Thermo Fisher Connect Platform, Enterprise Edition | Version 1.0

Product Security Information Guide

Thermo Fisher™ Connect Platform, Enterprise Edition | Version 1.0 | August 2024

Document valid through August 15, 2025

Introduction

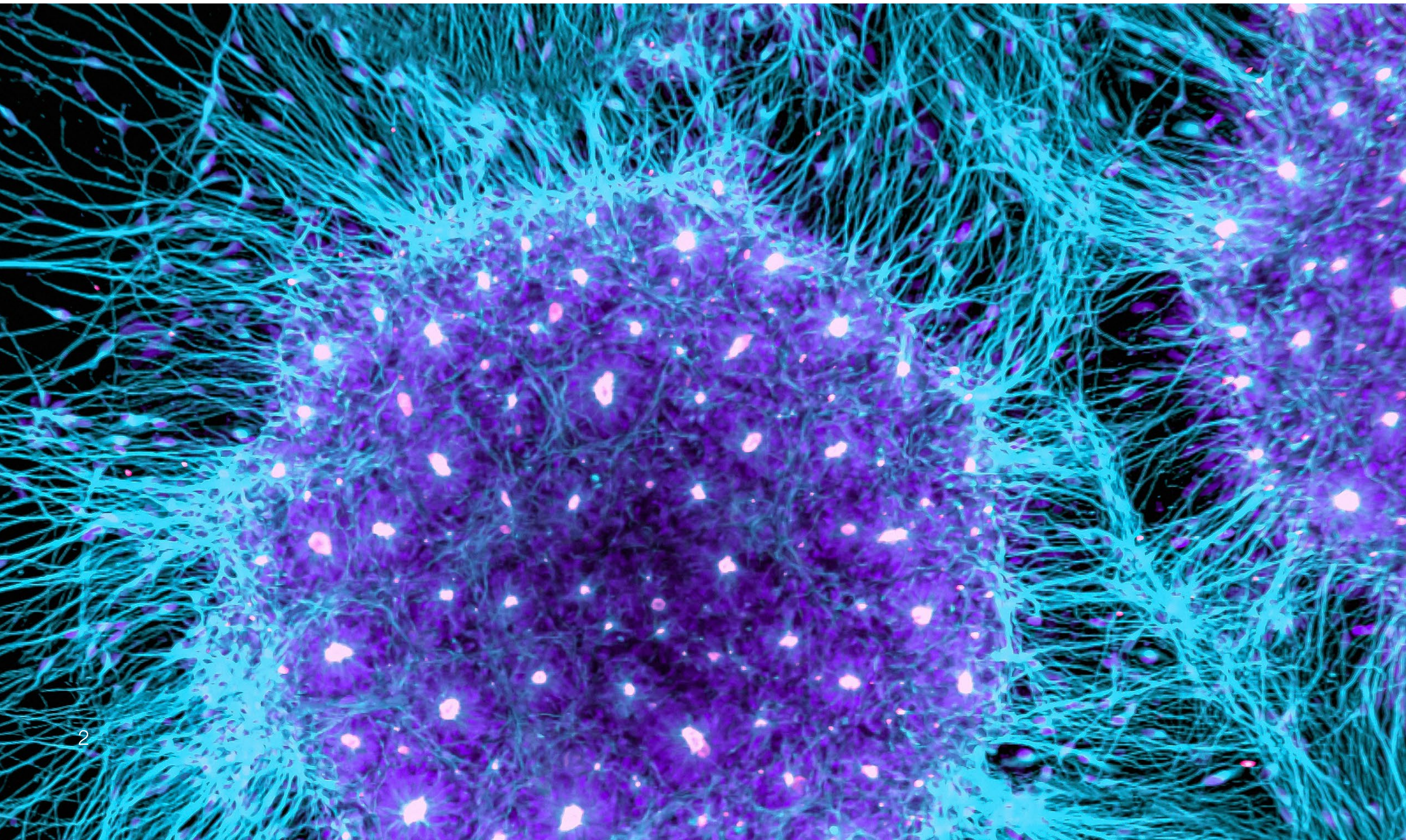
Thermo Fisher Scientific™ maintains a Cybersecurity Program which is designed to safeguard the confidentiality, integrity and availability of data and systems within our environment. Thermo Fisher Scientific supports a continuously improving security program model that is focused on reducing risk, defending against threats, maintaining data privacy and protecting our company's confidential information, including trade secrets and intellectual property.

