White Paper

Agilent
Trusted Answers

Agilent Seahorse Analytics Security

Version 2.0.1

Overview

Data security and privacy, and its different aspects such as availability, integrity, and confidentiality, are of the highest importance for our customer. With our commitment to deliver the best quality services to our customers, security is addressed in all stages of a product's development lifecycle.

This White Paper shows how the Agilent Seahorse Analytics cloud platform implements security measures to meet the security needs of our customers.

Intended use

The Agilent Seahorse Analytics platform is intended for storage, visualization, and analysis of data generated by Agilent Seahorse XF Analyzers. The platform enables users to perform primary analysis of XF assay results, including assessment of data quality, outlier identification and removal, and normalization to a cellular parameter using flexible, intuitive analysis views and data widgets. Integrated result calculators allow users to create analysis reports for one or multiple assays performed on a single plate, then export these result reports to external file types such as Microsoft Excel and GraphPad Prism. The collaboration features allow users to share their data as the data are formatted, aiding in interpretation and explanation of experimental results.

Platform introduction

Agilent Seahorse Analytics is a software-as-a-service (SaaS) product. The tools included in the platform are delivered as services, meaning that the customer does not need to manage any components. The entire solution, from hosting to software updates and maintenance is operated by Agilent. The product is a multitenant SaaS application. The application architecture is designed to provide secure separation of customer data.

The underlying infrastructure, allowing the delivery of our SaaS solution, is based on the Amazon Web Services (AWS) infrastructure. We chose to host Seahorse Analytics in AWS data centers for the following reasons:

- Highly secured data centers with SOC2 and ISO27001 compliance
- Geographically spread infrastructure to store data close to the customer to improve performance and user experience
- High availability thanks to full redundancy of all hardware components
- Commitment to security standards and regulations

Web applications are accessible from the customer's office through a secure encrypted connection. Once connections have been filtered by the firewall system, users must authenticate to gain access to the application.

The platform leverages AWS features for administrator access, file storage, and logging. All AWS services used are designed for high availability. Data in transit to the application are encrypted using SSL encryption. Files in AWS are stored in an encrypted AWS Simple Storage Service (S3) using AES 256-bit encryption. Data residing in databases are not encrypted, protected by a private network. The application is multitenant, and is scaled to meet overall demand, not for a specific set of users.

The backend environment is not accessible from the public internet, and contains the databases and computer servers used for the services.

Backup and disaster recovery

File storage is designed for mission critical data. These strategies will mitigate data loss:

- Files are stored on multiple devices across multiple facilities.
- The database will be replicated in multiple zones, providing a backup in the event of catastrophe.
- The database will have automated backups.
- Snapshots are created daily with a finite retention policy.
- Automated backups will be performed weekly during low usage.

Agilent access to information

The following policies and conditions control access to user-generated content by Agilent personnel:

- Access user-generated content for the purpose of user support
- The Agilent Cloud Site Reliability Engineering team
- Privileged members of the Agilent Cell Analysis R&D Engineering group have default access to underlying code and data stored in the application for system maintenance purposes

Product development process

- All software applications are developed using industry best practices, and incorporate information security throughout the development lifecycle. Development teams have ISO 9001 certification.
- All system and software changes are tested before deployment.
- Separate development, staging, and production environments are maintained.
- Production data are never used for testing or development.
- All test data and accounts are removed before production systems become active.
- All temporary accounts, usernames, and passwords are removed before an application is released to customers.
- Source code is reviewed, and applications are tested periodically for security vulnerabilities, especially those related to:
  - Invalid login and authentication
  - Cross-site scripting (XSS) attacks
  - Injection vulnerabilities (for example, SQL injection)
  - Cross-site request forgeries (CSRF)
  - Improper error handling
  - Logical data separation to ensure that one customer's data is not visible to others even through programmer error
  - Customer data are protected from corruption even in the event of programmer error

Monitoring

The product has services that provide application-level logging and performance alerts for solution components. EC2 application servers will maintain HTTP-level logging.

The product has services that also provide alerts for components exceeding predefined system thresholds including (among others):

- Disk space
- CPU load
- Memory usage
- Backup success and failure
- Connectivity and availability
- Hardware issues

Failure to comply with predefined thresholds and any abuse of the service results in account termination and deletion of account content.

Security measures

This section addresses the main aspects of data security.

Availability: Ensuring that authorized users have prompt access to the information when they need it

Integrity: Safeguarding the accuracy of the information and the methods used to process it

Confidentiality: Ensuring that information is accessible only to those who need to use it

Auditability: Keeping evidences of events for root cause analysis

Availability

Security Feature	Implementation
Facilities	AWS data centers demonstrate a strong physical security process as acknowledged by their ISO 27001 certification.
Backup	All AWS features used to store data (S3, EC2, RDS) are backed up and replicated in different data centers.
Disaster Recovery	Application data are synchronously copied to another data center for recovery in case of a major incident.

Integrity

Security Feature	Implementation
PKI	All communication between customers and the application or within the applications themselves are encrypted and signed by certificates delivered by a certificate authority (CA).
Hardware Checks	All hardware underlying AWS services are proactively checked for failures, and proactive migrations are performed.

Confidentiality

Security Feature	Implementation
Authentication	Users must authenticate to a central login application and receive a session-based token.
Authorization	All users and administrators have specific access rights based on the least privilege principle.
Intrusion Detection	The application has services that protect against DDoS. Brute force attacks will be mitigated by account disabling in the event of multiple failed logins. AWS WAF ACLs will be used at the CDN and load balancing (ALB) levels to filter known intrusion patterns and block any traffic to the service. Vulnerability scanning is performed before product release to detect potential security breaches.

Auditability

Security Feature	Implementation
Logging	All user and administrator actions are centrally logged and regularly reviewed.
Change Management	All application changes or infrastructure changes go through a strict process that guarantees multiple levels of review before implementation.
Incident Management	All incidents (minor or major) are centrally logged. A root cause analysis is performed to improve overall security.

Regulations and compliance

The platform hardware is located in a SAS 70, Type II certified facility, which meets the most stringent civilian hardware uptime and security standards. Facilities ensure 24/7 information availability, prevent unauthorized access to hardware, and provide protection against hardware damage from accidents and natural disasters.

The implementation of the platform on AWS is reviewed by the Agilent Information Security Risk Management (ISRM) group, and must meet Agilent's Cloud Security Standards. These standards define guidelines around firewall implementations, server patching, etc.

The Agilent Seahorse Analytics platform is intended for research use only. The platform is not validated for HIPAA, GLP/GMP, or for use in diagnostic procedures.

The user data including files can be removed if the user closes their account, or for inactivity over 12 months.

www.agilent.com/chem/discoverxf

For Research Use Only. Not for use in diagnostic procedures.

This information is subject to change without notice.

Printed in the USA, February 19, 2020
5994-1562EN
DE.5557407407

Agilent
Trusted Answers