



Product security information guide

Thermo Scientific LabLink 360 Quality Assurance software | August 2026

Document valid through August 15, 2027

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 supports a continuously improving security program model that is designed to focus on reducing risk, defending against threats, maintaining data privacy and protecting our company's confidential information, including trade secrets and intellectual property.

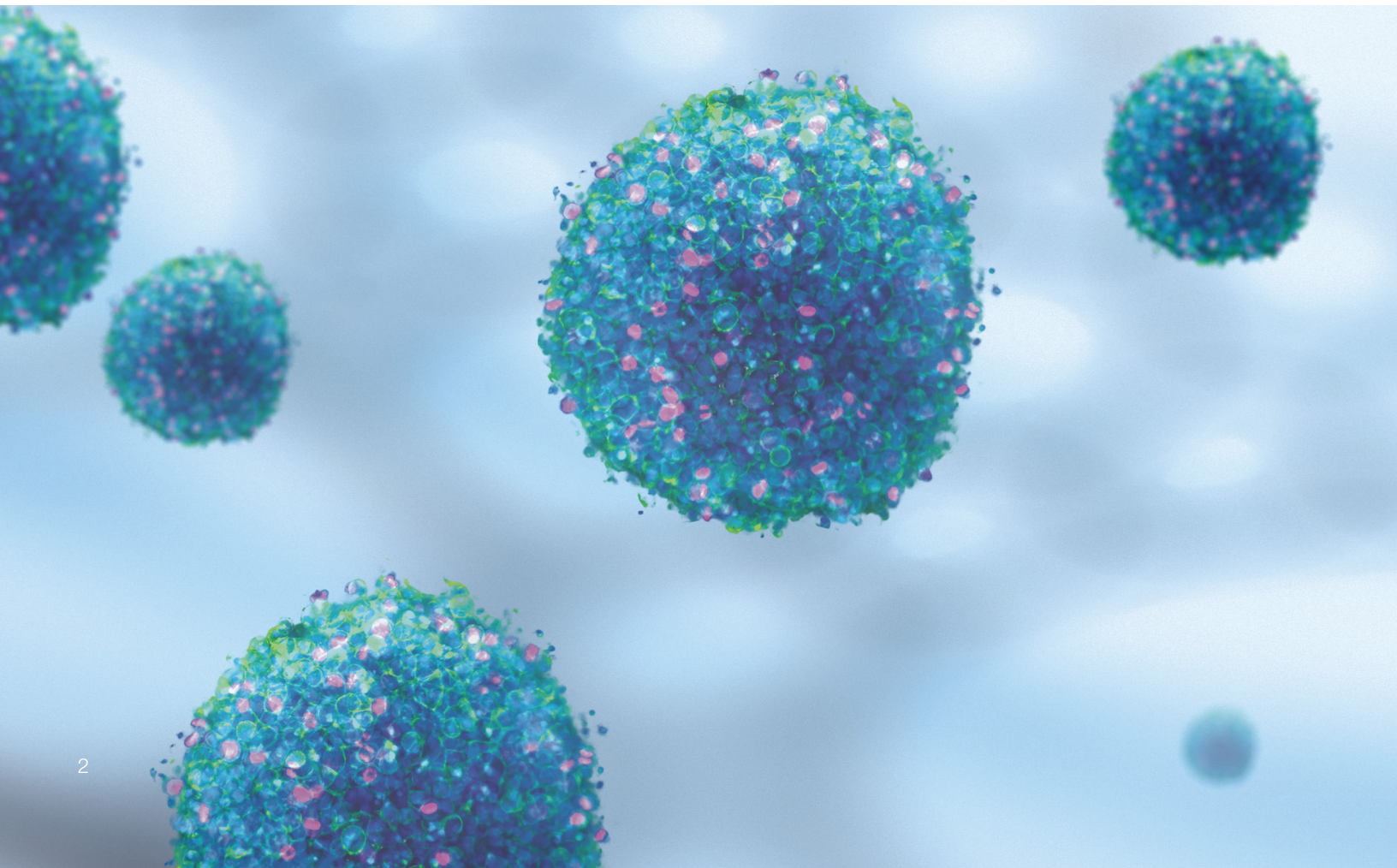
About this guide

Thermo Fisher has implemented safeguards and protections designed to help protect the Thermo Scientific™ LabLink™ 360 Quality Assurance software against intrusion or data compromise. This document describes the various standards, controls and data security approaches and business practices that Thermo Fisher uses in this effort.