About this guide

Thermo Fisher Scientific has implemented safeguards and protections designed to help protect the Thermo Fisher Connect Platform, Enterprise Edition application against intrusion or data compromise. This document describes the various standards, controls, and data security approaches and business practices that Thermo Fisher Scientific uses in this effort.

Due to the ever-changing cyber landscape, Thermo Fisher Scientific updates this Product Security Information Guide annually to maintain current, and accurate information. This guide expires on **August 15, 2025.** Contact your account representative to get the latest published version.

The information contained in this Product Security Information Guide is for reference purposes only. Nothing contained in this document or relayed verbally to any customer will be deemed to amend, modify or supersede the terms and conditions of any written agreement between such customer and Thermo Fisher Scientific, or Thermo Fisher Scientific subsidiaries or affiliates (collectively, "Thermo Fisher Scientific"). Additionally, this Product Security Information Guide does not create an independent contract or agreement between any customer and Thermo Fisher Scientific. Thermo Fisher Scientific does not make any promises or guarantees to customers that any of the methods or suggestions described in this Product Security Information Guide will eliminate security risks, restore customer's systems, resolve issues related to any malicious code or achieve any other stated or intended results. The customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this Product Security Information Guide.



Corporate Cybersecurity Program

Cybersecurity Program and leadership

Thermo Fisher Scientific's Cybersecurity Program employs technical, administrative and physical safeguards designed to detect vulnerabilities and address potential threats.

Thermo Fisher Scientific's Cybersecurity Program maintains an International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2013 certification for the management of the following areas:

- Cybersecurity program management and governance including risk management;
- Cybersecurity operations including security operation centers;
- Product security;
- Cybersecurity architecture and engineering; and
- Security awareness and training.

Cybersecurity governance and risk management

Thermo Fisher Scientific remains vigilant against potential threats for cyberattacks and other cybersecurity incidents and, therefore, we incorporate cybersecurity into our overall risk management process. We accomplish this through various corporate mechanisms, including quarterly business reviews, annual budget planning and targeted risk-based engagements.

Our commitment to cybersecurity emphasizes using a risk-based, "defense in depth" approach to assess, educate, block, identify, respond to and recover from cybersecurity threats. Recognizing that no single technology, process or control can effectively prevent or mitigate all risks, Thermo Fisher Scientific employs a strategy using numerous technologies, processes and controls to manage or reduce risk.

Digital forensics and incident response

The Thermo Fisher Scientific Digital Forensics and Incident Response Program leverages threat intelligence and internal data along with digital forensics techniques to investigate potential cyber incidents within Thermo Fisher Scientific's enterprise network. The capabilities of the Digital Forensics and Incident Response Program extend to monitoring the Connect Platform, Enterprise Edition assets.

