Spectral Flow Analysis (SFA) - Life Sciences Cloud Platform Security Information

The Sony Group recognizes the importance of information security to maintaining the trust of our customers. To help attain this goal, Sony Group Corporation has established policies which set forth Sony Group's commitment to protecting the information assets, the customers, and the products and services of the Sony Group. These policies are based on the framework of ISO/IEC 27001:2022.

The security controls and documentation of the Spectral Flow Analysis (SFA)* platform are audited, reviewed, and approved by Sony Group Corporation security teams.

This document provides specific security information about the SFA Platform.

The SFA Platform is a cloud-based solution for flow cytometry data analysis that can efficiently perform a wide array of analysis protocols. Conventional analyses include gating, in which only specific cell populations are selected for analysis and quantification based on differences in scattered light and fluorescence signal intensity. Advanced analyses include dimensionality reduction, which enables a two-dimensional view of multidimensional information, and clustering, which automatically classifies cell populations.

System Structure

Physical and Environmental Security

The SFA Platform is hosted in Amazon Web Services (AWS) datacenters which follow the strictest requirements for physical and environmental security, ensuring the highest level of confidentiality, integrity, and availability.

System Architecture

The SFA Platform adopts a client-server model to provide various analysis capabilities to users. The client software is a PC application, and the server systems are built using the AWS infrastructure. All communications between the client software and the server systems are encrypted to exchange data securely. All confidential information which is stored on the server systems is encrypted as well. In addition to this, the server architecture is designed to provide secure separation of customer data. The software updates for security measures are provided by Sony according to Sony Security Development Lifecycle (SDL) which is described later.

Server-Side Infrastructure

The SFA Platform leverages AWS as its server-side infrastructure because it provides secure, high-performing, resilient, and efficient platform services. The SFA Platform utilizes the following AWS services: Amazon Elastic Compute Cloud (EC2), Amazon Simple Storage Service (S3), Amazon Relational Database Service (RDS), Amazon API Gateway, AWS Lambda, and Amazon Cognito. All services are used in accordance with Sony technical implementation standards which have been developed by Sony IT & Security staff and the AWS teams. Those configurations are enforced and managed.

All customer data files are securely stored in Amazon S3 with server-side encryption. Amazon S3 server-side encryption uses 256-bit Advanced Encryption Standard (AES-256).

External communications to the SFA platform and application servers only allow connections using Hypertext Transfer Protocol Secure. The SFA Platform uses end-to-end traffic encryption and Secure Sockets Layer (SSL)-terminating load balancers to ensure session traffic is encrypted using Transport Layer Security. A 2048-bit SSL certificate is used for secure communications.

Each user's data is stored in a different Amazon S3 bucket to achieve secure separation. Furthermore, Amazon S3 is designed to provide 99.999999999% (11 9's) data durability and redundantly stores data on multiple devices across a minimum of three Availability Zones (AZs) in an Amazon S3 Region.

All metadata related to customer data files is securely stored in Amazon relational database services (RDS) encrypted DB instances which use the industry standard AES-256 encryption algorithm—the same as Amazon S3. We designed the SFA Platform to launch Amazon RDS encrypted database (DB) instances into Amazon Virtual Private Cloud to achieve secure separation as well. Additionally, Amazon RDS provides a point-in-time recovery feature which enables restoration of data from a specified time within a certain retention period. All metadata in Amazon RDS is stored redundantly across multiple AZs.

Security Development Lifecycle

General

The SDL is a development process advocated by Microsoft Corporation (MS) since 2004 for safe software product development. In 2012, Sony adopted a reworking of the MS SDL as its own unique SDL (Sony SDL).

In the Sony SDL, practices to improve the quality of security (security measures) are implemented at each stage of product and network services development, from planning to shipping, operation, maintenance, and even disposal. These practices contribute to reducing the possibility and severity of incidents that may cause problems related to the quality of product security (security incidents).

Malware / Antivirus

Sony Group Corporation leverages the best-in-class cloud security tools to apply, maintain, and scale security policies across all deployment environments. Powerful security capabilities include the strongest host-based intrusion prevention systems (IPS), automation templates, and scripts. These tools deliver the following continuous cross-generational threat defense techniques to Sony AWS workloads and security operations requirements:

- Defend against network and application attacks. Proven security controls, like IPS and application control deployed on the server, enable context-based, high performance proactive protection.

