WHITE PAPER

Connect platform

Technical and organizational data security measures supporting the Connect platform

Introduction

Thermo Fisher Scientific has implemented several standards and policies in order to help protect data from unauthorized access in our Connect platform. This document describes the various standards, data security approaches, business practices, and certifications used for the cloud-based storage that supports Connect.

Physical access control

Secure areas

Thermo Fisher Scientific uses physical access controls as well as globally controlled cardkeys and security cameras to maintain information security when accessing cloud-based third-party services. Cardkeys are managed globally by the physical security team and access can be added or revoked within minutes by 24/7 physical security representatives. Each Connect facility has a facility security plan that was externally audited and given an ISO 27001 Information Security certification. Each Connect facility has a Site Lead who ensures that only appropriate persons have access to the facility, and that access is appropriate for controlled access areas within the facility.

Network architecture controls

Our cloud database relies on the Amazon Web Services™ (AWS) platform for their network architecture controls. AWS provides Distributed Denial of Service (DDoS) protection through use of scalability features and elastic load balancers. Thermo Fisher Scientific limits access to application servers and infrastructure from both outside and inside of the corporate Thermo Fisher network. Network infrastructure is maintained by AWS, which provides their own certification for their processes. Segregation is maintained by virtual private clouds (VPCs) and networks, assigned to specific environments, and security groups are configured for least access necessary.

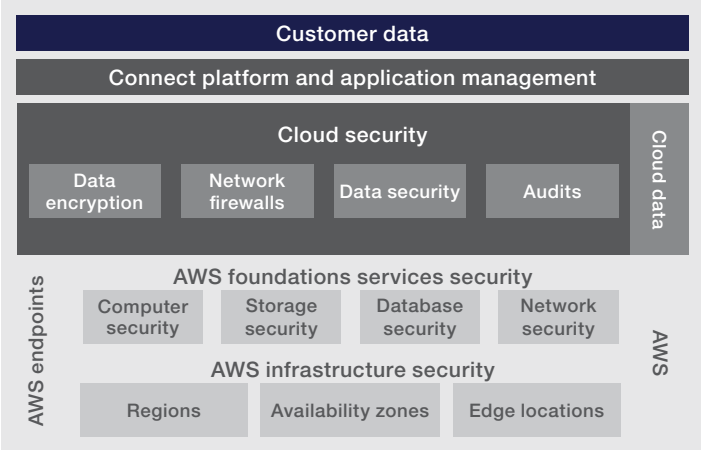

Figure 1. Architecture supporting the Connect platform.

ThermoFisher SCIENTIFIC

Note that the cloud does not provide infrastructure as a service (IaaS) to customers. The cloud is a multi-tenant software as a service (SaaS) application suite. Moreover, in terms of platform as a service (PaaS), the cloud is a collection of microservices based on a multi-tenant SaaS application. All microservices are configured for communication to relevant services, enforced through a custom security and routing infrastructure as well as AWS security groups. Cloud environments are configured for minimum network services. Access to these environments is possible only through specifically designed and deployed gateways to mediate authenticated access to APIs.

In terms of SaaS, Connect has features for data sharing that allow users to assign privileges to members of a sharing group. In addition, admin-level users can manage instrument access. Access to data is applied at the group level, with four levels of authorization: Admin, Edit & Delete, Edit, and Read Only.

Operational security

Thermo Fisher follows a standardized change control process that requires supervisor, configuration item owner, and QA governance approval. All releases are security scanned for application and infrastructure vulnerabilities, and all application teams maintain test procedures that are executed in test, stage, and production environments.

Managers must approve an employee's remote access. Remote access to the Thermo Fisher network is secured through certificates and access is terminated in the event of employee separation. Access is controlled through the use of secure VPN connections on authorized devices from Thermo Fisher Scientific. Connect application teams maintain assessments and registers of risks through the ISO 9001 certification process.

