White Paper

# Agilent Clinical Informatics Platform Security

## Alissa Reporter

**Author**

Remi Bruggeman,
Agilent Technologies Belgium
S.A./N.V.

## Overview

Data security, privacy, and their various aspects, such as availability, integrity, and confidentiality, are of critical importance to our customers. Agilent commits to delivering the highest quality services to its customers, addressing security at all stages of the product development life cycle.

This White Paper explains how the Agilent Alissa Reporter implements security measures that comply with international regulations and standards. We have defined a set of policies, processes, and controls for security and privacy described in this document.

The document is divided into three sections:

- The platform architecture and implementation that enables us to deliver the highest level of security and to comply with the regulations
- The security measures we have deployed to ensure data availability, data integrity, and data confidentiality
- The applicable data privacy regulations and how we comply

## Introduction

The Agilent Alissa Reporter is a Software as a Service (SaaS) product. The tools included in the Agilent Informatics Genomics area are delivered as services, meaning the entire solution, from hosting to software application, is operated by our teams.

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

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

The Agilent Alissa Reporter is deployed in a layered architecture, as depicted in Figure 1.

Customers can access the platform's web application using a web browser and a secure, encrypted connection. After connections have been filtered by the firewall, users must authenticate to access the Alissa Reporter.

The platform leverages AWS features for administrator access, file storage and logging. All AWS services used are designed for high availability. The backend environment is not accessible from the internet. This backend environment contains the databases, message brokers and the compute servers used to execute bioinformatics pipelines.

