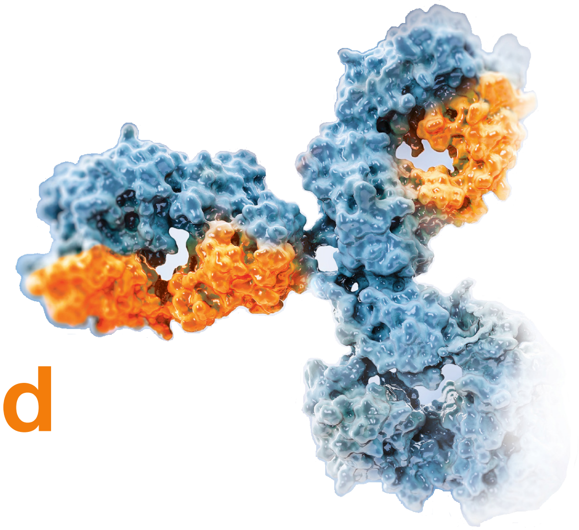
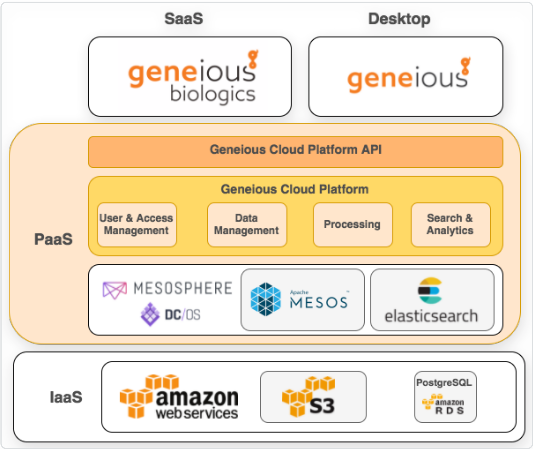


Ensuring Data Security in the Cloud

Geneious Biologics is a software-as-a-service (SaaS) solution delivered through the cloud. Data integrity and security is of utmost importance and we are committed to continually updating and improving the Geneious Biologics cloud capabilities to ensure customer data is hosted in the most secure environment possible.



Amazon Web Services

To leverage industry-leading security standards, we have chosen Amazon Web Services (AWS) as our primary cloud infrastructure provider. AWS is recognized for its comprehensive security and compliance features.

AWS ensures a very high uptime and security of data. Moreover, AWS is constantly monitored for intrusion by third party companies through audits and penetration testing to ensure no vulnerabilities exist.

Authentication and Data Access

Geneious Biologics users require authentication to access data stored in the underlying system architecture. For this, we use token based authentication.

Geneious Biologics is a single page web application that utilizes AWS functionality via REST API over secure HTTP (HTTPS). Geneious desktop applications utilize elements of this cloud functionality in the same manner.

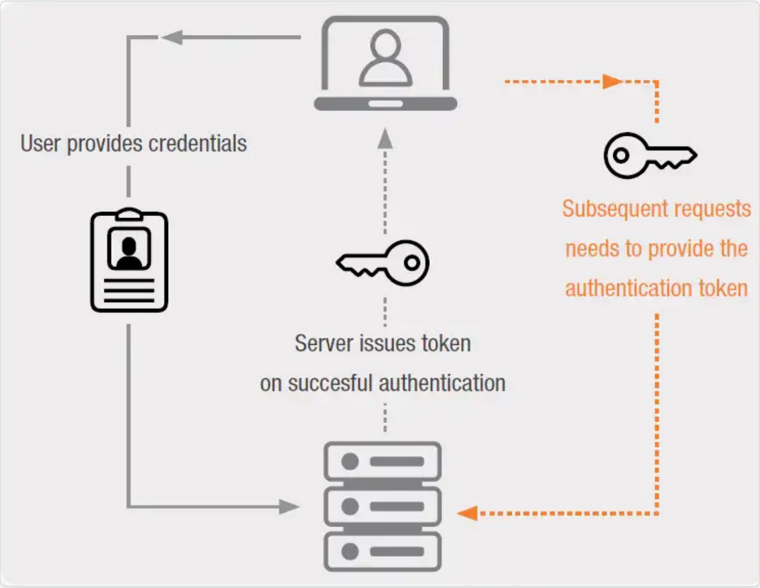

User provides credentials
Subsequent requests needs to provide the authentication token
Server issues token on succesful authentication

Figure 2. Geneious Cloud Platform user authentication process

Data Access

We guarantee that customer data can only be shared with users within the same organization. All uploaded and application generated data is by default accessible only to the user who created it. The owner of data needs to explicitly share their data with other users, within the same organization, in order for them to be able to access it.

Data at Rest

"Data at Rest" is inactive data that is stored physically in a database, disk or similar. Geneious Biologics data is stored within the highly secure AWS environment in either SQL databases or in BLOB storage (files) and is always encrypted.

Customers can choose to have their data reside within our EU or US environments. We follow the EU-US Safe Harbour Principles. Data will not leave the zone (EU or US) in which it was uploaded.

Data in Motion

"Data in Motion" refers to data that is traversing over the network. Communication involving the transfer of data between servers and the customer is encrypted. All communication or connection to Geneious Biologics or Geneious Prime uses Transport Layer Security (TLS) which is an encryption standard for data being sent over the internet. TLS connections use at least 128-bit encryption or stronger. The private key to generate the cipher key is at least 2048 bits.

Data in Use

"Data in Use" refers to data that is stored in computer RAM, CPU cache or other CPU registers during pipeline job processing. While, in some instances, data in use may be unencrypted, all pipeline job processing takes place within the highly secure AWS environment.

References

Amazon Web Services: Overview of Security Processes (White paper)

AWS Cloud Security (Resource center)

AWS Cloud Compliance (Resource center)

Data Backup

We guarantee that all customer data stored within the cloud is backed up on a frequent basis. This is to prevent any accidental loss of customer data due to unforeseen events. Customer data cannot be restored if customers delete their own data.

Data Retention

Upon termination of service, we guarantee that all client data will be physically removed from our databases. However, client data from previously performed database backups will only be removed once backups have gone past their end of life date.

Security Audits

We continuously monitor platform security and any security issues found as an outcome of such audits will immediately be given highest priority.

Our AWS account and source code are continuously monitored for vulnerabilities. In addition we engage with 3rd party firms to ensure the security of our platform and make sure we are following best practices. This includes an annual penetration test performed by a CREST certified member and a regular assessment of our cloud infrastructure by a member of the AWS Partner Network.

Other security measures

For a detailed description of AWS' security and compliance commitments, see the references section below.