

DNASTAR Cloud Security

Introduction

DNASTAR Inc. was incorporated in 1984, and we introduced our first cloud product in 2013. The DNASTAR Cloud lineup now includes Cloud Assemblies and the Cloud Data Drive in SeqMan NGen and NovaCloud in Protean 3D.

Our cloud-based applications enable storage and processing of vast amounts of data, including simultaneous genomic assemblies or protein structure predictions, without the need for costly computer upgrades. With proper credentials, a user can monitor projects and download results anywhere in the world with Internet access.

Cloud computing, by its nature, raises concerns about potential security issues. Data security has always been one of DNASTAR's highest priorities, which is why we have implemented a secure cloud framework that keeps our users' data and results safe.



DNASTAR Cloud Infrastructure

DNASTAR uses Amazon Web Services (AWS) as the supporting infrastructure for all our DNASTAR Cloud software applications. The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and data segregation.

AWS's world-class, highly protected data centers utilize state-of-the-art security monitoring and multi-factor access control systems. AWS supports compliance requirements for almost every regulatory agency in the world, including FedRAMP, GDPR, NIST, FIPS, and more. [Click here](#) for an AWS webpage with links to their security and compliance documentation.

DNASTAR builds on the AWS framework to keep your data completely secure and private: from initial cloud communications to long-term results storage.

When you use the DNASSTAR Cloud to upload and store data and/or to perform analyses, your data is password protected and is accessible only to you. Within your user account, data is encrypted for further protection. This means that neither DNASSTAR employees nor anyone else can access your data or results without your explicit permission (e.g., for troubleshooting an issue).

Data Security Pathway

DNASTAR has implemented several complementary strategies which ensure that your cloud data is protected, both in transit and in long-term storage.

Figure 1 and the rest of this section concern the flow of data between the user, the DNASSTAR Cloud application, and the Amazon Web Service (AWS).