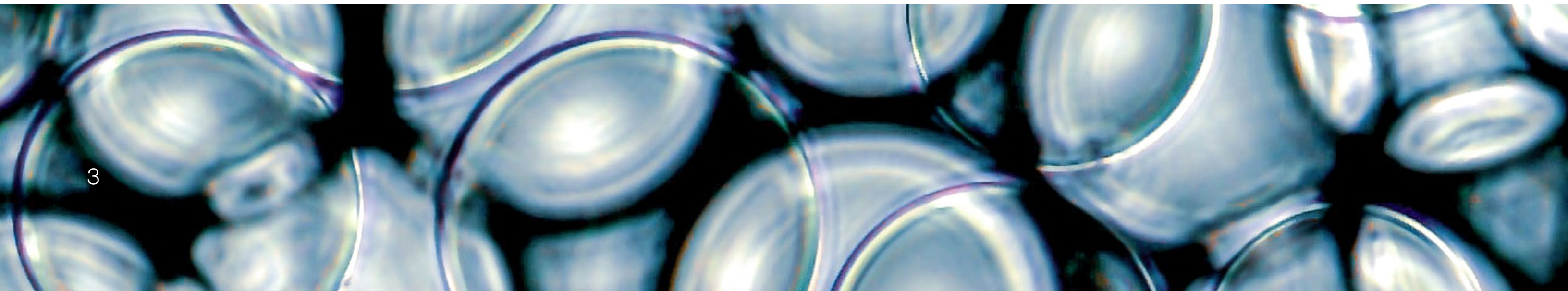
Incident management

Thermo Fisher Scientific maintains a process for managing cybersecurity incidents according to our Incident Response Plan. Thermo Fisher Scientific stores incidents in an Incident Management System and assigns an Incident Response Coordinator for threat mitigation and remediation. Once mitigation occurs, the team performs root cause analysis to reduce opportunities for recurrence and allow for continuous improvement.

Customers remain informed during potential security incidents that could impact their information as required by applicable laws, regulations and contractual requirements.

Threat intelligence

Thermo Fisher Scientific maintains relationships with various threat intelligence partnerships, including subscription sources and community-based or "crowdsourced" intelligence. This helps Thermo Fisher Scientific develop a deep understanding of existing and emerging security hazards and respond to threats.



Product overview

The Connect Platform, Enterprise Edition offers a robust suite of digital capabilities designed to enhance laboratory efficiency to deliver a more streamlined experience. The Connect Platform, Enterprise Edition, supported by dedicated Amazon™ Virtual Private Cloud™ (Amazon VPC™) infrastructure for each customer, provides cloud-based data storage, scientific analysis applications and peer collaboration tools to simplify data analysis and enable greater data visibility. The solution also monitors real-time telemetry data and allows for remote analysis of instruments to help prevent and resolve issues with Thermo Fisher Scientific's dedicated service team.

Security certifications and/or regulatory standards

Connect Platform, Enterprise Edition is developed under a Quality Management System certified to International Organization for Standardization (ISO) 9001:2015. Our ISO 9001:2015 certification can be accessed at the Thermo Fisher Scientific Digital Science Support Resource Center website.

Note: User authentication is required to access the Thermo Fisher Scientific Digital Science Support Resource Center website. Access is permitted through a valid support agreement. If you have questions, please contact a Thermo Fisher Scientific technical support resource at digital.support@thermofisher.com for more information.

Connect Platform, Enterprise Edition and its applications **are not** currently validated for Good Laboratory Practices (GLP)/Good Manufacturing Practices (GMP) compliance for platform as a service (PaaS) or software as a service (SaaS) offering.

Architecture diagram

The following diagram depicts the Connect Platform, Enterprise Edition architecture, providing a high-level overview on how users can access and interface with the platform.

