Product security information guide

Thermo Scientific™ myLibrary Enterprise | version 1.1 | December 2024

Document valid through December 31, 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 procedures designed to help protect the Thermo Scientific™ myLibrary Enterprise version 1.1 application 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, 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.

The 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 myLibrary Enterprise application assets.

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 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 myLibrary Enterprise application is a harmonized library platform that enables the creation of curated MS2 and MSn spectral libraries. The application lets you build, store, collaborate, manage and search your own private 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.

The myLibrary application 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 utilizes role-based access control (RBAC), limiting permissions for different user types. An IT administrator assigns roles that provide access to specific features in the myLibrary Enterprise application. When users log in, the myLibrary Enterprise application navigation pane displays only those features for which they have permission to access. In addition, the myLibrary Enterprise application maintains a change log that is displayed in the notification pane.

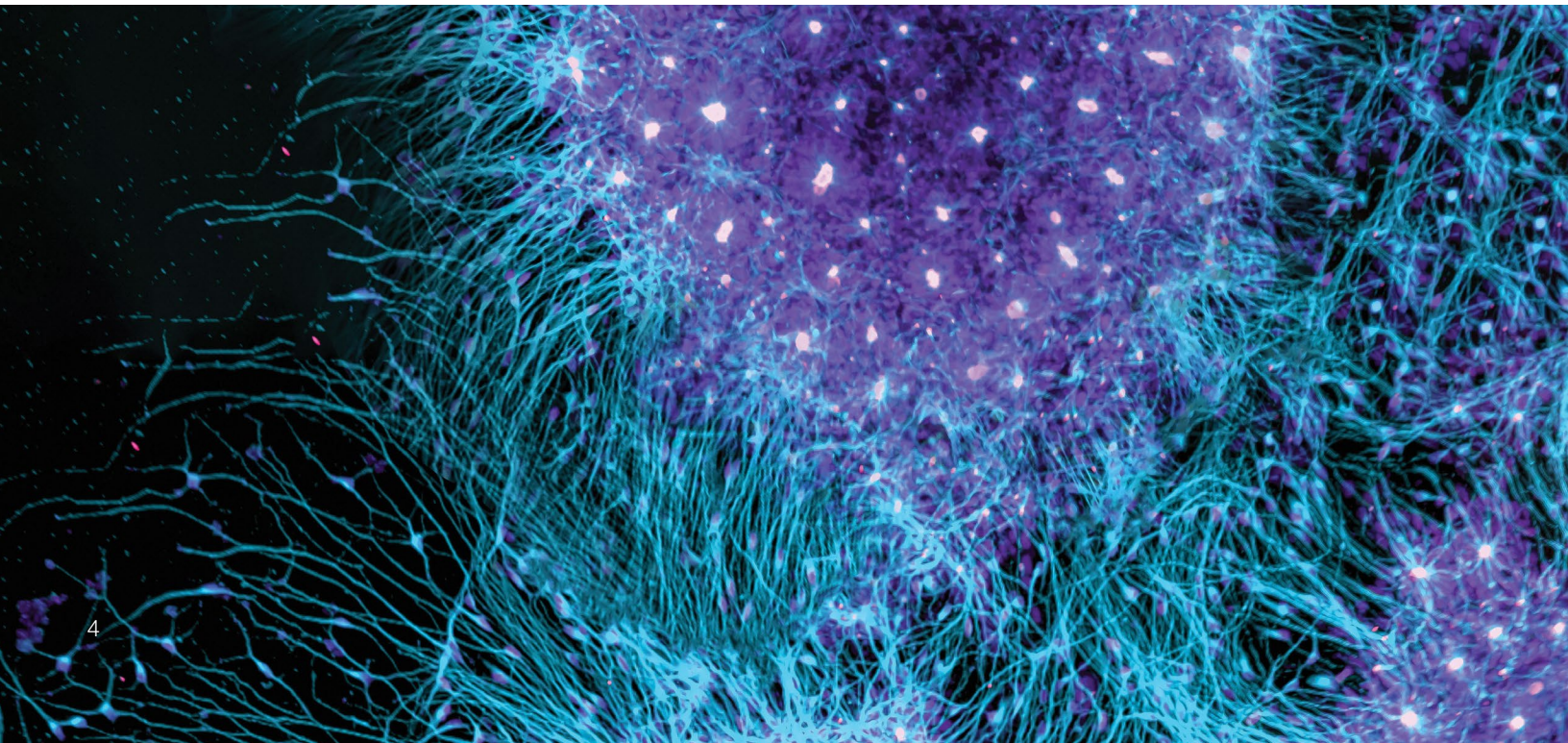
System compatibility

The myLibrary Enterprise application is compatible with the following web browsers:

