Product security information guide

Thermo Scientific™ myLibrary Enterprise | version 1.1 | December 2023

Document valid through December 31, 2024

Introduction

Thermo Fisher Scientific™ maintains a Cybersecurity Program, led by a dedicated Chief Information Security Officer (CISO), 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 procedures designed to help protect myLibrary Enterprise Version 1.1 against intrusion or data compromise. This document describes the various standards, controls, 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 ensure it contains current, accurate information. This guide expires on **December 31, 2024.** Please reach out to your account representative to obtain 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”). 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 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 maintains a Cybersecurity Program that includes technical, administrative and physical safeguards designed to detect vulnerabilities and address potential threats. Controls include web application firewalls (WAFs), intrusion detection systems (IDSs), endpoint detection and response solutions, multifactor authentication (MFA) and email protection. Thermo Fisher Scientific's Cybersecurity Program maintains International Organization for Standards (ISO) 27001:2013 certification.

Critical asset protection

Thermo Fisher Scientific has a dedicated Critical Asset Protection team which helps protect the company's critical digital assets and intellectual property using enhanced monitoring tools and digital forensic techniques.

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.

Incident management

Thermo Fisher Scientific maintains a process for managing potential 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 immediate threat mitigation and remediation. Once mitigation occurs, the team performs root cause analysis for continuous improvement and to reduce opportunities for recurrence.

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 Thermo Scientific myLibrary Enterprise application is a harmonized library platform that enables the creation of curated MS2 and MSn mass spectral libraries. The application lets customers build, store, collaborate, manage and search customer-specific MS spectral libraries across the organization. It facilitates a shared centralized spectral library capability to allow multiple users and sites to collaborate and connect research activities to routine work.

MyLibrary Enterprise is a single-tenant Amazon™ Web Services™ (AWS) cloud instance hosted on the Thermo Fisher Scientific Ardia Platform. Each myLibrary Enterprise instance is customer specific. The Ardia Platform lets customers configure and connect to their organization's identity provider (IdP) and assign user access. The application uses Role Based Access Control (RBAC), limiting permissions for different user types. An IT administrator assigns roles that provide access to specific features in myLibrary Enterprise. When users log in, the myLibrary Enterprise navigation pane displays only those features for which they have permission to access. In addition, myLibrary Enterprise maintains a change log that is displayed in the notification pane.