Due to the ever-changing cyber landscape, Thermo Fisher updates this product security information guide annually to maintain current and accurate information. This guide expires on August 15, 2027. Contact your account representative or visit our [information security website](#) 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, or Thermo Fisher subsidiaries or affiliates (collectively, “Thermo Fisher Scientific” and/or “Thermo Fisher”). Additionally, this product security information guide does not create an independent contract or agreement between any customer and Thermo Fisher. Thermo Fisher 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 or reduce 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's Cybersecurity Program employs technical, administrative and physical safeguards designed to detect vulnerabilities and address potential threats.

Thermo Fisher's Cybersecurity Program maintains an [International Organization for Standardization/International Electrotechnical Commission \(ISO/IEC\) 27001:2022 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 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 employs a

strategy using numerous technologies, processes and controls to manage cybersecurity risk.

Digital forensics and incident response

The Thermo Fisher 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's enterprise network. The capabilities of the Digital Forensics and Incident Response Program extend to monitoring the infrastructure supporting the LabLink 360 Quality Assurance software.

Incident management

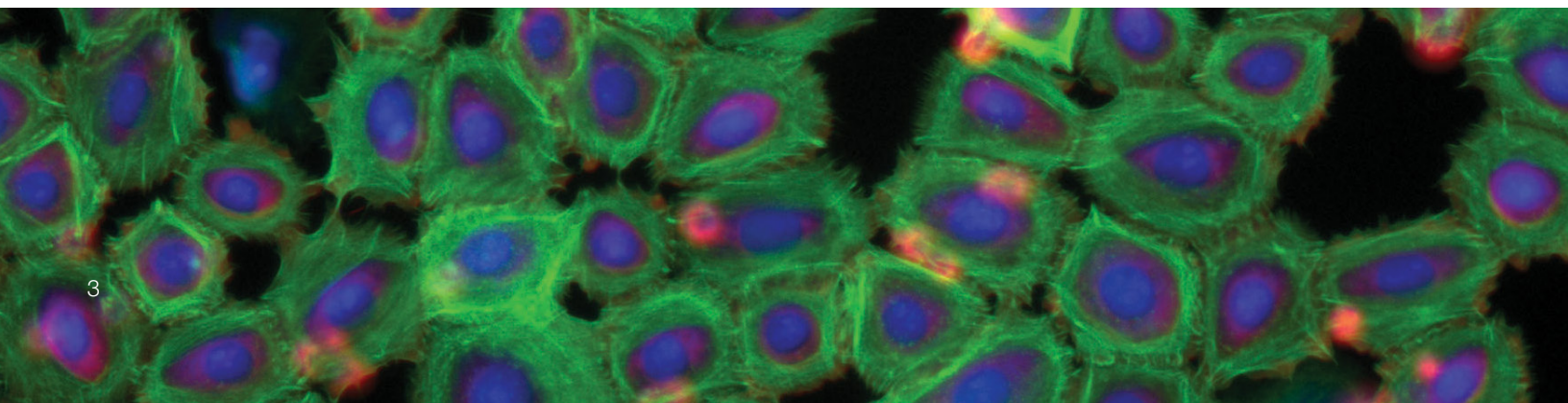
Thermo Fisher maintains a process for managing cybersecurity incidents according to our Incident Response Plan.

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



Product overview

The Thermo Scientific™ LabLink™ 360 Quality Assurance software is a cloud-based quality control (QC) and quality assurance (QA) software platform that is designed to help clinical laboratories manage, monitor and optimize their QC processes. The primary purpose of the software is to automate the collection and analysis of QC data, reducing manual entry and minimizing transcription errors.