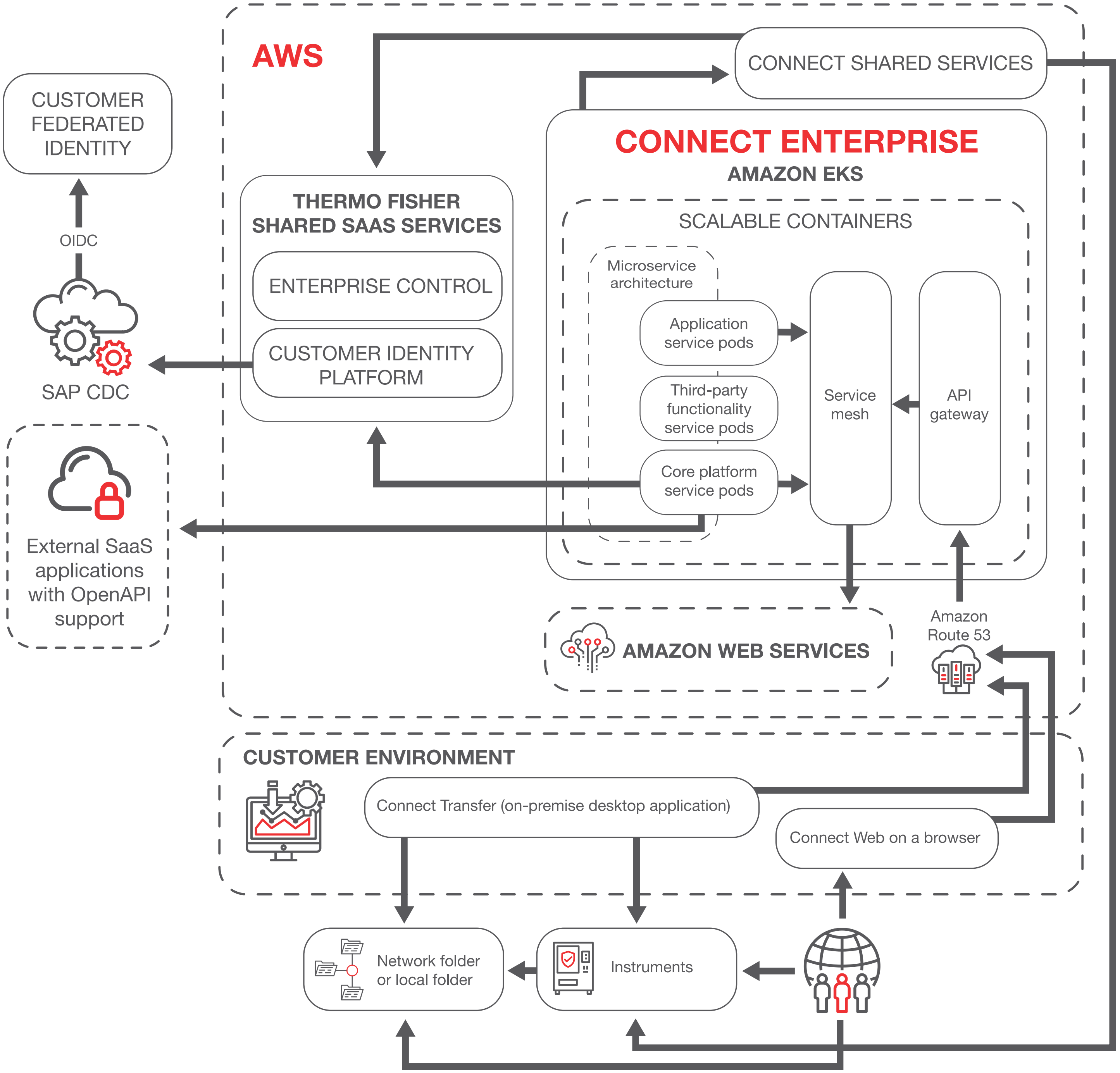

AWS
CONNECT SHARED SERVICES
CUSTOMER FEDERATED IDENTITY
OIDC
SAP CDC
THERMO FISHER SHARED SAAS SERVICES
ENTERPRISE CONTROL
CUSTOMER IDENTITY PLATFORM
CONNECT ENTERPRISE
AMAZON EKS
SCALABLE CONTAINERS
Microservice architecture
Application service pods
Third-party functionality service pods
Core platform service pods
Service mesh
API gateway
External SaaS applications with OpenAPI support
AMAZON WEB SERVICES
Amazon Route 53
CUSTOMER ENVIRONMENT
Connect Transfer (on-premise desktop application)
Connect Web on a browser
Network folder or local folder
Instruments