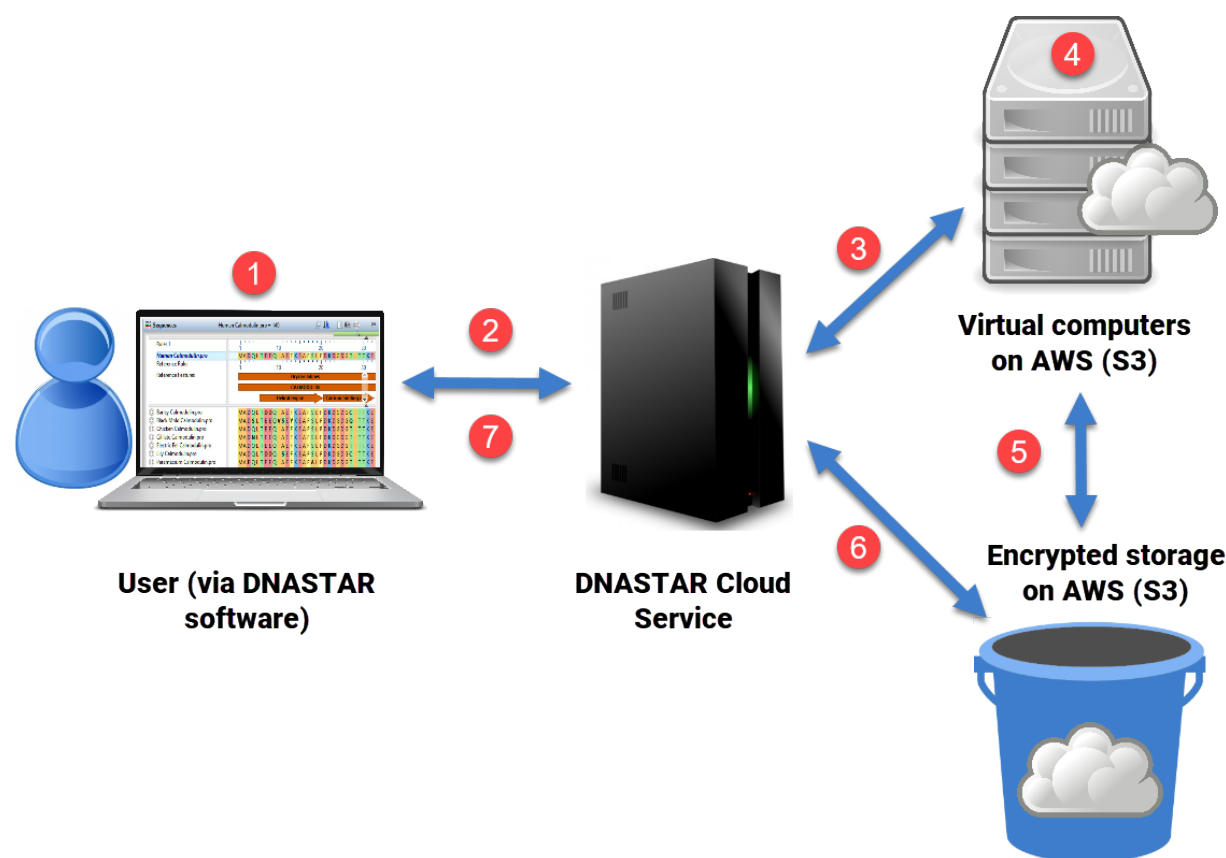


Figure 1. Example data flow between the user, DNASSTAR Cloud application, and AWS

The numbered steps shown in Figure 1 are outlined below:

Authentication is secured using a DNASTAR username and password, in the case of Cloud Assemblies. NovaCloud instead uses your license credentials to authenticate.

- 1) The user starts a Cloud Assembly job from within SeqMan NGen or a NovaCloud protein prediction job from within Protean 3D.
- 2) The DNASTAR Cloud Service, hosted on www.dnastar.com, authenticates the user's credentials and coordinates the rest of the cloud systems independently of the user's computer. For administrator logins, the username, timestamp, and IP address are logged in the admin console for tracking purposes. NovaCloud predictions also show their timestamps in the Protean 3D "Jobs" panel in the Start Time and End Time columns.

Communications are encrypted in transit with HTTPS/TLS and SSH/SSL protocols. For HTTPS, the standard port is 443.

- 3) The request to upload data, download results, or start a job is sent to the DNASTAR Cloud Service.
- 4) After starting one or more virtual computers on AWS, the DNASTAR Cloud Service relays authentication information, input data, and instructions to them.

Calculations are performed on isolated virtual cloud computers.

- 5) Calculations are performed using the AWS EC2 virtual server system via the Amazon Virtual Private Cloud (VPC). The virtual computers involved in a job are exclusive to a single user. For additional security, the virtual computers and all local data are deleted after the job is complete and after the data is transferred to a different secure location as directed by the user. These machines are firewalled from the Internet, except for required encrypted communications authenticated by the DNASTAR Cloud Service.

Results are encrypted and stored on the S3 cloud.

- 6) When the job is complete, results files are encrypted for storage with AES-256 on the AWS Simple Storage Service (S3) and retained there. S3 provides secure cloud storage and retrieval for any amount of data.

- 7) After a user's credentials have been validated by the DNASTAR Cloud Service and AWS, S3 facilitates fast and easy downloading of results to a local computer. If the progress dialog remains open through the end of a NovaCloud job, Protean 3D will download the results automatically. Otherwise, re-authentication of user credentials is necessary for continued access. Note that the URLs created by the DNASTAR Cloud Service for accessing files on S3 expire after several hours.

Notes about NovaCloud v.19

With the release of Lasergene v19 in 2026, there are two changes to how NovaCloud works in Lasergene Protein:

- Protein predictions run on the NovaCloud now use a token-based system. Data is only accessible from the physical machine where the prediction was initiated, and not from the DNASTAR account. Leaving Protean 3D open while the prediction takes place or opening it soon after the prediction finishes will cause the results to be downloaded immediately. Note that any results that are not downloaded within 90 days will be permanently deleted from the cloud and cannot be retrieved at that point.
- Boltz was added as a protein prediction algorithm in Lasergene v19. When you elect to predict a protein structure using the Boltz algorithm, an MMSeqs server is required to run the prediction. You can elect to install a local version of MMSeqs, use the DNASTAR-hosted server, or use the publicly available MMSeqs2 server on the Colabfold website. The DNASTAR MMSeqs server does not save or store any data and is therefore more secure than Colabfold.

Contact Us for More Information

Website: <https://www.dnastar.com>

Email: support@dnastar.com

USA Phone: 608.258.7420 or toll-free at 1.866.511.5090

UK Phone Free: 0.808.271.1041