

DNASTAR Cloud Security

Introduction

DNASTAR Inc. was incorporated in 1984 and we introduced our first Cloud product in 2013. We have since expanded our lineup to include a variety of powerful and convenient Cloud-based applications: Cloud Assemblies, Cloud Data Drive, and the four Nova Applications: NovaFold, NovaFold Antibody, NovaDock, and NovaFold AI.

Each of these 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 DNASTAR 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 DNASTAR employees nor anyone else can access your data or results without your explicit permission.

Data Security Pathway

DNASTAR has implemented a number of 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 describe the flow of data between the user, the DNASTAR Cloud application, and the Amazon Web Service (AWS).

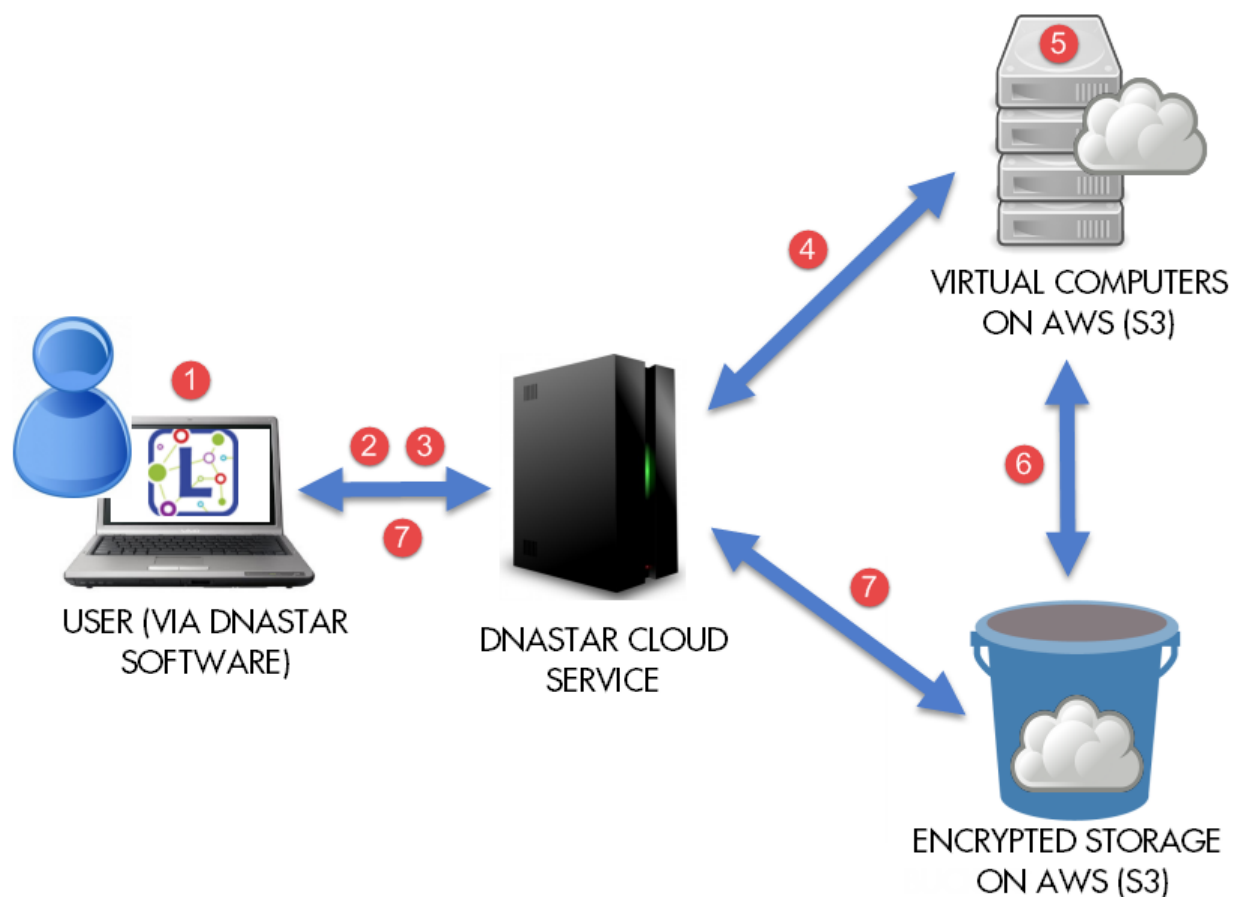


Figure 1. Example data flow between the user, DNASTAR Cloud application, and AWS

- **Authentication** is secured using a DNASTAR username and password.

The user launches a DNASTAR Cloud application and logs in using a unique username and password.

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 for tracking purposes.

- **Communications** are encrypted in transit with HTTPS/TLS and SSH/SSL protocols.

The request to upload data, download results, or start a job is sent to the DNASTAR Cloud Service.

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.

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 cloud.

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.

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. The URLs created by the DNASTAR Cloud Service for accessing files on S3 expire after several hours; re-authentication of user credentials is necessary for continued access.

Contact

For information on DNASTAR's Cloud-based applications, please visit www.dnastar.com or contact us at the telephone numbers below or at support@dnastar.com.