Connect applications follow a documented software development plan and standard operating procedures for management of infrastructure resources, and the applications utilize a standard logging platform that captures all application logs. Application health is also monitored using application health checks, resource utilization alarms, logging alarms, and synthetic transactions.

The cloud maintains four environments to support a software development plan (SDP): development, test, stage, and production. All applications are promoted through these environments, which are logically separated in AWS through separate accounts and VPCs.

Personnel security

Human resource personnel from Thermo Fisher perform background checks on all employees and contractors to the extent permitted under applicable law. Annual security awareness and information security policy review is required and documented for all employees.

Logical access control

Access control

The cloud utilizes an AWS VPC–specific network configuration. Everything is created and configured through the AWS CloudFormation. All deployments are made to either a US- or China-based instance of AWS. Services are deployed to multiple availability zones to ensure redundancy and availability. Servers and security proxies are deployed to a public network, and servers handling API calls and back-end logic are deployed to private subnets. Databases are also deployed to the private subnets. Each service deployment includes configurations for Amazon Elastic Compute Cloud™ (Amazon EC2™) security groups to ensure least-access privileges. By utilizing AWS VPC and Amazon EC2 security groups, each independent server has its own associated firewall rules. Network access is configured for least privilege, and privileges are only granted based on job requirements.

Encryption

Data in transit to the cloud is encrypted using SSL encryption. Data at rest in AWS Simple Storage Service (S3) is encrypted using server-side AES 256-bit encryption. Data that resides in databases, such as references to data in S3 and metadata, is not encrypted at rest. Keys are managed by AWS; hence, the encryption process is transparent to Connect applications. Here are the two types of encryption methods used:

In transit

Data uploaded from a user's computer or instrument to the cloud is encrypted. Web and mobile client access to the cloud data uses HTTP over TLS, otherwise known as HTTPS, utilizing 256-bit encryption. The HTTPS connections are terminated at the cloud web tier, API gateways, and the AWS S3 service. For Internet-of-Things (IoT) connected devices integrated with Connect, both Message Queuing Telemetry Transport (MQTT) over TLS and HTTPS are used to secure communications. MQTT is a standard protocol used for communicating device information. Each instrument is issued its own X.509 certificate, which is used to identify the instrument and encrypt data.

At rest

User-uploaded data for Connect is stored in the AWS S3. The data is encrypted using AWS S3 server-side encryption that utilizes 256-bit Advanced Encryption Standard (AES-256). All backups performed that contain customer data are also encrypted at rest.

Authentication

For administrative use, Thermo Fisher Scientific maintains authentication mechanisms utilizing both generated SSH (secure shell) keys and individual user credentials. Passwords are required to follow industry best practices for complexity and life cycle. Encryption keys for encryption of data are provided as a service by AWS and not maintained directly by Thermo Fisher Scientific. For administrative access, SSH keys are generated and stored securely. These keys are retired and changed as necessary.

Security and audit logs

Logs are retained in the Corporate Information Security (CIS)–managed log and security information and event management (SIEM) tool. Audit logs of user actions in AWS administration are recorded using AWS CloudTrail, retained in the corporate SIEM tool, and archived for a period of up to a year. Audit logs are not made available to end users or customers. This system ensures that logs are not tampered with and it manages access. Automated mechanisms are implemented to mine audit logging for suspicious activity. Also, AWS provides synchronization for audit logs produced through AWS CloudTrail.

Our security team performs security tests against the Open Web Application Security Project™ (OWASP™) top 10 security threats (Figure 2) and helps ensure that any identified vulnerability is fixed through a combination of code and configuration changes.

Web application security vulnerabilities

- Invalidated input
- Unsecured configuration management
- Buffer overflows
- Unsecured storage
- Cross-site scripting (SXSS) flaws
- Denial of service
- Injection flaws
- Improper error handling
- Broken access control
- Broken authentication and session management

Figure 2. Web application security vulnerabilities.