Figure 1: Connect Platform, Enterprise Edition

Component glossary

Component glossary

Component	Description
Customer federated identity	The customer's preferred Identity Provider (IdP). Other IdPs may be used for customers that do not use SAP™ Customer Data Cloud.
Customer identity platform (CIP)	The CIP assesses and validates OpenID Connect (OIDC) requests from the customer's IdP and creates an ID token upon successful authentication to Connect Platform, Enterprise Edition.
Enterprise control	Enterprise Control associates authenticated users with their specific tenant and subscribed applications.
Connect Shared Services	Connect Shared Services is an add-on subscription that extends the capabilities of Connect Platform, Enterprise Edition and Team edition. It enables seamless connectivity with a wide range of instruments and introduces a collection of specialized applications designed for different domains, such as Lab Management, Synthetic Biology and NGS. By leveraging Connect Shared Services, users can access enhanced functionality to improve workflow efficiency and productivity. Please contact your Thermo Fisher Scientific account manager for more information about adding Connect Shared Services to your subscription.
Service mesh and service proxy	Connect Enterprise, Enterprise Edition utilizes open-source platforms Istio (service mesh) and Envoy (service proxy). The service mesh coupled with the service proxy allow for microservices management and provide network and observability capabilities within the containers under Kubernetes™. Kubernetes is an open-source orchestration system used to automate software deployment, scaling and management of containerized applications.
Service pods (containers)	A group of one or more containers with specifications on how to run each container. There are three kinds of pods within Connect Platform, Enterprise Edition: application, third-party dependent and core platform. Each service pod utilizes microservices to perform a specific action within the application.
Application programming interface (API) gateway	Connect Platform, Enterprise Edition utilizes Kong, an open-source API gateway. Kong API gateway acts as an Ingress controller within Kubernetes where web browser (user interface) and programmatic (API) external requests flow into the gateway. The API Gateway uses the CIP to authenticate requests.
Connect Transfer	The Connect Transfer provides customers with the capability to configure file transfers. Local files, network drives and Amazon Simple Storage Service™ (Amazon S3™) buckets can be used for transferring to/from Connect Platform, Enterprise Edition. Files imported to Amazon S3 buckets use Hypertext Transfer Protocol Secure (HTTPS).
Connect Web Application	The Connect Platform, Enterprise Edition's browser-based user interface that lets customers perform application functions such as data management and workflow automation.

Table 1: Component glossary

Component glossary

Component	Description
Amazon EKS™ (Elastic Kubernetes Service)	The Amazon EKS service is a managed service that runs Kubernetes in the AWS environment.
Amazon Aurora™ PostgreSQL™ database	Amazon Aurora PostgreSQL is a fully managed, PostgreSQL-compatible relational database used to store data uploaded from customers to Connect Platform, Enterprise Edition.
Amazon Simple Email Service™ (SES)	An AWS-managed email service used for customer notifications.
Amazon S3	An AWS-managed file storage service used to store files uploaded from customers into the Connect Platform, Enterprise Edition environment.
Amazon Simple Notification Service™ (SNS)	An AWS-managed notification service that lets customers view all available system-generated notifications and alerts.
Amazon OpenSearch™ service	An AWS-managed search service based on the open-source search engine Elasticsearch. The OpenSearch Service allows Thermo Fisher Scientific to deploy a search cluster within the Connect Platform, Enterprise Edition environment.
Amazon MQ	An AWS-managed service for message brokers that uses RabbitMQ to communicate information within the Kubernetes cluster.
Amazon Route 53™	An AWS-managed domain name system (DNS) service used to route end users to their dedicated Connect Platform, Enterprise Edition tenant.

Table 1: Component glossary, continued

System access controls

Authentication and authorization

Customers leverage two methods to authenticate to Connect Platform, Enterprise Edition: direct login and federated login.

- **Direct login:** Users can establish their system identities directly within the platform.
- **Federated login:** Connect Platform, Enterprise Edition supports federated login through a customer IdP on either OIDC or Security Assertion Markup Language (SAML) protocols. Thermo Fisher Scientific's CIP team can configure a trust relationship with the customer's IdP upon request, providing two options:
  - Domain-based authentication: All users from the customer's IdP can authenticate to Connect Platform, Enterprise Edition.
  - Specific-user authentication: This option restricts the authentication to a predefined list of users.

Administrative access to Thermo Fisher Scientific application servers and infrastructure (including access to the AWS console that manages Connect Platform, Enterprise Edition) requires multifactor authorization (MFA). Thermo Fisher Scientific limits access to application servers and supporting infrastructure to authorized personnel only.

