, how it is used, and the choices you have regarding your data. We collect only the minimum amount of personal data necessary to provide the services you request.

Backup and data loss

Your data is safeguarded with a robust backup system that protects against unexpected disruptions. Your work is continuously **backed up regularly** to a failover cluster, ensuring that it remains accessible even in the event of a system outage. Additionally, **daily backups** of the entire database are **stored separately** from the main data center, providing an extra layer of protection against data loss.

In addition to regular and enforced industry standard data backups, **data loss protection** solutions are implemented to monitor data usage and prevent unauthorized access, exfiltration, or modification of customer data. Data loss protection tools can identify and flag sensitive data, enforce retention policies, and block attempts to send sensitive data to unauthorized destinations. Furthermore, network segmentation is used to isolate sensitive data from other applications and servers.

User accounts and administration

Access to FlatFrog Board is protected by user accounts managed by Firebase Authentication. We allow users to sign up with email and password or use existing Google accounts. It is recommended to use Google accounts with multi-factor authentication for highest security.

For **enterprise accounts**, we provide a **tenant-based** cloud administration service that is a centralized platform to manage and control user access to cloud resources. It provides a unified view of user accounts, permissions, and configurations (including devices), enabling administrators to efficiently manage user access and enforce security and device policies. Each tenant has its own dedicated cloud environment, ensuring data and security isolation.

Our enterprise users can leverage SAML-based SSO (single sign-on) to seamlessly integrate TeamTablet and TeamTablet Flex into their **existing identity management systems**, enabling team members to access FlatFrog services using their existing credentials.

Guest Access

In FlatFrog Board, we allow guests to access boards using links or 6-character codes. The purpose of this is to allow users to conveniently evaluate the service.