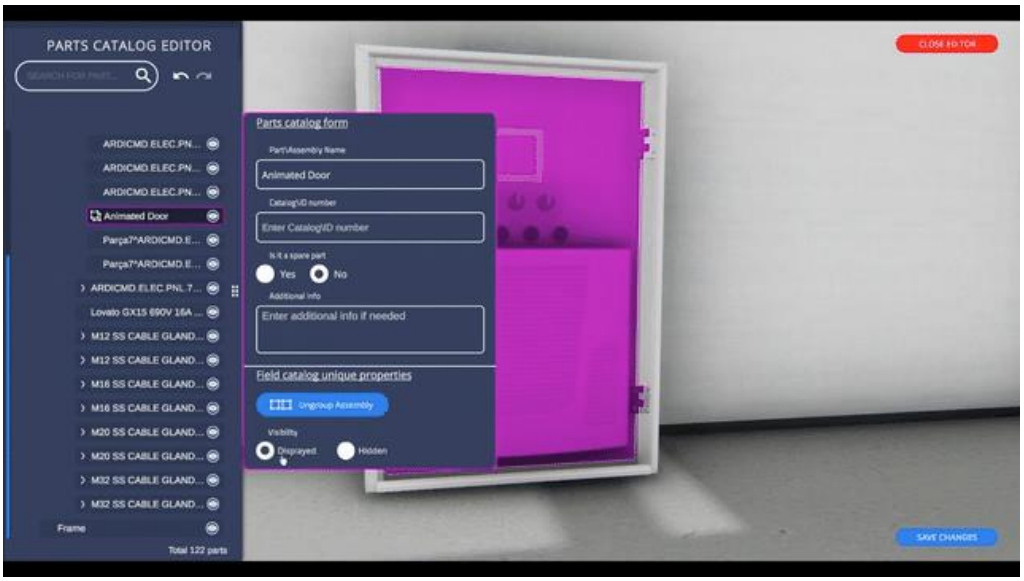
frontline.io - *Architecture and Data Security*



frontline.io solution is based on high-end solutions provided by leading IT companies including Microsoft, Google, and MongoDB, while supporting the highest standards of security and regulations.

How my data is secured using ***frontline.io*** – The Highlights:

- **Data is stored at one of the top three secured cloud providers.**
  - The storage cloud encrypts customer content stored at rest, without any action required from the customer, using one or more encryption mechanisms.
  - All data stored in a storage cloud is encrypted at the storage level using AES256, with the exception of a small number of Persistent Disks created before 2015 that use AES128.
  - The cloud service uses a common cryptographic library, Tink, which incorporates our FIPS 140-2 validated module, BoringCrypto, to implement encryption consistently across almost all Cloud products. Consistent use of a common library means that only a small team of cryptographers needs to implement and maintain this tightly controlled and reviewed code.

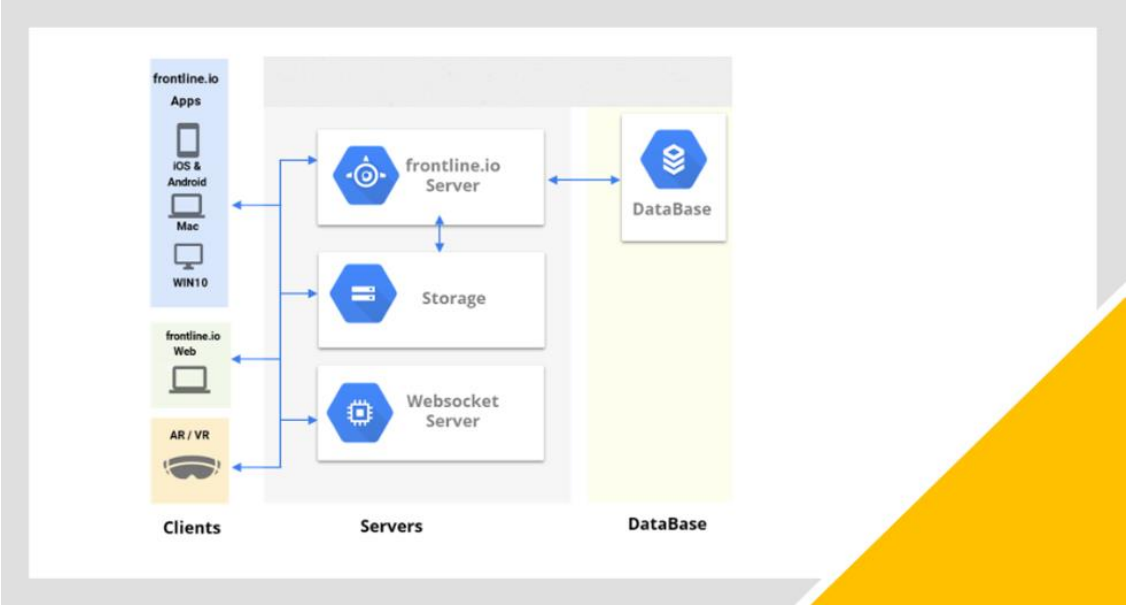
- **Only authorized users can view the data.**
  - Only invited users can join the workspace.
  - Permissions and authorization are assigned to each user.
  - Multi Factors Authentication on sign-in.