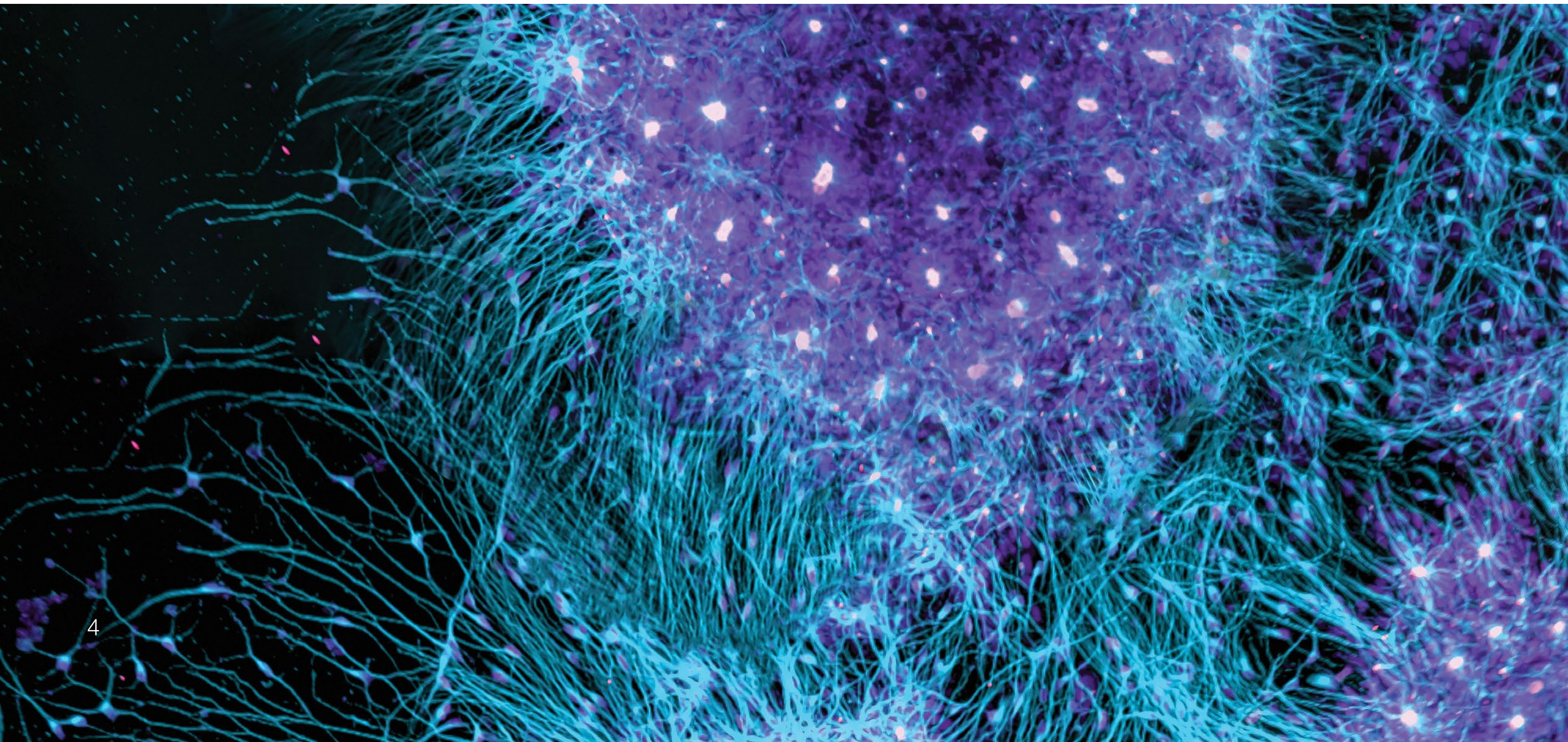
System compatibility

MyLibrary Enterprise is supported on the following operating systems and web browsers:

- Operating system
  - Microsoft Windows™ 10 Enterprise Long-Term Servicing Channel (LTSC) 2016
- Web browsers
  - Google™ Chrome™ browser (Version 81.0 or above)
  - Mozilla™ Firefox™ browser (Version 76.0 or above)

Regulatory standards

Thermo Fisher Scientific maintains a Quality Management System (QMS) aligned with ISO 9001 standards that encompasses policies and procedures including, but not limited to, disaster recovery, data backup and recovery, business continuity, data security and change management procedures.



