Trusted Family

Security Overview



Trusted Family provides family businesses and family offices all the tools needed to manage communication, sensitive information, workflows, events and meetings in a single place.

Striking an optimal balance between security and usability, it affords an ideal private and secure environment to engage directors, shareholders and family members across generations.

OVERVIEW

With security at the heart of everything we do, Trusted Family's architecture incorporates patterns such as application containerization, encryption, event sourcing, and infrastructure as code. These assure optimal security in its use, ensure efficient recovery in case of errors, and provide control over security options that suit the needs of your organisation and its users.

Trusted Family

Our **business model** guarantees that data ownership is 100% yours and you can exercise full control over who has access.

We partner with best-in-class **infrastructure** providers who are equipped with state-of-the-art network and physical security solutions and processes in order to ensure high availability.

The **application**, available both on the web and most common mobile platforms, is developed with integrity baked right into our development processes. Moreover, it provides for your confidentiality through features that afford security without compromising usability.

Understanding that security is only as good as the **processes** in place and the **people** who implement them, we are devoted to following a holistic and disciplined approach.

Security is ongoing and we are committed to the continuous improvement of our posture. We routinely contract independent security experts to **test and audit** our platform through rigorous penetration testing and vulnerability assessments.

BUSINESS MODEL

Data ownership is 100% yours: We retain no rights to access, copy, or use it, except to provide you support and for troubleshooting. You have full control over who has access to not only the platform but also the different categories of data and can monitor and change these permissions at any time.

INFRASTRUCTURE

We partner with best-in-class infrastructure providers currently in the EU.

Our **application and databases** are hosted on DigitalOcean, an AICPA SOC 2 Type II and SOC 3 Type II compliant infrastructure provider who has also achieved Cloud Security Alliance (CSA) STAR Level 1 certification.

Trusted Family

For our **file storage and and search indices**, we avail of the Amazon Web Services' SOC 1, 2, and 3 compliant infrastructure.

As an additional security measure, we employ the SOC 2 Type II-certified **Content Delivery and Web Application Firewall** infrastructure of Cloudflare, an ISO 27001 certified organisation.





Trusted Family has been architected using Infrastructure as code allowing us to boot up different instances of our file storage and database on request, eventually allowing clients to choose their **geographical data residency**. This implementation also allows us to test the migration path of significant updates thereby avoiding issues during the final release to users. Availability of our infrastructure is **monitored 24x7** so that our support team can step in to handle issues as they arise.

To ensure **authorised access**, all secrets required for the infrastructure and the application API are stored in a dedicated encrypted vault. Access to servers is restricted only to **vetted system administrators** and their activities are fully logged.

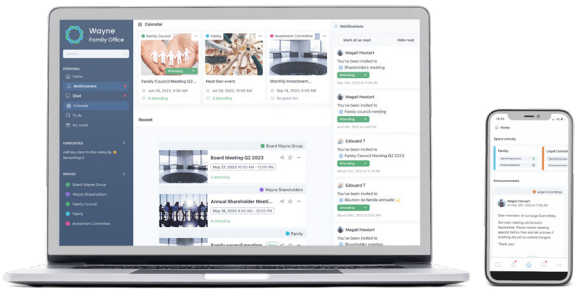
Daily **backups** are taken using redundant tooling and are distributed geophysically to ensure business continuity and disaster recovery.

APPLICATION

Available both on the web and mobile, our application avails of a **singular (strictly-typed) API** drastically minimising the potential attack surface.

Architected and implemented in **containers**, each application can not only be updated and released independently, but also availability and other issues impacting one application stay restricted without impacting the entire platform.

Trusted Family



Besides **encryption** of data at rest and in transit, we have taken encryption further to ensure your data is safe and secure from prying eyes. Not only does each client have a unique master key stored in a vault, but also the data in the database is encrypted with individual encryption keys. Since the master key (stored in a separate system) is required to decrypt the data, mere access to the database and backup drives doesn't provide access to the data itself.

An event sourcing pattern is employed to record (encrypted) all system-wide changes in the database facilitating **auditing, compliance, forensics, and non-repudiation**.

Besides static analysis running on our code, we also have a suite of unit, integration, and visual regression **tests that ensure optimal quality**. Development, integration and release **environments are distinct** and a continuous integration system is responsible for automated code builds (after making consistency and security checks), release, and rollback in case issues are found in production.

Access to the platform is restricted to invited members. Your community's access to content can be moderated through a sophisticated system of groups and permissions. Mechanisms for **authentication** include customisable policies and two-factor authentication. Administrators of your network will also have access to tools to secure user accounts.

BUSINESS PROCESSES

Attaining a requisite level of availability and security is a continuous process and is well assimilated in the day to day operations at Trusted Family.

Trusted Family

Employees are selected after rigorous vetting and undergo a security onboarding as soon as they join. Permissions are granted only as-needed and they undergo routine training and exercises that cover client confidentiality processes and data privacy regulations.

All Apple laptops are managed centrally through a **device management suite** and have their hard disks encrypted for enhanced security.

We use a suite of tools to monitor multiple aspects not limited to availability, application issues, and vulnerabilities and work seamlessly with our infrastructure providers to ensure a recovery point objective of twenty-four hours and a recovery time objective of four working hours. We have a well-tested **business continuity process** including incident response and disaster recovery and it is backed with adequate cyber insurance.

We routinely contract CREST-accredited experts to conduct network infrastructure **penetration testing** as well as (web and mobile) application **vulnerability assessments**.

Identified issues are discussed in the security committee which includes senior management and relevant issues are resolved as top priority.

Trusted Family

Revolutionize the way your family business operates digitally.

www.trustedfamily.com

©Trusted Family, All rights reserved