The Connect Platform, Enterprise Edition leverages role-based access control (RBAC) to grant permissions and access to authorized users, where roles are configurable to meet necessary business requirements. Thermo Fisher Scientific recommends that role assignments follow the principle of least privilege, providing only the required system access needed to manage the Connect Platform, Enterprise Edition.

Firewall and network controls

Thermo Fisher Scientific manages the security of the Connect Enterprise Platform network by providing customers their own dedicated AWS account and networking infrastructure, including VPCs to isolate virtual networks. In addition, AWS security groups can be leveraged for host-level virtual firewalls and network access control lists (NACLs) are used for controlling traffic in and out of subnets. Network access is restricted using these AWS services to allow only necessary traffic according to business requirements. Only externally facing services of the Connect Platform, Enterprise Edition are accessible via the internet.

Password management

Thermo Fisher Scientific recommends that password requirements follow organizational or industry best practices. For access to internal systems, Thermo Fisher Scientific's Information Security Password Policy mandates all employees to generate complex passwords, enforced by internal controls managed by the Cybersecurity Program.

Password requirements for Connect Platform, Enterprise Edition are dependent on the customer-configured authentication mechanism.

- If using the direct login authentication method: Customers can generate passwords that meet their specific requirements at the time of account creation.
- If using the federated login method: Customers can leverage the password requirements established by their IdP solution.

Audit logging

Connect Platform, Enterprise Edition captures events that occur within the application to help evaluate and document specific user tasks. The types of audit events captured in Connect Enterprise include data modifications, such as creation, update and/or deletion of data, who performed the action to alter the data and when the action occurred. Customers can view these events directly within Connect Platform, Enterprise Edition.

An internal log aggregation system stores logs generated for infrastructure and system performance. By default, storage of these logs occurs in a secure location with access limited to only authorized Thermo Fisher Scientific personnel.

Data storage and encryption

Encryption at rest

Thermo Fisher Scientific stores and encrypts customer-uploaded data to Connect Platform, Enterprise Edition using the Aurora PostgreSQL database, S3 buckets and Amazon Elastic Block Store (EBS). Full encryption of the PostgreSQL database, the S3 buckets and EBS is enabled using 256-bit Advanced Encryption Standard (AES-256).

Encryption in transit

Transmitted data being sent to and from the Connect Platform, Enterprise Edition communicates over a Secure Socket Layer (SSL) connection using Transport Layer Security (TLS) v1.3.

Web and mobile client access to platform data employs HTTPS, which requires using port 443 to protect external communications between the client and the platform via the internet.

Security certificates

Connect Platform, Enterprise Edition uses security certificates to support the encryption of data in transit, where the certificates automatically renew prior to expiration.

Cloud protection

Cloud compliance monitoring

Thermo Fisher Scientific has implemented a security control framework solution that monitors security controls implemented across various cloud accounts. Some examples of the controls it can enforce include network and firewall management, credential management, audit trail and log management and data protection configuration management.

Distributed denial-of-service (DDoS) protection

Connect Platform, Enterprise Edition leverages AWS to host its infrastructure where AWS provides distributed denial-of-service (DDoS) protection through their service, AWS Shield™. Also, Thermo Fisher Scientific leverages a third-party solution that deflects network-layer DDoS traffic and absorbs application DDoS traffic at the network edge.

Web application firewalls (WAFs)

Two comprehensive WAF technologies provide a strong defense against web-based attacks. The first layer of defense is a cloud-based WAF solution that guards against web-based attacks before they reach Connect Platform, Enterprise Edition. The second layer is a WAF solution deployed to the infrastructure supporting Connect Platform, Enterprise Edition which analyzes traffic at the web server level, provides visibility to quickly identify and mitigate threats, and prompts incident response.

Endpoint protection

Antivirus/anti-malware

The infrastructure supporting Connect Platform, Enterprise Edition leverages an antivirus solution to detect and prevent the execution of malicious software using signature-based indicators of compromise through its threat database. The solution provides both real-time and on-demand protection against file-based threats.