MyLibrary Enterprise architecture diagram

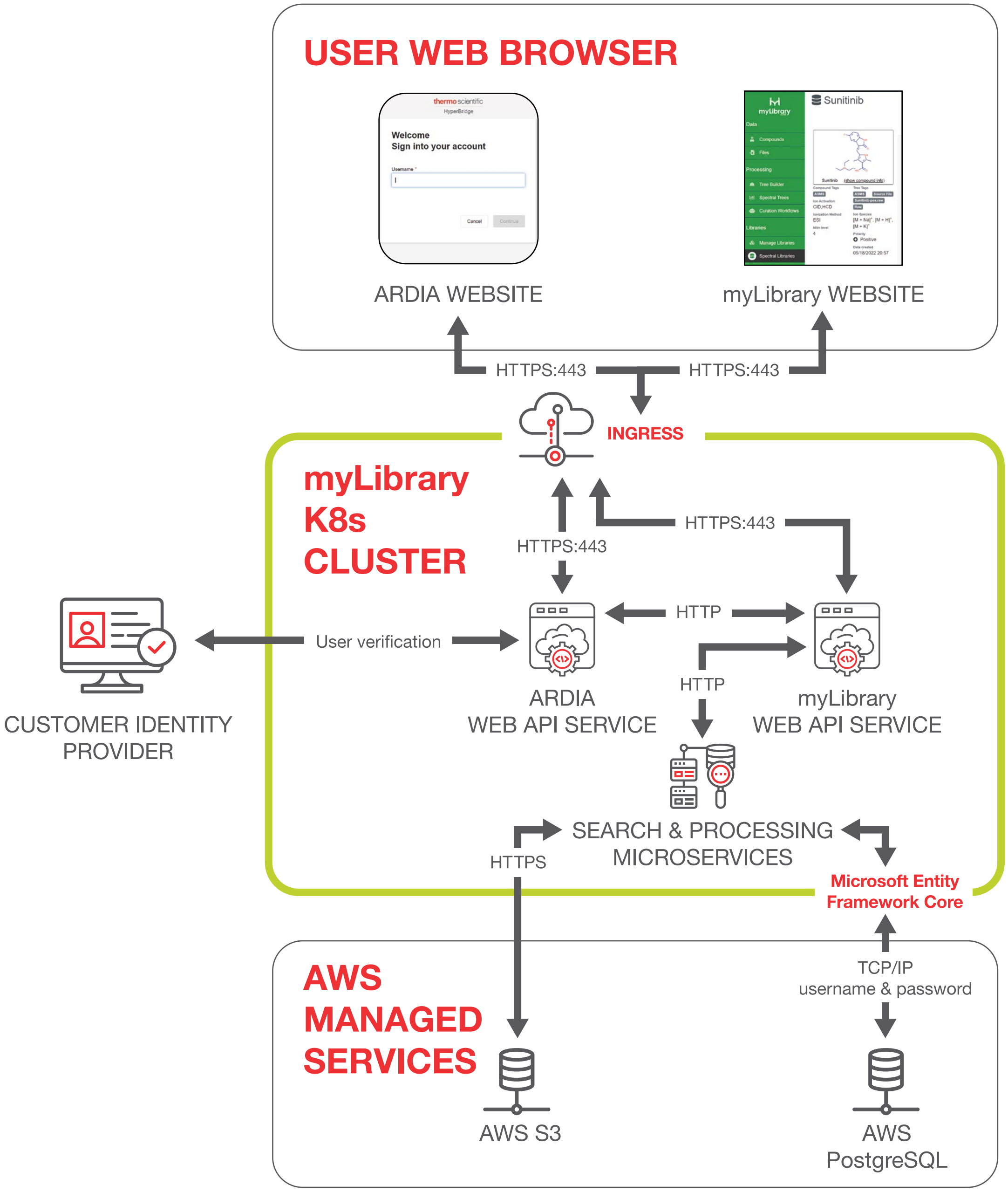


Figure 1: MyLibrary Enterprise architecture

MyLibrary Enterprise component glossary

MyLibrary Enterprise features the following components.

Component term	Definition
MyLibrary Enterprise website/application	MyLibrary Enterprise's browser-based user interface (UI) allows users to create, search and browse the spectral library.
Ardia Platform website	The Ardia Platform's identity server UI allows users to access myLibrary Enterprise according to roles and permissions assigned by the customer's IdP.
Ingress	Component that routes the client's request to the relevant internal service. Network traffic to the cluster must pass through Ingress using Hypertext Transfer Protocol Secure (HTTPS).
Ardia web application programming interface (API) service	The primary component for user access management. The Ardia Platform web API service allows for the assignment of roles and groups within myLibrary Enterprise based on the IdP configuration.
MyLibrary Enterprise web API service	The core internal service used within the Kubernetes™ cluster (platform for managing workloads and systems). It directs user requests to the appropriate microservice to perform a desired action in the spectral library.
Search and processing microservices	A collection of services within the Kubernetes cluster to perform actions in the spectral library (such as the search service, metadata search service, indexing service or tree builder service). All communication within the cluster remains internal and uses HTTP or the gRPC remote procedure call protocol framework.
AWS Simple Storage Service (S3)™	An AWS-managed service used for file storage. Within myLibrary Enterprise, AWS S3 functions as a temporary storage location to transfer files between internal services. Files are imported into AWS S3 through HTTPS.
AWS PostgreSQL™ database	An AWS-managed service used for the storage of processed data, such as spectral data or compound data. Users authenticate via username and password.