Monitoring, access management, and business practices

Network monitoring

Connections to the network are monitored and reviewed to confirm only authorized access and appropriate usage that includes internal and external connections. Logs are retained online for at least 3 months, and logs are reviewed daily using threat management tools and custom alerts. Performance is monitored through the use of AWS CloudWatch.

Identity and access management (IAM)

Access permissions are programmatically generated for AWS accounts based on the needs of a software developer and the application being developed. Access rights are assigned to individuals and applications based on their need to manage and support applications and are configured with AWS IAM roles. Specifically, a user's profile is associated with an AWS IAM role.

The Thermo Fisher Information Security policy mandates password restrictions; complexities and other standard restrictions are based on industry best practices. As a security practice, a list of access owners is regularly audited by assigned managers, and sensitive information is not distributed. Authorized mobile access to Thermo Fisher information assets is provided only via SSL connection, and mobile device management (MDM) is in place to further secure mobile devices.

Process and procedures

Thermo Fisher Scientific has corporate information security policies as well as standards and procedures for the Connect platform team that have been externally audited for ISO 27001 Information Security certification. Based on the Information Security Policy, information is classified (by requirements for confidentiality, integrity, and reliability) into the categories of Secret, Confidential, Internal Use Only, or Public. The information security policy and procedures are documented both as incident management procedures and as human resource procedures. Information security identification and reporting procedures are documented for the following five categories of incident:

- Production incident
- Nonproduction information security incident
- Cyber security incident
- Safety, health, and environmental incident
- Physical security incident

Application, monitoring, access card, VPN and system logs, and security camera footage are all components of the evidence collected and actively maintained against the possibility of an information security incident.

Connect partners with Thermo Fisher Legal to identify and comply with applicable legal requirements. Security incidents are escalated according to the procedure for the type of security incident that occurred. Customer communications, including incident communications, originate with Information Security or Product Management and are reviewed by Legal before being released to customers. The Connect platform allows customers to delete assets from DataConnect. If these assets are files, the files are removed from the primary S3 storage. The platform retains a copy in the backup S3 storage. If the assets are references, called app links, then DataConnect will send a notification out via AWS Simple Notification Service (SNS). When an application is subscribed to using app links, it will process the notification and delete the customer's data.

Authorization

Note that the intent of the platform is for each user to utilize his or her own individual account. For administrative access, Thermo Fisher maintains two-factor authentication and logins with the highest permission levels trigger alarms that are monitored by the CIS team. For administrative access, it is maintained and audited for appropriateness.

Connect maintains a standard change management process that is reviewed by key stakeholders including QA and Release Management. Least-access privileges are assigned, and administrators only have access to specific infrastructure and services that are necessary to provide support to their microservices.

Root accounts or highest-level privileges are maintained by the CIS team and require multifactor authentication tokens. These tokens are stored in a security digital storage location, which requires CIS team access and distribution. Customers are not provided with an administrator role over all users, and customers can create a collaboration group and invite users with necessary privileges to their data.

Backups and disaster recovery

Data are backed up once a day. Backups are maintained for at least seven days. In the event of a large-scale recovery, there is a standard order of restoration; however, there is currently no standard schedule for restoration process testing.

Data is maintained in AWS services within a specific region. Connect maintains high availability within an AWS region by utilizing multiple availability zones and appropriate networking and load-balancing services. At this time, the cloud maintains restoration plans because data are not currently replicated between regions. In the event of a wide-scale service interruption within the deployed AWS region, Thermo Fisher will only restore service once AWS has restored service to the region.

Multiple copies of the data are maintained for backups, utilizing AWS S3 that maintains object durability service-level agreement (SLA) of 99.999999999%.

Thermo Fisher maintains requirements for recovery point objective (RPO) and recovery time objective (RTO). Infrastructure is maintained as “Infrastructure-as-Code” utilizing scripts, including standard Amazon Machine Images (AMIs), and AWS CloudFormation configuration for AWS services. Databases are backed up daily, using AWS and third party–provided services.