Extended detection and response

In addition to an antivirus solution, the infrastructure supporting Connect Platform, Enterprise Edition features an Extended Detection and Response (EDR) platform to detect, prevent and assist in responding to attacks proactively. Detection methods utilize predictive techniques, including algorithms, to examine code for potential threats. The EDR platform allows security analysts to perform rapid forensic examinations and deploy countermeasures to mitigate threats.

Secure product development lifecycle

Secure software development training

Software development training is available to the Connect Platform, Enterprise Edition Product Development team, which reinforces their knowledge of secure coding principles and allows them to review the latest development standards and guidelines.

Company-wide cybersecurity training

We believe cybersecurity is the responsibility of every Thermo Fisher Scientific employee, and regularly educate and share best practices with them to raise awareness of cybersecurity threats. Thermo Fisher Scientific accomplishes this through a security awareness training program, including regular exercises, periodic cyber-event simulations and annual attestation to our Technology Acceptable Use Policy.

Product security assessments

Products, instruments, software and devices undergo custom security assessments as part of the product development lifecycle. Customization is based on the components included with the solution and their complexity. The assessment may include technical review, focused testing of identified components and regulatory review, if applicable. The Connect Platform, Enterprise Edition Product Development team reviews, evaluates and prioritizes security assessment findings for remediation and acts on them based on criticality and a business risk management process.

Source code management

Connect Platform, Enterprise Edition source code is stored in a Thermo Fisher Scientific-approved version control solution that contains built-in redundancy to support data loss prevention. Continuous Integration/Continuous Deployment (CI/CD) is in use, automating the implementation and delivery of changes made to the code.

Artifact management

Software artifacts including, but not limited to, executables, images and libraries for Connect Platform, Enterprise Edition are stored and maintained in a Thermo Fisher Scientific-approved artifact management solution. This provides visibility and control on developed software builds, enabling the Connect Platform, Enterprise Edition team to identify dependencies with known vulnerabilities that are prioritized for remediation based on criticality and a business risk management process.

Static analysis

The Connect Platform, Enterprise Edition Product Development team utilizes a Thermo Fisher Scientific-approved static analysis tool to scan code repositories during each code commit. This tool helps identify potential security defects, maintain code quality and integrity and allow for the prompt review and prioritization of security alerts for remediation based on criticality and a business risk management process.

Peer code reviews

The Connect Platform, Enterprise Edition Product Development team conducts manual peer reviews of code before testing and deployment to help assess adherence to coding standards and design requirements. These reviews provide additional insight into the overall context and business logic of the code, complementing the information gathered from the static analysis tool.

Web application scanning/dynamic analysis

The Connect Platform, Enterprise Edition Product Development team uses a Thermo Fisher Scientific-approved dynamic analysis tool to evaluate web applications and APIs upon execution for potential code defects and/or vulnerabilities. Unlike static analysis where the code is reviewed prior to execution, dynamic analysis identifies defects during software runtime. APIs are scanned for security vulnerabilities and resilience to outside influence. The Product Development team reviews and prioritizes findings from the scans for remediation based on criticality and a business risk management process.

Architecture review

Thermo Fisher Scientific conducts a security architecture review on Connect Platform, Enterprise Edition to assess its security measures. Led by product security architects, this assessment involves understanding the components, interactions and connections within the product and evaluating potential security implications. The feedback and findings from the review are then prioritized by the Connect Platform, Enterprise Edition Product Development team for remediation based on criticality and a business risk management process.

Penetration testing

Thermo Fisher Scientific's Penetration Testing team tests core components of the Connect Platform Enterprise Edition against the Open Worldwide Application Security Project (OWASP) Top 10 list and OWASP API Top 10 list, representing some of the most critical security risks to web applications and APIs. The team is comprised of trained penetration testers who use technical and non-technical approaches to identify vulnerabilities during product development.

Vendor assessments

To evaluate risks from cybersecurity threats associated with the company's use of certain third-party technology providers, we have incorporated a risk-based assessment into the corporate information technology procurement process designed to assess the security risk of certain third parties providing new technology solutions to our environment. This process does not extend to all suppliers or situations but reflects a balanced approach to reduce risk and effectively manage resources.

