Data Security on QMENTA Cloud

Security frameworks on the platform

QMENTA

QMENTA provides a powerful cloud based solution for neuroimaging to better understand the mechanisms of the brain and its various associated illnesses.

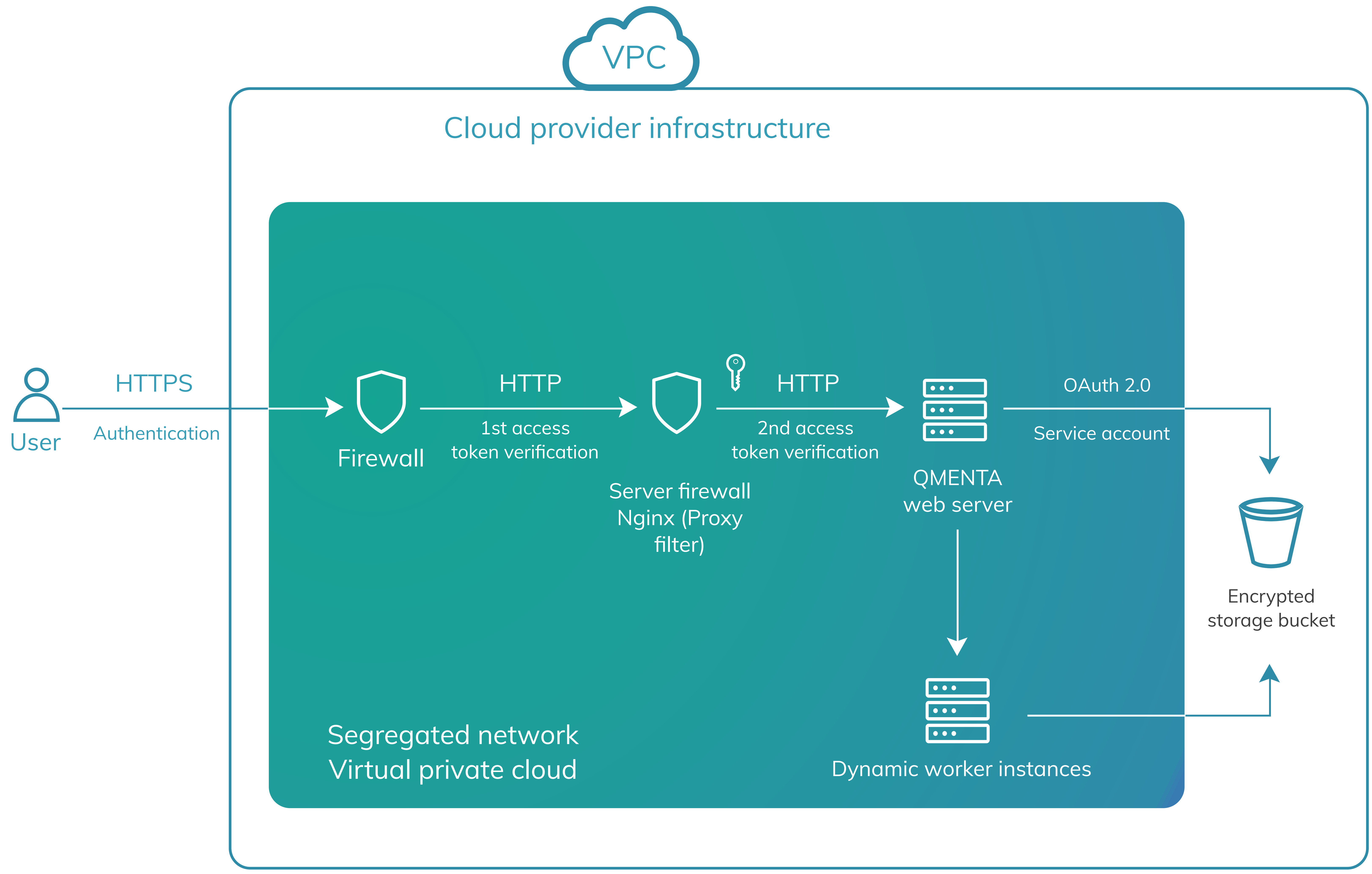
We aim to accelerate the discovery and development of treatments for brain diseases and further advance methods to identify and understand problems of the brain.

Introduction

QMENTA platform and its database has helped specialists, research organizations, biopharmaceutical companies and Clinical Research Organizations (CROs) in learning more about the human and animal brain, following the industry's comprehensive security framework.