Table 1: MyLibrary Enterprise components

System access controls

Authentication

The customer's IdP administers authentication through myLibrary Enterprise. Customers leverage their organization's IdP to validate user access to the application when an administrator enters user email addresses into the Ardia Platform user interface. Once validated against the IdP, roles and group assignments can be associated to an email address, which allows for the assignment of additional permissions.

Administrative access to Thermo Fisher Scientific's AWS console requires MFA. Thermo Fisher Scientific limits access to application servers and supporting infrastructure to authorized personnel only.

Authorization

MyLibrary Enterprise 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 be configured using the principle of least privilege providing only the required system access needed to manage myLibrary Enterprise tasks.

System hardening practices

The myLibrary Enterprise Product Development team has implemented system hardening, a security function that helps prevent potential attacks and reduce risk. These security hardening practices include:

- Disabling unnecessary ports and protocols within myLibrary Enterprise; and
- Leveraging "golden images," or standard Microsoft Windows images that include additional security controls (including deployment of antivirus tools), on the infrastructure supporting myLibrary Enterprise.

Firewall/network controls

Thermo Fisher Scientific manages the security of the myLibrary Enterprise network using access control lists (ACLs) to restrict network access in conjunction with using various AWS services, such as virtual private clouds (VPCs) and security groups, to separate customer environments. Only myLibrary Enterprise's externally facing services can be accessed via the internet.

In addition to the various security measures limiting network exposure, myLibrary Enterprise also utilizes an Ingress component within the application cluster to appropriately route the client's request to a relevant service. Network traffic to the cluster must pass through the ingress using HTTPS.

Password management

For access to internal systems, Thermo Fisher Scientific's Information Security Password Policy mandates all colleagues to generate complex passwords, enforced by internal controls managed by the Cybersecurity Program.

For myLibrary Enterprise, customers establish password requirements and complexities (enforced by the IdP) to allow for compliance with business policies and local regulatory requirements.

Logging

MyLibrary Enterprise logs multiple activities, including system events and code exceptions, to evaluate system performance. Argo™ CD, a GitOps continuous delivery tool for Kubernetes, accesses logs within the myLibrary Enterprise application cluster. GitOps uses a Git repository as the single source of truth for infrastructure definitions. Git is an open-source version control system that tracks changes in code and files.

Data storage and encryption

Data storage

Thermo Fisher Scientific stores customer-uploaded data, such as data used for library creation, in AWS S3 buckets and in an AWS Relational Database Service™ (RDS) PostgreSQL database. The information stored within the application infrastructure is used to build and curate the spectral library as well as track file actions within the library. The query for spectral data, which includes the spectral query itself as well as that of the user running the query, is not stored within myLibrary Enterprise.

Encryption at rest

Thermo Fisher Scientific encrypts myLibrary Enterprise customer-uploaded data in AWS S3 buckets and in the RDS PostgreSQL database. The S3 buckets leverage server-side encryption using 256-bit Advanced Encryption Standard (AES-256). Full encryption of the PostgreSQL database is enabled using AES-256.

Encryption in transit

Transmitted data being sent to and from myLibrary Enterprise communicates over a Secure Socket Layer (SSL) connection using Transport Layer Security (TLS) v1.3, and TLS v1.2 for browsers that do not currently support TLS v1.3. Web client access to myLibrary Enterprise application data employs HTTPS, which requires using port 443, to protect external communications between the client and the application via the internet.