Product security maintenance

Change control

Thermo Fisher Scientific follows a standardized change control process that requires various approvals based on logical segregation of duties prior to progression to a higher environment. The Connect Platform, Enterprise Edition Product Development team focuses on requirements traceability for feature enhancements and performs unit tests to assess functionality, where identified issues are addressed based on criticality and a business risk management process.

Vulnerability and patch management

The Connect Platform, Enterprise Edition Product Development team assesses security updates and system patches throughout the lifecycle of the product and deploys them to the impacted environments based on criticality and a business risk management process. Security updates and system patches for the infrastructure supporting Connect Platform, Enterprise Edition are planned for release on a quarterly cadence.

Thermo Fisher Scientific recommends that customers utilize our Reporting Security Issues form to report suspected or potential security issues.

Disaster recovery and business continuity

Non-production and productions system backups are maintained for at least 30 days and utilize a remote backup tool to maintain persistent data sources, such as S3 buckets, and Amazon Relational Database Service™ (Amazon RDS™) PostgreSQL database. The availability of services provided by Connect Platform, Enterprise Edition is a shared responsibility between AWS and Thermo Fisher Scientific. In the event of a large-scale system recovery of the cloud, AWS will be responsible for ensuring the services offered are resilient and available. Thermo Fisher Scientific will be responsible for the resiliency and availability of the services selected. This approach only applies to infrastructure supporting the Connect Platform, Enterprise Edition managed by Thermo Fisher Scientific, as business continuity plans can vary based on customer requirements.

Health monitoring

Connect Platform, Enterprise Edition infrastructure and application management follow documented standard operating procedures. Thermo Fisher Scientific monitors application and infrastructure health via health check tools, resource utilization and logging alarms.

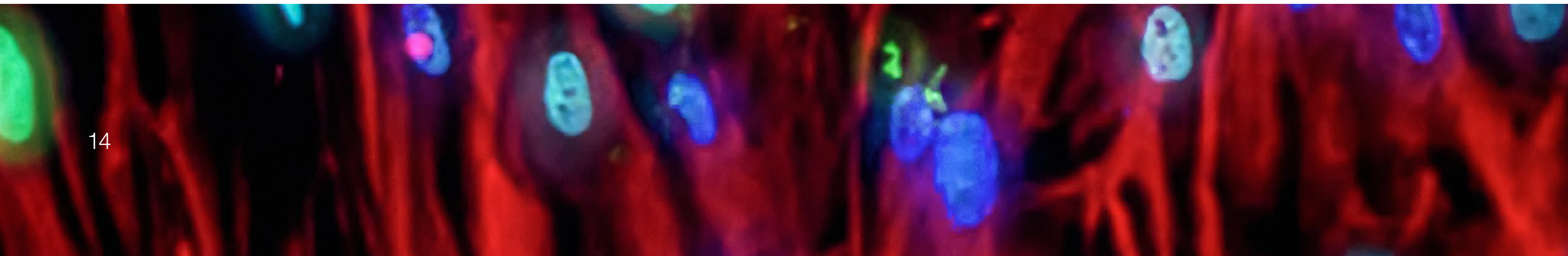
Scalability

The Connect Platform, Enterprise Edition is a single-tenant web-based application scaled to meet necessary demands for customers as infrastructure needs change. Service-level agreements are not guaranteed due to dependencies on AWS infrastructure and operations. Monitoring capabilities are leveraged to identify scaling needs.

Service handling

Application-specific support and global training serve as critical components to maintaining and supporting Connect Platform, Enterprise Edition. Thermo Fisher Scientific's experienced team of professionals use a global, follow-the-sun support approach for technical assistance and rapid escalation if critical issues should arise.

To request technical support for Connect Platform, Enterprise Edition, customers should place a support request through the Digital Science eService platform. Each customer receives an eService account as part of their support agreement with Thermo Fisher Scientific. For more information about Connect Platform, Enterprise Edition, documentation is accessible for customers by selecting the **Support** tab from within the platform.



Questions? To reach a member of our team to discuss the security of this product, please contact us at **product.security@thermofisher.com**