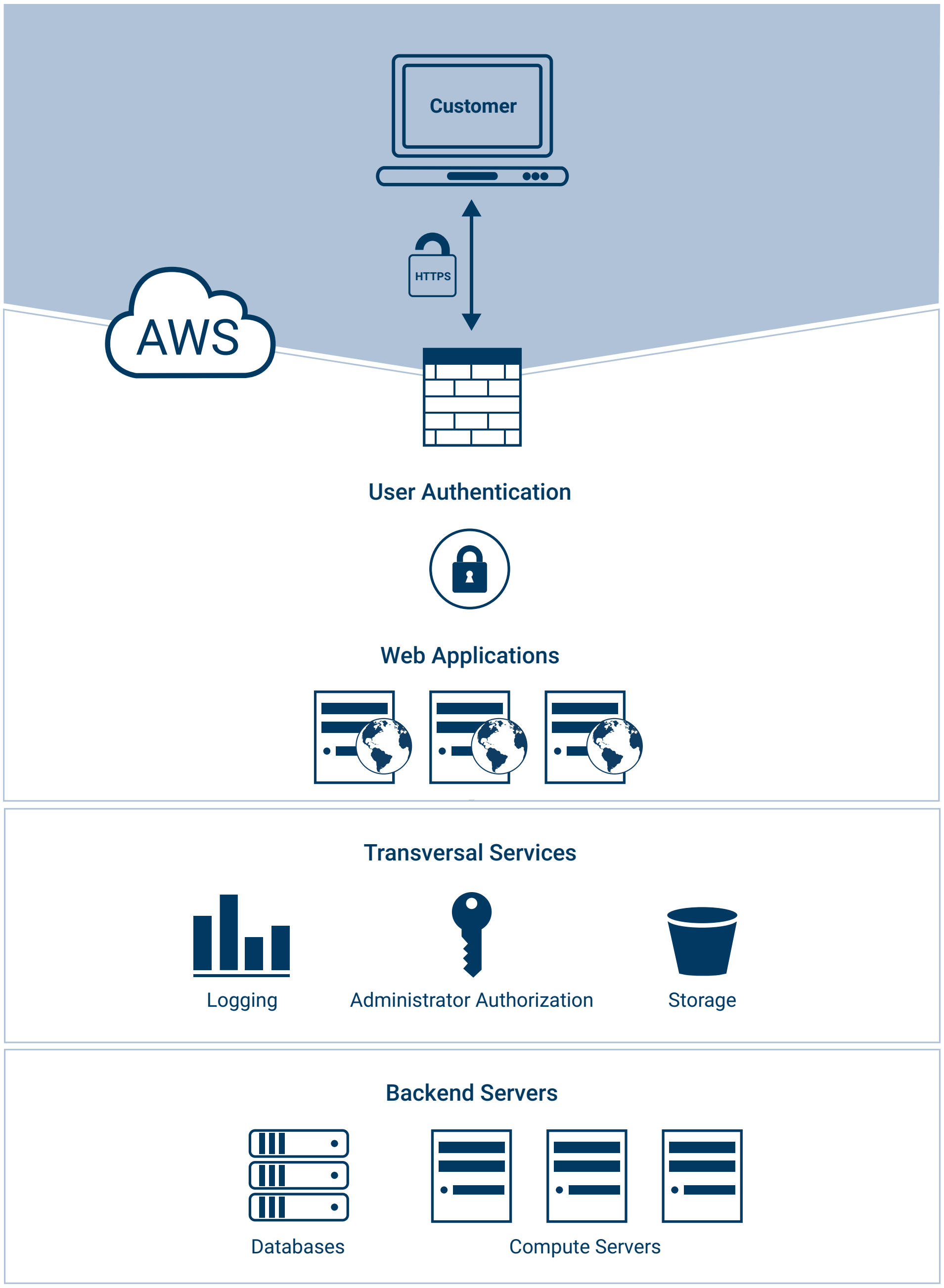

**Figure 1.** The secure layered deployment architecture of the Alissa Reporter platfrom.

## Security measures

This section details the the measures taken by Agilent to address the main aspects of data security:

- **Availability:** To ensure that authorized users have prompt access to information when they need it
- **Integrity:** To safeguard the accuracy of information and the methods used to process it
- **Confidentiality:** To ensure that information is accessible only to those who need it
- **Auditability:** To keep evidence of all events and facilitate root-cause analysis

## Regulations and compliance

Agilent software teams work with security experts worldwide to ensure that our SaaS products are compliant with international regulations and facilitate our customers 'compliance with international standards.

### Availability

| Security feature | Implementation |
|---|---|
| Facilities | AWS data centers demonstrate a strong physical security process, as acknowledged by their ISO/IEC 27001, ISO/IEC 27018, SOC1, SOC2, and SOC3 certifications. |
| Backup/restore | All features used to store data (S3, EC2, EBS, RDS, EFS) are backed up and replicated in different availability zones within the same geographical region; restore tests are performed at least once a year. |
| Disaster recovery | A disaster recovery plan is in place based on synchronous replication of the data and a strong backup/restore strategy for recovery in case of a major incident. |

### Integrity

| Security feature | Implementation |
|---|---|
| Public key Infrastructure | All communications between customers and the application or within the applications (between private services) themselves are encrypted (256-bit encryption) and signed by certificates delivered by an official certificate authority (CA). |
| Hardware checks | All hardware underlying the services are permanently checked for failures, and proactive migrations are performed. |
| Malware detection | All files uploaded in the platform are format controlled. |
| Intrusion detection | Continuous scanning of incoming and outgoing traffic is performed, which triggers alarms in case of suspicious events. Protection against DDoS and brute force attacks are in place. Vulnerability scanning is performed prior to product release to identify any potential security breach. |

### Confidentiality

| Security feature | Implementation |
|---|---|
| Authentication | Users must authenticate and receive a session-based token; a password policy is in place to avoid weak passwords, and a password expiration policy is in place. |
| Authorization | All users and administrators have specific access rights based on the least-privilege principle. |
| Encryption | All data in transit or at rest are encrypted. |

### Auditability

| Security feature | Implementation |
|---|---|
| Logging | All user and administrator actions are centrally logged and regularly reviewed; audit logs are accessible directly from the user interface. |
| Change management | All application changes or infrastructure changes go through a change control 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, and any incident involving personal data is communicated to the customer and to the appropriate authority, if required by law. |

## GDPR

In May 2018, the European Union (EU) General Data Protection Regulation (GDPR) replaced the 1995 EU Data Protection Directive (European Directive 95/46/EC).

We have designed processes to address new obligations under the GDPR that will enable us to help our customers comply with their GDPR obligations. To facilitate our global business, we adhere to the requirements for safeguarding transfers of personal data internationally, including through the use of Standard Contractual Clauses. All Agilent personnel receive training on the GDPR and Agilent's obligations as both a data controller and a data processor to our customers.

For a full explanation of how Agilent treats Your End User Personal Data please see our Privacy Policy at http://www.agilent.com/home/privacy-policy.

## Glossary

| | |
|---|---|
| **AWS** | Amazon Web Services |
| **DDoS** | Distributed Denial of Service |
| **EBS** | Elastic Block Storage |
| **EC2** | Elastic Compute Cloud |
| **EFS** | Elastic File System |
| **GDPR** | General Data Protection Regulation |
| **RDS** | Relational Database Service |
| **S3** | Simple Storage Service |
| **SaaS** | Software as a Service |
| **SOC** | System and Organization Controls |

## Legal disclaimer

This White Paper is for general information purposes only and should not be relied upon for the purposes of entering into legal relations with Agilent. All information in this White Paper is presented without any representation, guarantee, or warranty whatsoever regarding the accuracy, relevance,

or completeness of the information. Agilent accepts no liability for any loss, claims, or damages as a result of any party relying on the general information set out in this White Paper.

For more information on Alissa Reporter, please visit us at
www.agilent.com/chem/alissa-reporter

PR7000-3137

This information is subject to change without notice.

Printed in the USA, November 1, 2021
5994-4305EN

Agilent
Trusted Answers