- User's data is stored in a secured database by MongoDB.

- **Guest users**
  - Guests cannot access any private knowledge base.
  - Guests can join the virtual training room or remote support only if invited and admitted.
  - Guest data is not stored on the guest device and therefore cannot be copied or reused.

frontline.io Security in Details

The below diagram describes the frontline.io platform architecture



frontline.io platform Building Blocks

Database

- Used for holding frontline.io data including:
  - Users
  - Procedures
  - Tasks
  - Files' metadata (images, video, pdf, 3D files)
  - Sessions
  - Analytics
  - Settings
- Technology: mongodb
- Storage: Atlas by mongodb
- Can be accessed by:

- frontline.io server with API key – when relevant
- Admin console with email and password
- Administration applications

File Storage

- Used for storing the knowledge base elements
  - Images
  - Video
  - PDF
  - 3D models
- Storage: Top 3 providers Secured Cloud
- Security:
  - Read - served by username and password
  - Write - secured API calls

frontline.io server

- Uses:
  - A buffer between the clients and DB
  - A buffer for uploading elements for the storage
  - Running offline jobs (e.g. Calculation analytics)
- Technology:
  - Runs on Cloud service – using cloud App Engine
  - Using node.js - Express application
  - 0-∞ instances
- Security:
  - Cloud DDOS protection
  - Accessed by:
    - Admin console (email & password)
    - Authenticated (JWT) REST API calls

Websocket server

- Used for connecting clients in the AR remote support feature
- Technology:
  - Runs a VM service – on a cloud Compute Engine
  - Using node.JS - Express server application
  - 1 instance
- Security:
  - Cloud-baseded DDOS protection
  - Can be accessed by:
    - Admin console (email & password)
    - Open API calls for handshakes

- Before handshake - any WebSocket support app (browsers, native apps)
- No connection to the DB

frontline.io Mobile Client

- Used for running frontline.io mobile applications
- Technology
  - Files are installed as APK / IOS files from play / app store
  - Served with mobile phone / tablet
  - *Unity* to native deployments
  -

frontline.io Web Client (Knowledge management)

- Technology:
  - React.js / Unity base webgl components
  - Files are stored on Google Cloud
  - Served with any browser, no installation

IT security capabilities and features list

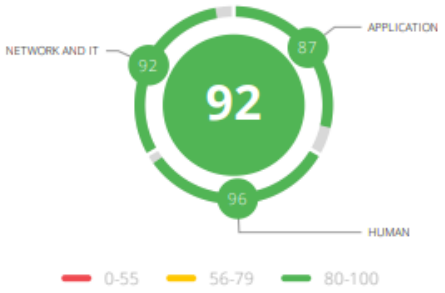
Feature / capabilities	Status
API security	Token based on REST API
Redundancy	All data is secured in leading cloud solutions - MongoDB Atlas – daily backup - Google storage – back is available upon customer request
Availability	All LLS services are committing to at least 99.98% availability
Passwords	Length – 8 characters Complexity – exists Rotation - exists
MFA	On signup – exists On sign-in – upon request
SSO	Upon request

frontline.io
by LLS

Cyber Security Monitoring Results by Panorays

Cyber Assessment

Cyber Posture Rating



Posture By Categories

Application	87
Application Security	87
Domain Attacks	100
Exposed Services	86
Technologies	94

Human	96
Responsiveness	71
Employee Attack Surface	100
Security Team	100
Social Posture	100

Network and IT	92
Asset Reputation	100
Cloud	100
DNS	100
Endpoint	--
Mail Server	92
TLS	86
Web Server	94

Industry Range

Internet Software & Services