MyLibrary Enterprise uses security certificates to support the encryption of data in transit, where the certificates are automatically renewed prior to expiration.

Cloud protection

Cloud compliance monitoring

Thermo Fisher Scientific has implemented a security control framework solution that simultaneously monitors and enforces thousands of controls in hundreds of 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

MyLibrary Enterprise leverages AWS to host its infrastructure, where AWS provides DDoS protection through their AWS Shield™ service. In addition to AWS Shield, myLibrary Enterprise also leverages a Thermo Fisher Scientific-approved 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 defense against web-based attacks. The first layer of defense, a cloud-based WAF solution, guards against web-based attacks before they reach myLibrary Enterprise.

The second layer, a WAF solution deployed to infrastructure supporting myLibrary Enterprise, analyzes traffic at the web server level, provides visibility to help identify and mitigate threats, and prompts incident response.

Endpoint protection

Antivirus/anti-malware

MyLibrary Enterprise 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, myLibrary Enterprise 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 myLibrary Enterprise Product Development team, which reinforces their knowledge of secure coding principles and allows them to review the latest development standards and guidelines. Additionally, Thermo Fisher Scientific colleagues receive regular updates about the latest cybersecurity trends through the corporate Cybersecurity Program. These training activities help sustain and strengthen our "security first" mindset.

Product security assessments

Products, instruments and devices undergo custom security assessments as part of the product development lifecycle. Customization is based upon the components included with the solution and the complexity of these component interactions. The assessment may include technical review, focused testing of identified components and regulatory review, if applicable. The myLibrary Enterprise Product Development team reviews, evaluates and prioritizes security assessment findings for remediation, and acts on them based on criticality.

Source code management

MyLibrary Enterprise source code is stored in a Thermo Fisher Scientific-approved version control solution that is internally facing and contains built-in redundancy to support data loss prevention. Continuous Integration/Continuous Deployment (CI/CD) is used to automate the implementation and delivery of changes made to the code.

Artifact management

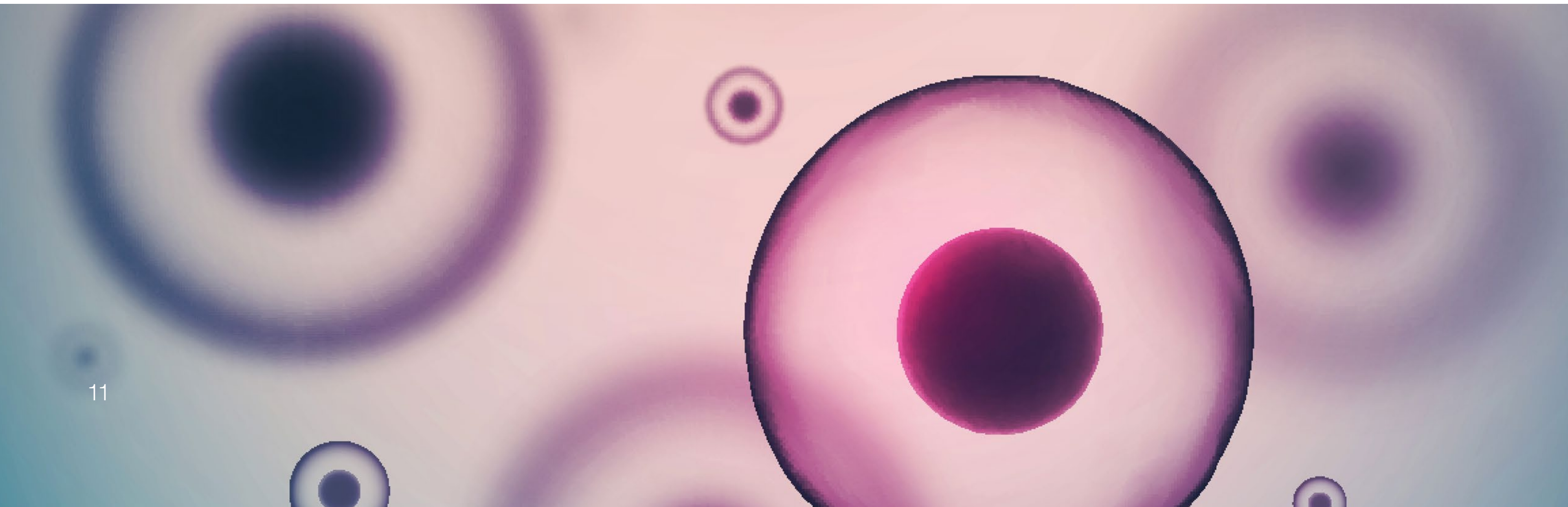
Software artifacts including, but not limited to, executables, images and libraries for the myLibrary Enterprise application are stored and maintained in a Thermo Fisher Scientific-approved artifact management solution that provides visibility and control on developed software builds. This allows for dependencies with known vulnerabilities to be identified and addressed.