Resource provisioning

Connect is a multi-tenant SaaS application and is scaled to meet necessary demand, not specific to an individual customer. SLAs are not guaranteed, however, scalability is “practically unlimited” as AWS services are utilized to achieve scalability. Monitoring capabilities are leveraged to identify scaling needs. All data are maintained in AWS storage services such as the Relational Database Service (RDS), DynamoDB, and S3 in the deployed AWS Region. AWS automatically handles the scalability of services, with the exception of RDS where Thermo Fisher manages storage levels and proactively provisions storage as necessary through configuration of the service.

The system is not regularly taken down for maintenance. In the unlikely event that a planned maintenance outage is necessary, Thermo Fisher will notify users through notifications within the application.

Incident management

Training is provided for the incident management process. Thermo Fisher maintains a standard first-level monitoring and support organization that is used to identify incidents and contact responsible parties. For major incidents, Thermo Fisher maintains a rigorous process for managing and maintaining incidents involving availability and security of applications and services.

The SIEM monitors network traffic as well as application logs. Incidents are documented within a Thermo Fisher incident management system. Customers are informed in the event a security incident pertains to their information/data, and they would be contacted by their account representative after receiving information from the CIS team based on the incident management policy.

Software development assurance

Connect follows a software development plan based on agile software development practices. Application development teams have achieved ISO 9001 certification, and the platform development team has achieved ISO 9001 and ISO 27001 certifications.

Source code is maintained in corporate-managed repositories through either the Apache Subversion™ (SVN) or Git system. Access is granted to developers who are participating on application development activities for specific repositories. Source code control systems are integrated with internal processes to help ensure access controls. System images are built with the minimum services and software installed, and the integrity of systems is monitored by security client software.

In addition to code reviews, the CIS team conducts vulnerability assessments of both infrastructure and applications before any production release.

Patch management

Thermo Fisher maintains standard images that are updated regularly or when vulnerabilities are detected, and applications are deployed using these standard images.

Our infrastructure as a service provider, AWS, maintains infrastructure for delivered services that Connect consumes. Thermo Fisher maintains processes to monitor and alarm for insecure configurations. For EC2 instances, Thermo Fisher maintains AMIs, which are updated and inherited by application development teams for the deployment of their microservices or applications.

Compliance claims

The Connect platform is ISO 27001:2013 certified, which is a global standard focused on information security management. ISO 27001 is a specification for information security management systems (ISMS). The ISMS is a framework of policies and procedures that includes all legal, physical, and technical controls involved in an organization's information risk management processes. ISO/IEC 27001:2013 certification means that we have taken the appropriate steps to keep assets with customer information secure. This certification helps ensure that the quality, safety, service, and product reliability of Connect has been safeguarded. In summary, regular assessments of all information security measures implemented ensure ongoing adherence to industry standards.

The Connect platform and applications are not currently validated for GLP/GMP compliance for PaaS or SaaS.

Acronyms

AMI	Amazon Machine Image
API	Application programming interface
AWS	Amazon Web Services
EC2	Elastic Compute Cloud
GLP	Good Laboratory Practice
GMP	Good Manufacturing Practice
IaaS	Infrastructure as a service
IAM	Identity and access management
MDM	Mobile device management
PaaS	Platform as a service
RPO	Recovery point objective
RTO	Recovery time objective
SaaS	Software as a service
SDP	Software development plan
SLA	Service-level agreement
SSL	Secure sockets layer
VPC	Virtual private cloud
VPN	Virtual private network

References

1. Amazon Web Services. Shared Responsibility Model. **https://aws.amazon.com/compliance/shared-responsibility-model**
2. Web Applications: Vulnerabilities and Security. **http://www.umsl.edu/~sauterv/analysis/f06Papers/Eghbal**

Find out more at **thermofisher.com/connect**

ThermoFisher SCIENTIFIC

COL18696 0319