The platform provides real-time visibility into instrument and method performance through advanced statistical tools such as:

- Levey-Jennings (LJ) charts (graphical tools for monitoring lab QC over time);
- Westgard and RiliBÄK rules (statistical control rules for lab QC); and
- Sigma metrics (which define the control boundaries on LJ charts and are used in Westgard rules to trigger alerts or rejections).

The platform also enables laboratories to compare their QC results with anonymized peer groups, helping users quickly identify trends, shifts or systemic issues. By centralizing QC data,

supporting regulatory documentation and enabling multi-site oversight, LabLink 360 Quality Assurance software is designed to help laboratories improve quality management and operational efficiency.

System compatibility

The LabLink 360 Quality Assurance software is compatible with the following web browsers:

- Google Chrome™
- Microsoft Edge™
- Mozilla™ Firefox™
- Apple™ Safari™

Security certifications and/or regulatory standards

LabLink 360 Quality Assurance software is developed in accordance with [ISO 15189:2022 Medical laboratories – Requirements for quality and competence](#).

Note: Please refer to the [ISO](#) website for additional information about the ISO 15189:2022 requirements.



Architecture diagram

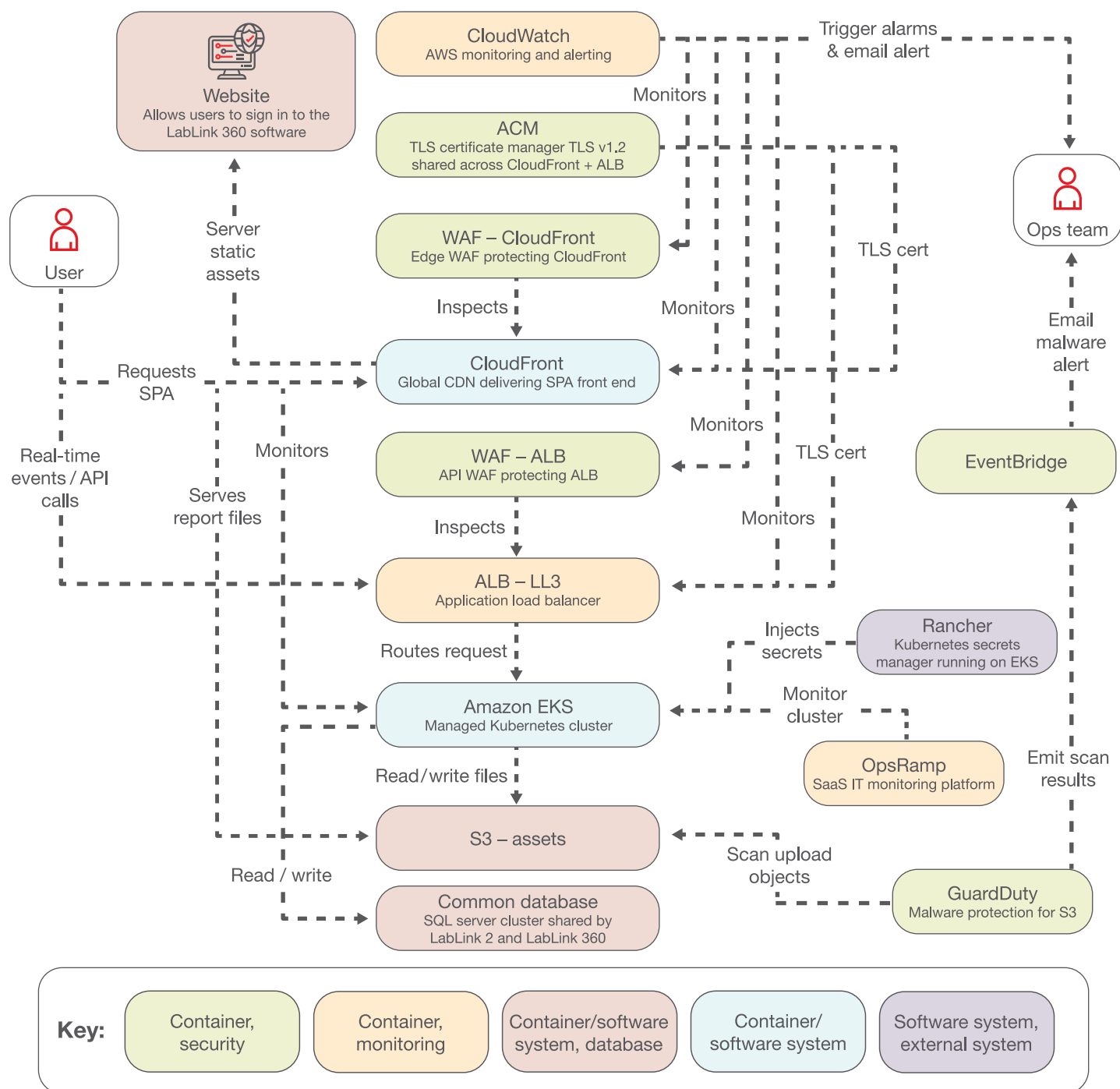


Figure 1: LabLink 360 Quality Assurance software system architecture diagram

Component glossary

Component	Description
Amazon EKS™ Cloud	An Amazon Web Services™ (AWS™)-managed Kubernetes™ service used to deploy, manage and scale containerized application services that support the LabLink 360 web application.
Amazon Virtual Private Cloud™ (Amazon VPC™)	An AWS-managed virtual network that isolates LabLink 360 cloud resources and enables secure communication between application components and external users.
Amazon Simple Notification Service™ (Amazon SNS™)	An AWS-managed messaging service used to send notifications and alerts between internal services and external endpoints.
Amazon™ Web Application Firewall (WAF)	A web application firewall that helps protect the LabLink 360 web application from common web exploits and malicious Hypertext Transfer Protocol Secure (HTTPS) traffic by filtering and monitoring requests.
Amazon CloudFront™ Content Delivery Network (CDN)	A content delivery network service designed to securely deliver web application content to users with low latency by leveraging globally distributed edge locations.