- Web browsers
  - Google™ Chrome™ browser (Version 81.0 or above)
  - Mozilla™ Firefox™ browser (Version 76.0 or above)

Relevant security certifications and/or regulatory standards

The myLibrary Enterprise application is developed under a Quality Management System certified to International Organization for Standardization (ISO) 9001:2015 standards that encompass 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

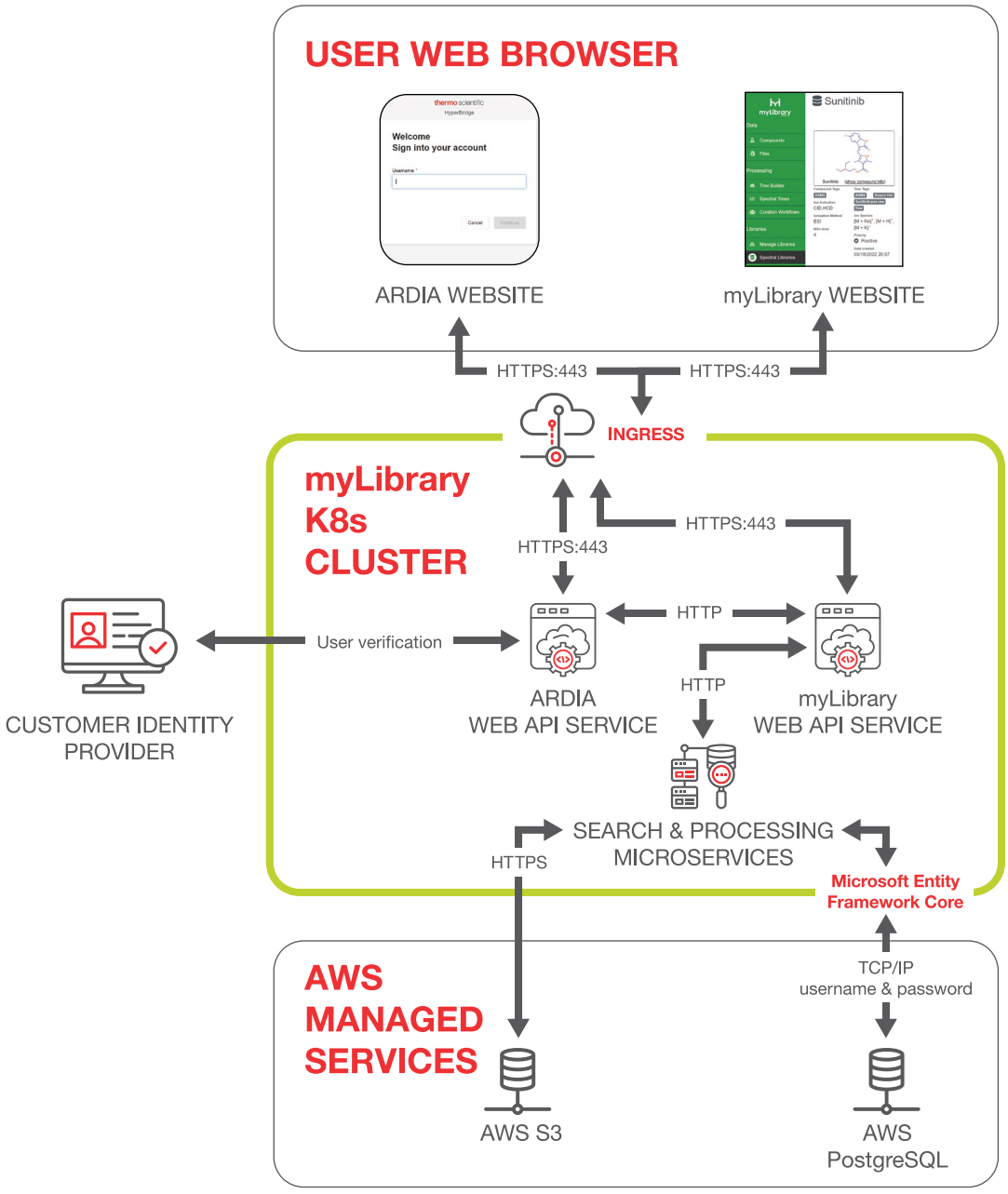


Figure 1: MyLibrary Enterprise architecture

Component glossary

The myLibrary Enterprise application features the following components.