Static analysis

The myLibrary Enterprise Product Development team uses a Thermo Fisher Scientific-approved and managed static analysis tool that scans code repositories each time code is committed to the system to identify potential security defects and ensures code quality and integrity through increased speed of code reviews. The Product Development team reviews and prioritizes security alerts for remediation based on criticality.

Peer code reviews

The myLibrary Enterprise Product Development team conducts manual peer reviews of code before testing and deployment. Manual code reviews provide benefit by accounting for the overall context and business logic in which the code was developed, which supplements information provided from the static analysis tool.



Web application scanning/dynamic analysis

The myLibrary Enterprise 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. The Product Development team reviews and prioritizes findings from the scans for remediation based on criticality.

The myLibrary Enterprise Product Development team scans APIs for security vulnerabilities and resilience to outside influence prior to product release.

Architecture review

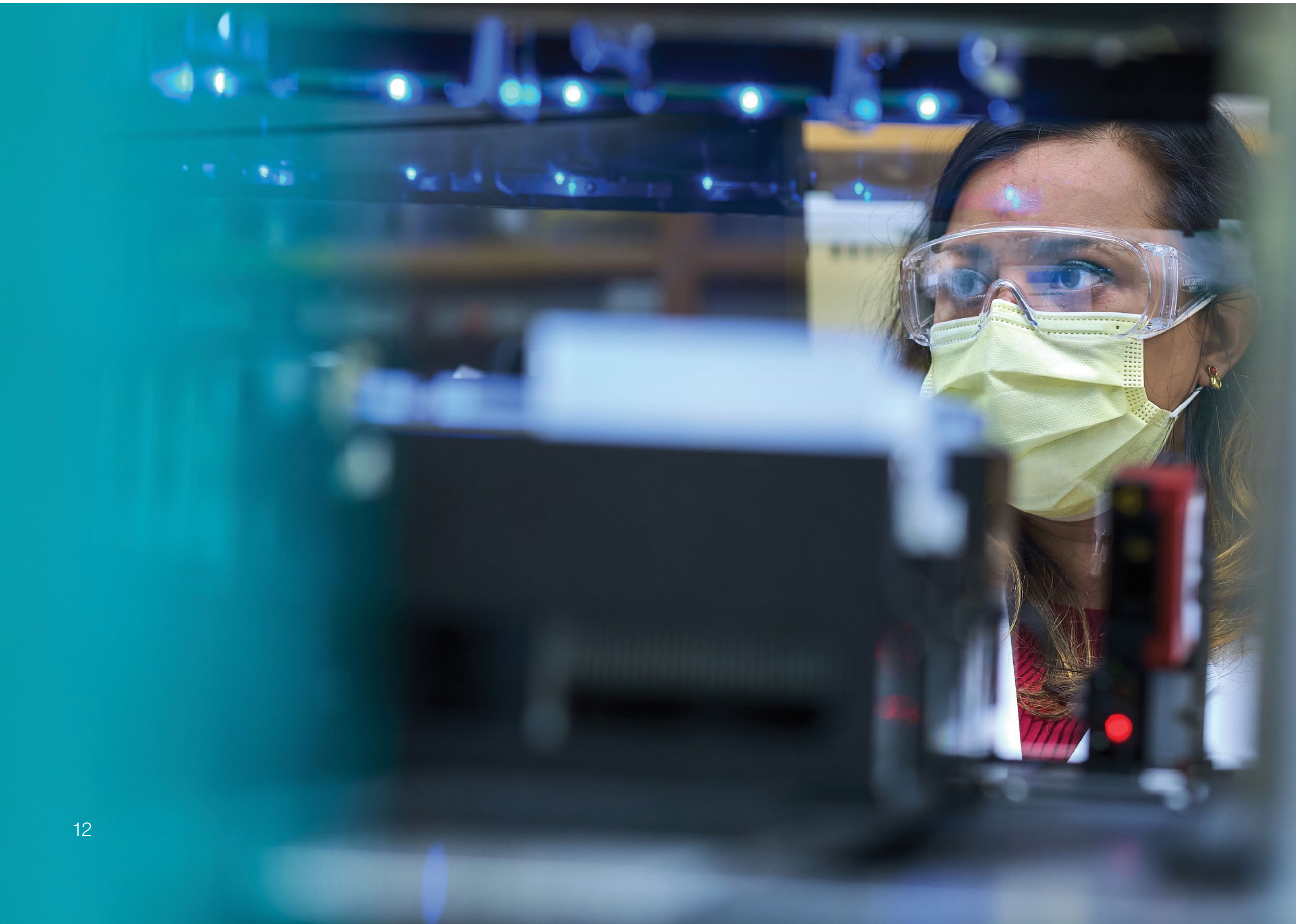
Thermo Fisher Scientific performs a security architecture review on myLibrary Enterprise as part of the product security assessment. Led by professional product security architects, the assessment consists of understanding the major components involved in myLibrary Enterprise, their interactions and connections to each other, and determining how security can be impacted based on the technology and configuration in use. Feedback and findings are considered and prioritized for remediation by the myLibrary Enterprise product development team based on criticality.