Amazon CloudWatch™	An AWS monitoring service used to collect logs, metrics and events to monitor the performance, availability and health of the LabLink 360 Quality Assurance software platform.
Application load balancer	A load balancing service that distributes incoming Hypertext Transfer Protocol Secure (HTTPS) traffic across multiple backend services to ensure high availability and scalability of the LabLink 360 web application.
LabLink 360 web application	A browser-based user interface that allows users to access and interact with LabLink 360 Quality Assurance software functionality, including data management, workflows and reporting.
AWS Certificate Manager	An AWS service used to provision, manage and automatically renew SSL/TLS certificates to secure web-based communications to and from LabLink 360 Quality Assurance software.
Simple Mail Transfer Protocol (SMTP)	A standard email communication protocol used by the platform to send outbound notifications and system-generated emails to users.
Amazon Simple Storage Service™ (Amazon S3™) buckets	AWS-managed object storage used to store files, datasets and application-generated content within the LabLink 360 Quality Assurance software environment.
Common DB (Microsoft™ SQL Server™)	The managed database used to store structured application data, including user information, configuration settings and system-generated data.
Rancher™	A Kubernetes management platform used to administer and monitor the Amazon EKS environment supporting LabLink 360 Quality Assurance software. Rancher manages Kubernetes resources, including secrets and configuration data used by application services within the platform.
OpsRamp™	A software-as-a-service (SaaS) IT operations and monitoring platform used to monitor the health, availability and performance of infrastructure and application components supporting LabLink 360 Quality Assurance software.
Amazon EventBridge™	An AWS-managed event routing service used to process and route security-related events within the LabLink 360 Quality Assurance software environment. Amazon EventBridge receives security events from Amazon GuardDuty™ and distributes security alert notifications to the operations team to support awareness and investigation of potential security events.

Table 1: Component glossary

System access controls

Authentication

Authentication to the LabLink 360 Quality Assurance software is administered through a direct login mechanism using a unique email address or login string and password. User credentials are validated against securely stored, Secure Hash Algorithm (SHA)-2 encrypted passwords within the application database.