Component term	Definition
MyLibrary Enterprise website/application	The myLibrary Enterprise application'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 the myLibrary Enterprise application 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 web API service allows for the assignment of roles and groups within the myLibrary Enterprise application 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.
Amazon Simple Storage Service™ (Amazon S3™)	An AWS-managed service used for file storage. Within the myLibrary Enterprise application, Amazon S3 functions as a temporary storage location to transfer files between internal services. Files are imported into Amazon 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 the myLibrary Enterprise application. 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 application servers and infrastructure, including access to the AWS console that manages the myLibrary Enterprise application, requires multifactor authentication (MFA). Thermo Fisher Scientific limits access to application servers and supporting infrastructure to authorized personnel only.

Authorization

The myLibrary Enterprise application leverages 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 Software 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 the myLibrary Enterprise application; and
- Leveraging "golden images," or standard Microsoft™ Windows™ images that include additional security controls, such as the deployment of antivirus tools, on the infrastructure supporting the myLibrary Enterprise application.

Firewall/network controls

Thermo Fisher Scientific manages the security of the myLibrary Enterprise application 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 externally facing services of the myLibrary Enterprise application are accessible via the internet.

In addition to the various security measures limiting network exposure, the myLibrary Enterprise application 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

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.

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

Logging

The myLibrary Enterprise application logs various 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, an open-source version control system, tracks changes in code and files.

Data storage and encryption methods

Data storage

Thermo Fisher Scientific stores customer-uploaded data, such as data used for library creation, in Amazon S3 buckets and in an Amazon Relational Database Service™ (Amazon 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 the myLibrary Enterprise application.

Encryption at rest

Thermo Fisher Scientific encrypts myLibrary Enterprise customer-uploaded data in Amazon S3 buckets and in the Amazon RDS PostgreSQL database. The Amazon 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 the myLibrary Enterprise application 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.

The myLibrary Enterprise application 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 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

The myLibrary Enterprise application leverages AWS to host its infrastructure, where AWS provides DDoS protection through the AWS Shield™ service. 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 the myLibrary Enterprise application.

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

Endpoint protection

Antivirus/anti-malware

The infrastructure supporting the myLibrary Enterprise application 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.

Endpoint detection and response

In addition to an antivirus solution, the infrastructure supporting the myLibrary Enterprise application features an endpoint 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 Software 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 upon 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 myLibrary Enterprise Software 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

The myLibrary Enterprise application 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 the myLibrary Enterprise application are stored and maintained in a Thermo Fisher Scientific-approved artifact management solution. This provides visibility and control on developed software builds, enabling the MyLibrary Enterprise Software Development team to identify dependencies with known vulnerabilities that are prioritized for remediation based on criticality and a business risk management process.

Static analysis

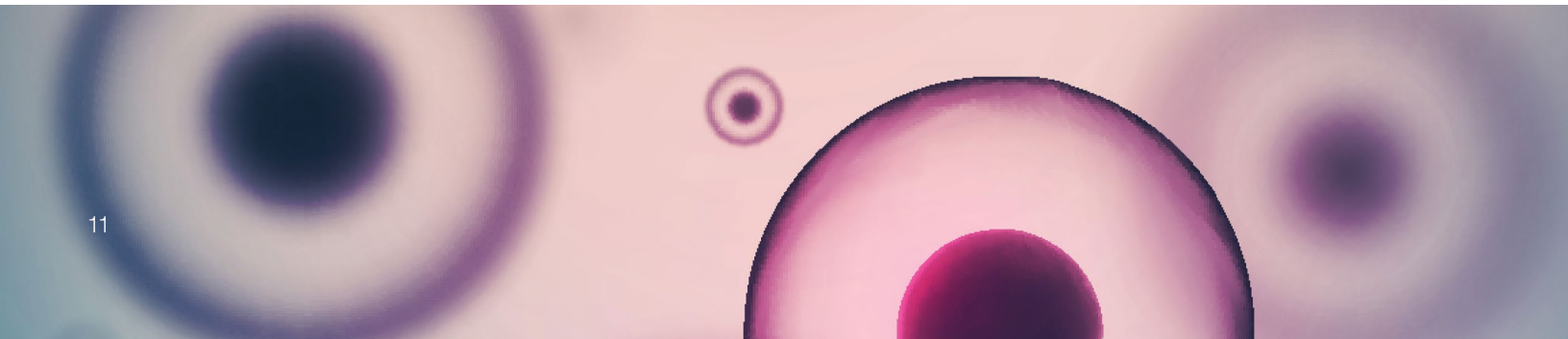
The myLibrary Enterprise Software Development team utilizes a Thermo Fisher Scientific-approved static analysis tool to scan code repositories during each code commit. This tool helps identify potential security defects, maintain code quality and integrity and allow for the prompt review and prioritization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

