DNASTAR Cloud Security

(Last updated May 11, 2021)

Introduction

DNASTAR Inc. was incorporated in 1984 and introduced its first Cloud product in 2013. We have since expanded our lineup to include four powerful and convenient Cloud-based applications: DNASTAR Cloud Desktop, Cloud Assemblies, Cloud Data Drive, and NovaFold. 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.

©2021, DNASTAR, Inc., Madison, WI – Phone 608.258.7420 or Toll-Free 1.866.511.5090 – Fax 608.258.7439 – UK Phone Free 0.808.234.1643

Cloud Infrastructure

DNASTAR uses Amazon Web Services (AWS) as the supporting infrastructure for all our DNASTAR Cloud software applications. AWS's world-class, highly protected data centers utilize state-of-the-art security monitoring and multi-factor access control systems.

The AWS virtual infrastructure has been designed to provide optimum availability while ensuring complete customer privacy and data segregation. AWS has met numerous federal and private security certification requirements, including FedRAMP*. The remainder of this document explains, in detail, how DNASTAR builds on the AWS framework to keep your data private and safe, from initial Cloud communications to long-term results storage.

---

*For a complete list of AWS Compliance certifications, including the United States Department of Health and Human Services' Agency Authority to Operate under the Federal Risk and Authorization Management Program (FedRAMP) see https://aws.amazon.com/compliance.

©2021, DNASTAR, Inc., Madison, WI – Phone 608.258.7420 or Toll-Free 1.866.511.5090 – Fax 608.258.7439 – UK Phone Free 0.808.234.1643

Data Security Pathway

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). The example used here pertains to NovaFold and Assemblies on the Cloud, but other DNASTAR Cloud products follow a similar path.

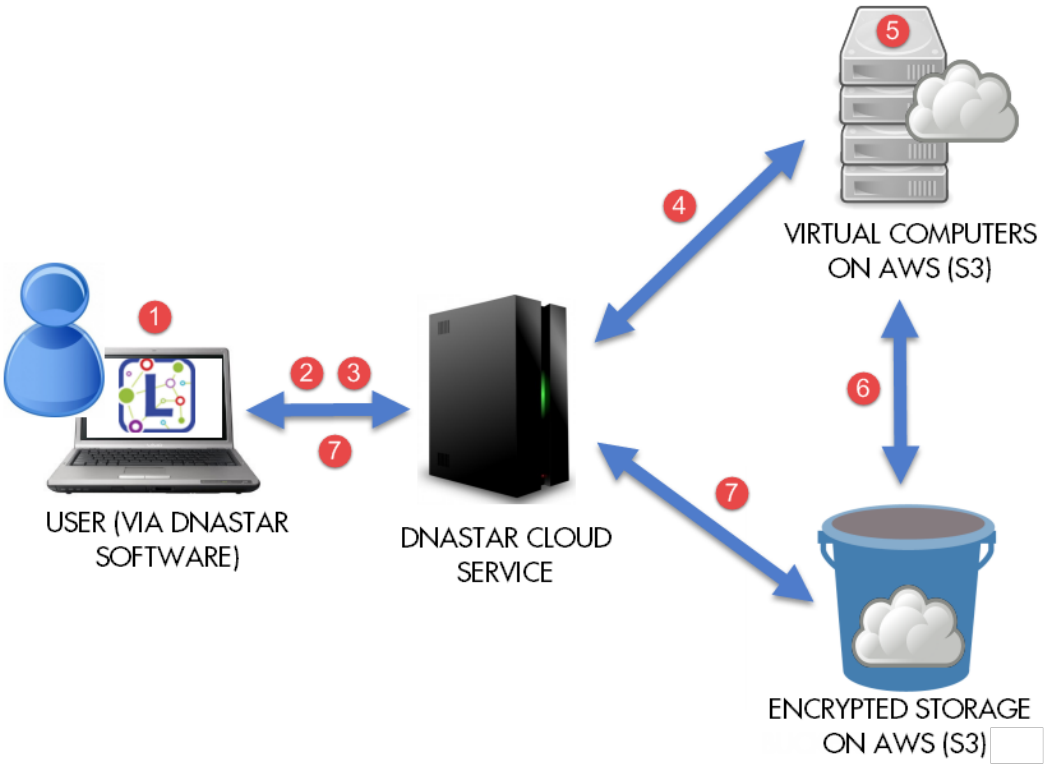

Figure 1. Example data flow between the user, DNASTAR Cloud application, and AWS

©2021, DNASTAR, Inc., Madison, WI – Phone 608.258.7420 or Toll-Free 1.866.511.5090 – Fax 608.258.7439 – UK Phone Free 0.808.234.1643

- Authentication is secured using a DNASTAR username and password.

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

    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 for tracking purposes.

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

    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.

©2021, DNASTAR, Inc., Madison, WI – Phone 608.258.7420 or Toll-Free 1.866.511.5090 – Fax 608.258.7439 – UK Phone Free 0.808.234.1643

- Calculations are performed on isolated virtual cloud computers.

5) Calculations are performed using the AWS EC2 virtual server system. 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.

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

©2021, DNASTAR, Inc., Madison, WI – Phone 608.258.7420 or Toll-Free 1.866.511.5090 – Fax 608.258.7439 – UK Phone Free 0.808.234.1643

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.

Conclusion

DNASTAR has implemented a number of complementary strategies which ensure that your Cloud data is protected, both in transit and in long-term storage. Neither DNASTAR employees nor anyone else can access your data or results without your explicit permission.

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.

©2021, DNASTAR, Inc., Madison, WI – Phone 608.258.7420 or Toll-Free 1.866.511.5090 – Fax 608.258.7439 – UK Phone Free 0.808.234.1643