The LabLink 360 Quality Assurance software provides optional multifactor authentication to enhance account security. Customers can enable multifactor authentication for their users at the organizational level. When enabled, multifactor authentication requires a second form of verification delivered via either short messaging service (SMS) or email. Both phone number and email address fields are required for all users to support multifactor authentication functionality. Users may select their preferred verification method at the time of authentication.

Upon successful authentication, LabLink 360 Quality Assurance software generates a JSON Web Token (JWT), which is transmitted to the client via a HTTPS-only cookie. This token is included in subsequent requests to validate the user session and establish session context.

Administrative access to Thermo Fisher application servers and infrastructure, including access to the AWS infrastructure that manages the LabLink 360 Quality Assurance software, requires multifactor authentication. Thermo Fisher limits access to application servers and supporting infrastructure to authorized personnel only.

Authorization

The LabLink 360 Quality Assurance software leverages role-based access control (RBAC) to grant permissions and access to authorized users, where roles are configurable to meet necessary business requirements. Specifically, LabLink 360 Quality Assurance software utilizes four permission levels: Guest, Basic, Intermediate and Elite. Only those users assigned with the Elite role can access laboratory and user settings as well as audit review functionality. Audit review enables customers to view events that occur within their laboratory environment. For more information, refer to the Audit logging section.

Thermo Fisher recommends that role assignments follow the principle of least privilege, providing only the required system access needed to manage LabLink 360 Quality Assurance software.

Firewall and network controls

LabLink 360 Quality Assurance software platform security is managed through utilizing Amazon VPC to host infrastructure. Network access is restricted using AWS services, such as security groups and network access control lists (NACLs), to allow only necessary traffic according to business requirements.

Incoming web traffic to the LabLink 360 Quality Assurance software platform is routed through an application load balancer, which distributes requests across backend services deployed within Amazon VPC. LabLink 360 Quality Assurance software utilizes a WAF deployed to the supporting infrastructure, which analyzes traffic at the web server level, provides visibility to identify and mitigate threats and supports incident response.

Content delivery is optimized using a CDN to help reduce latency. Internal services communicate within the Amazon VPC using private networking, preventing direct external access.

Password management

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

For the LabLink 360 Quality Assurance software, passwords must be 8 to 32 characters in length and include a combination of uppercase letters, lowercase letters, numeric characters and special characters. Customers with Elite-level permissions have the option to set passwords to expire in 30, 60 or 90 days.

Note: Password expiration is not enforced by default.

Audit logging

The LabLink 360 Quality Assurance software captures events that occur within the application to help evaluate and document specific user tasks. The types of audit events captured include data modifications, such as the creation, update and/or deletion of data as well as the identity of the user performing the action and the date and time at which the action occurred. Customers can view these events directly within the LabLink 360 Quality

Assurance software through the Audit Log, accessible via the Settings menu. Access to the Audit Log is restricted to users with Elite-level permissions.

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 personnel.



Data storage and encryption

Data storage

Thermo Fisher stores customer-uploaded data, such as data used for QC analysis, reporting and workflow management, in Amazon S3 buckets and a Microsoft SQL Server database.

Encryption at rest

Thermo Fisher encrypts customer-uploaded data to the LabLink360 Quality Assurance software using full encryption of the Microsoft SQL Server database, Amazon S3 buckets and Amazon Elastic Block Store, which leverages 256-bit Advanced Encryption Standard (AES-256) for full encryption.

Encryption in transit

Transmitted data being sent to and from the LabLink 360 Quality Assurance software communicates over a Secure Socket Layer (SSL) connection using TLS v1.2 and greater.

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

Security certificates

The LabLink360 Quality Assurance software uses security certificates to support the encryption of data in transit, where the certificates automatically renew prior to expiration.



Cloud and endpoint protection

Cloud compliance monitoring

Thermo Fisher has implemented a 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 LabLink 360 Quality Assurance software leverages AWS to host its infrastructure, where AWS provides DDoS protection through AWS Shield.