Peer code reviews

The myLibrary Enterprise Software 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 myLibrary Enterprise Software 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 Software Development team reviews and prioritizes findings from the scans for remediation based on criticality and a business risk management process.

Architecture review

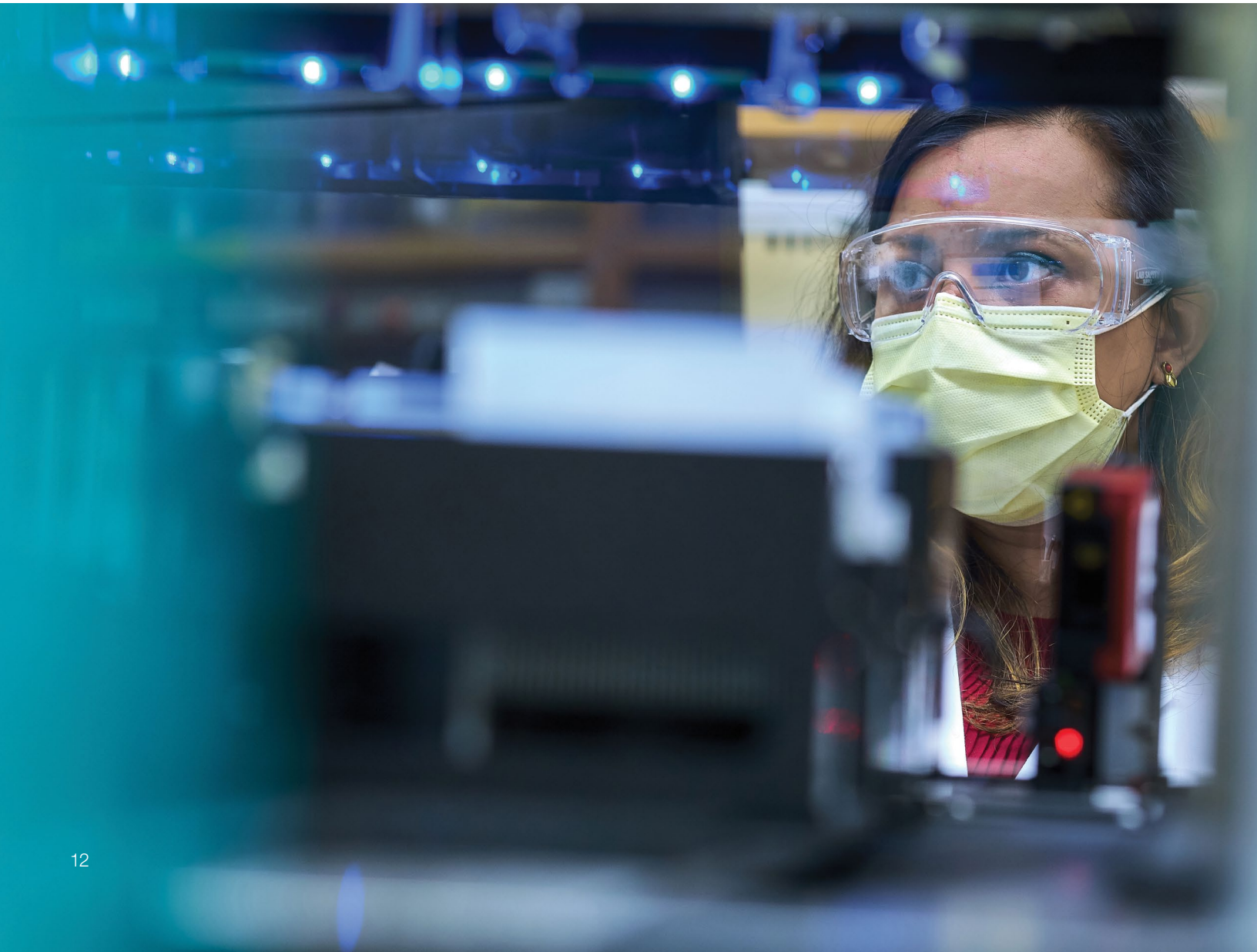
Thermo Fisher Scientific conducts a security architecture review on the myLibrary Enterprise application to assess its security measures. Led by product security architects, the assessment involves understanding the components, interactions and connections within the product and evaluating potential security implications. The feedback and findings from the review are then prioritized by the myLibrary Enterprise Software 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 myLibrary Enterprise application against the Open Worldwide Application Security Project (OWASP) Top 10 and API Top 10 lists, 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 myLibrary Enterprise Software 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 myLibrary Enterprise Software 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.