The platform manages protected health information (PHI) contained in medical images and derived data in secure segregated network and encrypted data transmission. Security is critical to run businesses and research in this industry.

QMENTA understands the security requirements of the cloud architecture and the platform is designed to deliver even better security than traditional on-premises data archiving systems. Our comprehensive security strategy includes technical implementation, organizational structure, and many other business operations. The client's data is protected at all times - whether it is travelling over the internet or stored on the platform.



Platform & Infrastructure Security

QMENTA's platform is hosted on a cloud provider infrastructure that provides built-in compliance and security with industry certifications. The platform runs in the segregated network so that the data access is separated from other networks in the infrastructure and monitored by firewall to prevent cyberattacks.

When a user visits the platform, all data is transferred in encrypted format with HTTPS protocol. Only authenticated users are allowed to browse and upload data on the platform. The user automatically receives an access token and the token is verified by the firewall and server firewall to avoid spoofing. The web server is protected from malicious attempts by firewalls and Nginx.

The server also manages the business logic and user interface. When an analysis is launched, a dynamic worker instance is initiated to run the analysis using medical images. The images are stored in an encrypted storage bucket. The servers are authorized through OAuth 2.0 using a service account of the cloud provider. Since only the service account is allowed to access the bucket, the medical images are protected.

Data security

Access Control

Access control is flexible and secure. Patient data is organized in a ‘Project’ and the access permissions are granted by the Project owner. The Project owner can assign collaborator access - who can modify the subjects’ data -, or guest access - who are only allowed to view the information - to users. The platform offers other roles according to the user requirements.

QMENTA takes care of internal procedures for the data handling. The access to the patient’s data is limited to QMENTA administrators and they follow appropriate data access protocols.

The access to the platform is allowed only for authorized users through username and password and QMENTA administrators monitor the usage to deactivate invalid user accounts. Furthermore, QMENTA retains audit logs to track the activity on the platform as required by HIPAA.

Data Location

QMENTA’s aim is to facilitate and guarantee a study's confidentiality and integrity of all its data. When creating a new study to host and share data, you can easily choose a data center's location from a list of countries in Europe, North or South America, or Asia Pacific.

The selection of data location is important to comply with the EU-US Privacy Shield. The Shield highly regulates the transfer of personal data from EU to US and recommends limiting the transatlantic data transfer only for necessary situations.

QMENTA platform helps you comply with these privacy regulations. If you run your R&D activities in the EU, for example, you can choose to store your data in an EU region to avoid transatlantic data transfer.

Encryption

Communication between client's web browser and the cloud infrastructure is through an encrypted and authenticated channel, with a strong protocol (TLS 1.2), a strong key exchange (ECDHE_RSA), and a strong cipher (AES_256_GCM).

Protected health information (PHI) and data anonymisation

QMENTA cloud platform provides built-in and automated anonymization of all uploaded data, removing PHI from uploaded DICOM image files regarding the requirements to protect patient identity.

The platform also features a tool to automatically remove facial features from 3D anatomical images, should it be desired by the user. For the user's convenience, it is also possible to upload data to the platform directly through our web-app. This is intended for experts who wish to upload data quickly without any installation and with minimal effort.

In this case, the data is set through an encrypted channel and de-identified immediately upon receival to the cloud.

Users can also upload their medical images through a lightweight local app. The app strips out PHI to avoid it being transmitted over the internet and sends the de-identified data to the cloud in an encrypted format. The PHI is always safely isolated at the client sites.

Security controls

A rigorous security framework is ensured with the implementation of administrative, physical, technical, organizational, documentational, retentional, and other measures of security control. QMENTA platform is compliant with strict industry standards such as HIPAA.

Requirement	Compliance on QMENTA's platform
Administrative Safeguards	The platform covers all required procedures, including risk assessment and workforce security. A contingency plan is built together with our cloud partners.
Physical Safeguards	Data center security is handled by our cloud partners. QMENTA has implemented workstation securities.
Techical Safeguards	QMENTA platform offers access controls, audit trails, and user authentication. Additionally, QMENTA provides a local app to strip out Protected Health Information (PHI) from the datasets before transferring them onto the platform.
Organizational Requirements	A Business Associate Agreement (BAA) is signed between QMENTA and its clients & its cloud providers.
Organizational Requirements	QMENTA team has built required procedures and documents them in a repository.

Contact

To learn more about our recent developments and security implementations, you can regularly check our website at **www.qmenta.com**

Please do not hesitate to reach out to **info@qmenta.com** for any questions, concerns, or feedback.

QMENTA