Antivirus/anti-malware

The infrastructure supporting the LabLink 360 Quality Assurance software leverages Amazon GuardDuty™ S3 malware protection

to detect malicious software and help prevent its execution 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 LabLink360 features an Endpoint Detection and Response (EDR) platform to help 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 LabLink 360 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 employee, and regularly educate and share best practices with them to raise awareness of cybersecurity threats. Thermo Fisher 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 LabLink 360 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 LabLink 360 Quality Assurance software source code is stored in a Thermo Fisher-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 LabLink 360 Quality Assurance software are stored and maintained in a Thermo Fisher-approved artifact management solution. This provides visibility and control on developed software builds, enabling the LabLink 360 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 LabLink 360 Software Development team utilizes a Thermo Fisher-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 LabLink 360 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 LabLink 360 Software Development team uses a Thermo Fisher-approved dynamic analysis tool to evaluate web applications and application programming interfaces (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.

Penetration testing

Thermo Fisher's Penetration Testing team tests core components of the LabLink 360 Quality Assurance software 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 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 follows a standardized change control process that requires various approvals based on logical segregation of duties prior to progression to a higher environment. The LabLink 360 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 LabLink 360 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. Security updates and system patches for the infrastructure supporting LabLink 360 are planned for release on a regular cadence.

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

Disaster recovery and business continuity

The availability of services provided by LabLink 360 Quality Assurance software is a shared responsibility between AWS and Thermo Fisher. In the event of a large-scale system recovery of the cloud, under the AWS shared responsibility model, AWS will be responsible for the resilience and availability of the AWS services it provides, while Thermo Fisher will be responsible for the resiliency and availability of the services it deploys. This approach only applies to infrastructure supporting the LabLink 360 Quality Assurance software managed by Thermo Fisher, as business continuity plans can vary based on customer requirements.

System hardening practices

The LabLink 360 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 LabLink 360 Quality Assurance software; 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 LabLink 360 Quality Assurance software.

Health monitoring

The LabLink 360 Quality Assurance software infrastructure and application management follow documented standard operating procedures. Thermo Fisher monitors application and infrastructure health via health check tools, resource utilization and logging alarms.

Scalability

The LabLink 360 Quality Assurance software is a web-based application designed to scale 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 the LabLink 360 Quality Assurance software. Thermo Fisher's experienced team of professionals uses a global, follow-the-sun support approach for technical assistance and rapid escalation if critical issues arise.

To request technical support for LabLink 360, customers should submit a support request through their designated support channels. For more information about the LabLink 360 Quality Assurance software, documentation is available at the [LabLink 360 web page](#) or by the following methods:

- Phone: 1 (800) 232-3342 (select option 2, then option 1)
- Email: Lablink.gap@thermofisher.com

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

© 2026 Thermo Fisher Scientific Inc. All rights reserved. All trademarks are the property of Thermo Fisher Scientific and its subsidiaries unless otherwise specified. Amazon, Amazon CloudFront, Amazon CloudWatch, Amazon EKS, Amazon EventBridge, Amazon GuardDuty, Amazon S3, Amazon Simple Notification Service, Amazon Simple Storage Service, Amazon SNS, Amazon Virtual Private Cloud, Amazon VPC, Amazon Web Services and AWS are trademarks of Amazon Technologies, Inc. Apple and Safari are trademarks of Apple Inc. Firefox and Mozilla are trademarks of Mozilla Foundation. Google Chrome is a trademark of Google LLC. Kubernetes is a trademark of LF Projects, LLC. Microsoft, Microsoft Edge, SQL Server and Windows are trademarks of Microsoft Corporation. OpsRamp is a trademark of Hewlett Packard Enterprise Development LP. Rancher is a trademark of SUSE Inc. Amazon Technologies, Inc., Apple Inc., Google LLC, Hewlett Packard Enterprise Development LP, LF Projects, LLC, Microsoft Corporation, Mozilla Foundation and SUSE Inc. trademarks may be registered and/or used in the U.S. and other countries.