Updates to the myLibrary Enterprise application infrastructure occur via a QuickFix, which is a service pack, or the release of a new application version. Thermo Fisher Scientific recommends that customers utilize our Reporting Security Issues form to report suspected or potential security issues.

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 Amazon S3 buckets and the Amazon RDS PostgreSQL database.

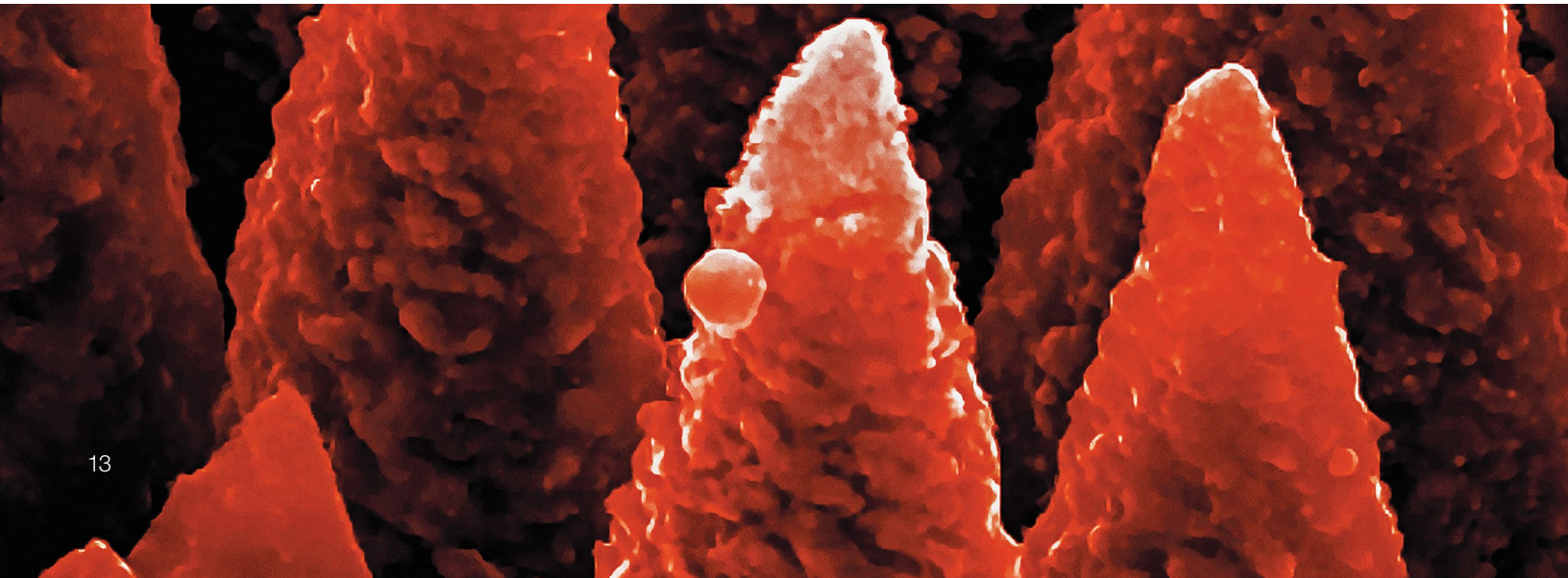
The availability of services provided by the myLibrary Enterprise application is a shared responsibility between AWS and Thermo Fisher Scientific. In the event of a large-scale system recovery of the cloud, AWS will be responsible for ensuring the services offered are resilient and available. Thermo Fisher Scientific will be responsible for the resiliency and availability of the services selected.

Health monitoring

The 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

B51003230 Rev B