- Keep malware, including ransomware, off servers by using sophisticated antimalware, application control, and IPS capabilities.

- Detect suspicious system changes. Changes may be an indicator of compromise, or they may simply need to be checked on for security and compliance. Where appropriate, changes can be blocked to protect against advanced threats.

- Accelerate compliance. It's critical for Sony organizations to remain compliant with the latest regulations.

- Lock down servers with application control built for the cloud. Give the power to prevent unauthorized software changes and stop unknown and unwanted applications from executing.

Patch Management

Regular updates of the SFA Platform provide a high protection level against new threats. The updated versions will address a wide range of known vulnerabilities in addition to new features. Moreover, the system is also releasing out-of-band fixes where necessary. In case a new relevant vulnerability is detected, a risk assessment will be conducted by Sony immediately. If required, a patch will be released to address serious vulnerabilities. An update of the client software is automatically detected at startup, and the update itself takes only a few minutes. Server-side infrastructure updates are performed automatically with no downtime.

User Authentication and Access

Authentication

The SFA Platform uses Sony Account for account management and authentication. Sony Account is Sony Group's global account service, which allows users to log in to various Sony group services with the same single account. All personal information related to the user account is managed securely by this account service. Sony Account complies with the personal data protection laws and regulations of each country and region, such as EU's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA).

The password policy of Sony Account includes the following requirements.

- Must not include 3 or more consecutive identical characters (example: 333 or BBB).

- Must not include 3 or more consecutive characters (example: 345 or ABC).

- Must be at least 8 characters.

- Must include at least 2 different types of special characters (letters, numbers or symbols (!, @, #, &, etc.)).

- Must not use the same string as the sign-in ID (email address).

Authorization

The SFA Platform has group management capabilities to provide access control and authorization to the resources such as acquired data from flow cytometers and experiment information. The group management consists of workspace and subordinate projects. Acquired data and experiment information are stored in a project, and all accesses to the resources are verified on the server side to check whether the accessing user belongs to the project and has access rights to it. Group members can be modified as desired to achieve dedicated access control and authorization.

Administrative Access

Access to the server side infrastructure is only by approved SFA platform personnel and is performed using the AWS management console. Administrator access requires multifactor authentication in addition to a password to gain access. Administrative accounts are prepared based on the principle of least privilege, and all such administrative access is logged and monitored. Access to sensitive information and confidential information is restricted, and account escalation is required to perform certain administrative functions and changes.

Regulations and Compliance

The implementations of both PC applications and server systems are reviewed by Sony's Product Security Department according to the Sony SDL. Sony's Information Security Department also reviews the implementation of the platform on the AWS infrastructure. Various security assessments are done such as risk assessment, static code analysis, and penetration test, according to Sony's security rules and guidelines.

Sony ensures to assess and remain in compliance with laws and regulations in the territory it intends to distribute its products. Therefore Sony's hosting provider, AWS, maintains certifications, including Health Data Housing (HDS), in line with applicable legal requirements.

Data Retention

Customer data is retained and protected for the duration of the service agreement. Upon termination of the agreement, Sony will collaborate with its clients to purge the data in accordance with the customers, and regulatory requirements.

Training

All Sony staff are trained annually for security and privacy compliance. Also, technical staff receive additional security and privacy training to complete their job functions.

Logging and Monitoring

The SFA platform is always monitored by the Sony global security operation center to detect anomalous activities and incursions to the network. All incidents are tracked and managed by trained professionals in collaboration with the necessary teams. Sony practices incident preparedness on a regular basis.

*SFA is a software name and an abbreviation for Spectral Flow Analysis. The SFA Platform is intended for Research Use Only. Please note that SFA is not designed to analyze, manage or store any experiment data which is linked with any personal information of sample donors. Please contact your Sales Representative with any questions or concerns about your intended use of SFA. The SFA Platform cannot analyze, manage, or store any experiment data which is linked with any personal information. The SFA Platform is only available in the US, Japan, France, Germany, UK, Belgium, Denmark, Sweden, Switzerland, Norway and the Netherlands.

For Research Use Only. Not for use in diagnostic or therapeutic procedures, or for any other clinical purpose.