Penetration testing

Thermo Fisher Scientific's Penetration Testing team tests core myLibrary Enterprise components against the Open Worldwide Application Security Project (OWASP) Top 10 list. The team, comprised of trained penetration testers, use technical and non-technical approaches to identify vulnerabilities during product development.

Vendor assessments

Our Cybersecurity Program performs security assessments of third-party vendors and service providers to evaluate and approve solutions for use within Thermo Fisher Scientific's environment. Assessments of third-party vendors and service providers help to ensure that new and existing vulnerabilities and attack vectors are not introduced into Thermo Fisher Scientific's environment.



Product security maintenance

Change control

Thermo Fisher Scientific follows a standardized change control process that requires supervisor, application owner and Quality Assurance governance approvals. Releases are security-scanned for application and infrastructure vulnerabilities. Prior to progression to a higher environment, testing from the product development team is conducted and discovered issues are addressed.

Vulnerability and patch management

The myLibrary Enterprise Product Development team tests and validates security updates and system patches throughout the lifecycle of the product and deploys them to the impacted environments based on criticality.

Updates to the myLibrary Enterprise infrastructure occur via a QuickFix, which is a service pack, or the release of a new application version. The team evaluates and schedules updates containing fixes to critical and high-priority vulnerabilities for remediation.

Disaster recovery and business continuity

Daily system data backups of non-production and production environments are stored for at least 7 days. Multiple copies of data are maintained, utilizing AWS S3 buckets and the AWS RDS PostgreSQL database.

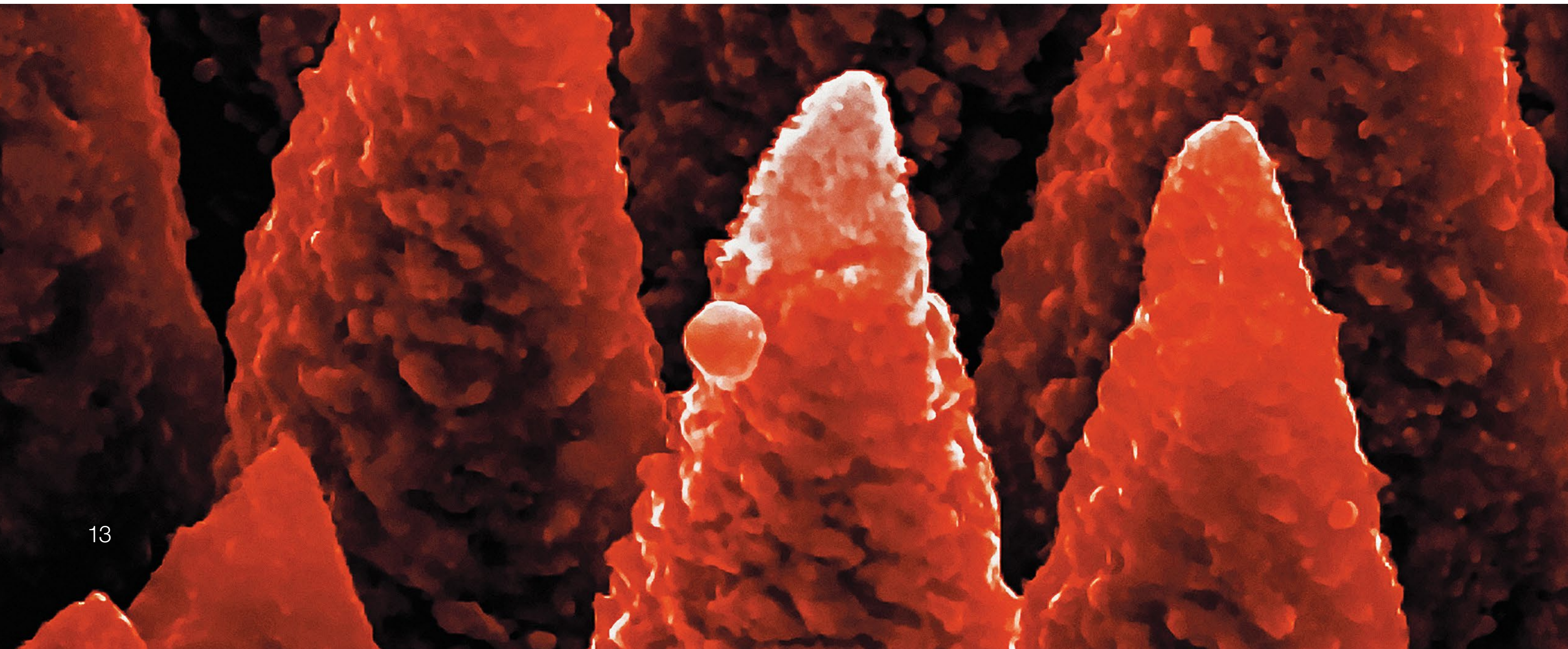
The availability of AWS services is a shared responsibility between AWS and Thermo Fisher Scientific. In the event of a large-scale system recovery of the cloud, AWS is responsible for ensuring the services offered within the platform are resilient and available. Thermo Fisher Scientific is responsible for the resiliency and availability of the services used to manage the myLibrary Enterprise infrastructure.

Health monitoring

MyLibrary Enterprise infrastructure and application management follow documented standard operating procedures. Thermo Fisher Scientific also monitors application and infrastructure activity via Argo CD, in conjunction with resource utilization and logging alarms to assess the performance of each individual component in the application.

Service handling

Application-specific support and global training serve as critical components to deploying and supporting the myLibrary Enterprise application. Customers can request support 24/7 by contacting the myLibrary Enterprise support team to raise any issues or concerns pertaining to the application. A member of the support team will reach out and provide a response during normal business hours.



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