



Product security information guide

Thermo Scientific Connect Edge virtual gateway (for electron microscopes) | June 2026

Document valid through June 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

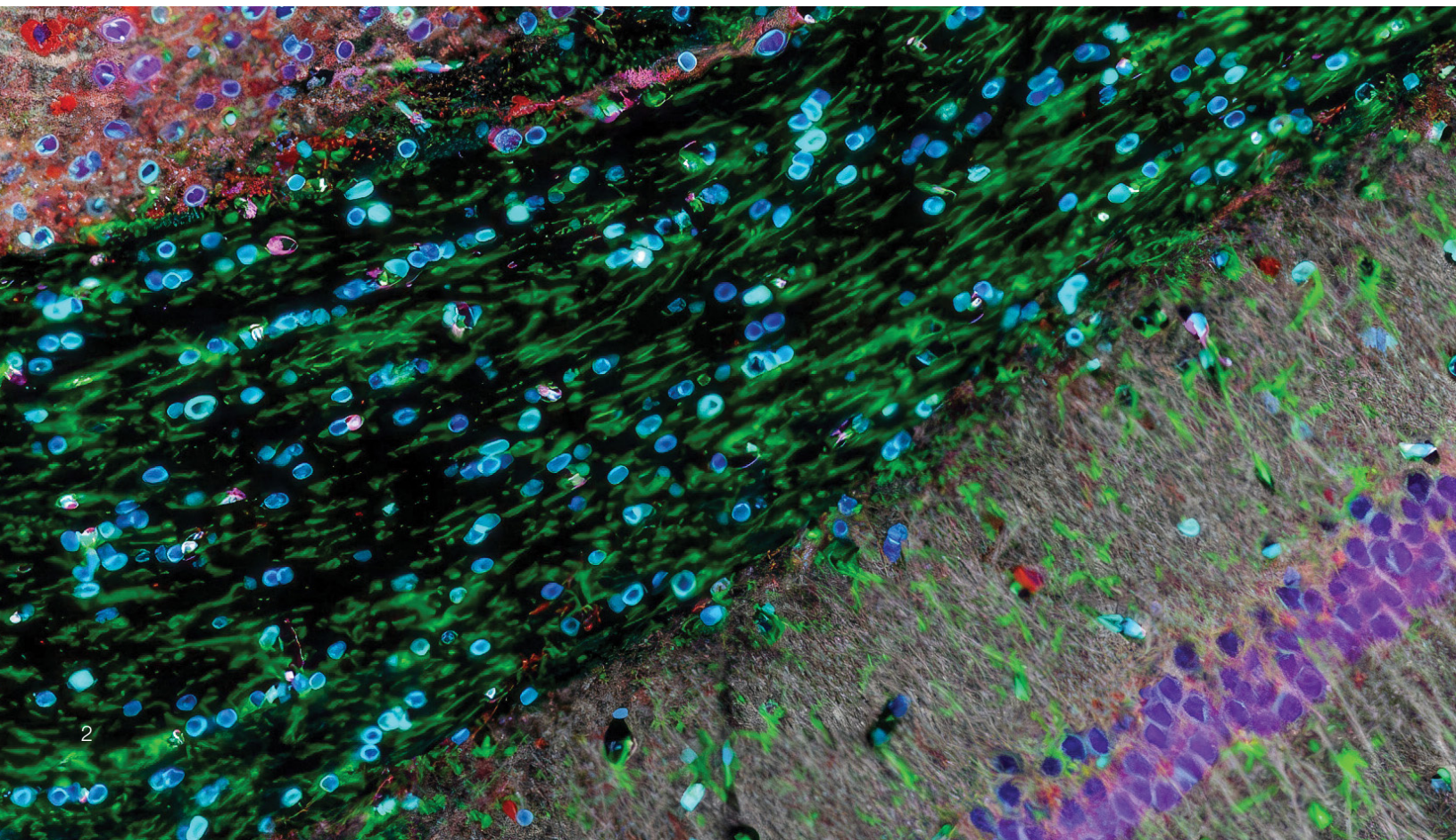
Thermo Fisher has implemented safeguards and protections designed to help protect the Thermo Scientific™ Connect Edge virtual gateway against intrusion or data compromise. This document describes the various standards, controls and data security approaches and business practices that Thermo Fisher has employed for this configuration.

Note: This document does not apply to security features within the optional Thermo Fisher™ Connect Platform.

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 **June 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 Scientific, or Thermo Fisher Scientific 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.



Product overview

The Thermo Scientific™ Connect Edge virtual gateway enables data communication between Thermo Scientific™ electron microscopes and the Thermo Fisher Connect Platform. Once connected, device sensor, scientific and operational health data may be transmitted through the Thermo Fisher Connect Platform in a standardized manner to support utilization monitoring and operational insights. The Thermo Fisher Connect Platform supports the Connect Edge virtual gateway capabilities including gateway management, device services, event history and notifications.

Note: The Thermo Fisher Connect Platform and its associated security controls are not in scope for this document. However, security information about the Thermo Fisher Connect Platform may be provided by contacting your account representative or visiting our [Information Security website](#).

System compatibility

The Connect Edge virtual gateway runs on a Docker™ container supporting Microsoft™ Windows™ 10 and later operating system (OS). Thermo Fisher recommends Windows 11 as the preferred OS. Prior to installation of the Connect Edge virtual gateway, installation of Windows Subsystem for Linux™ (WSL) and Rancher™ Desktop is required, which are installed by Thermo Fisher service personnel as part of the deployment process.

Regulatory standards

Development of the Connect Edge virtual gateway aligns with the [National Institute of Standards and Technology \(NIST\) Secure Software Development Framework \(SSDF\)](#).



Architecture diagram

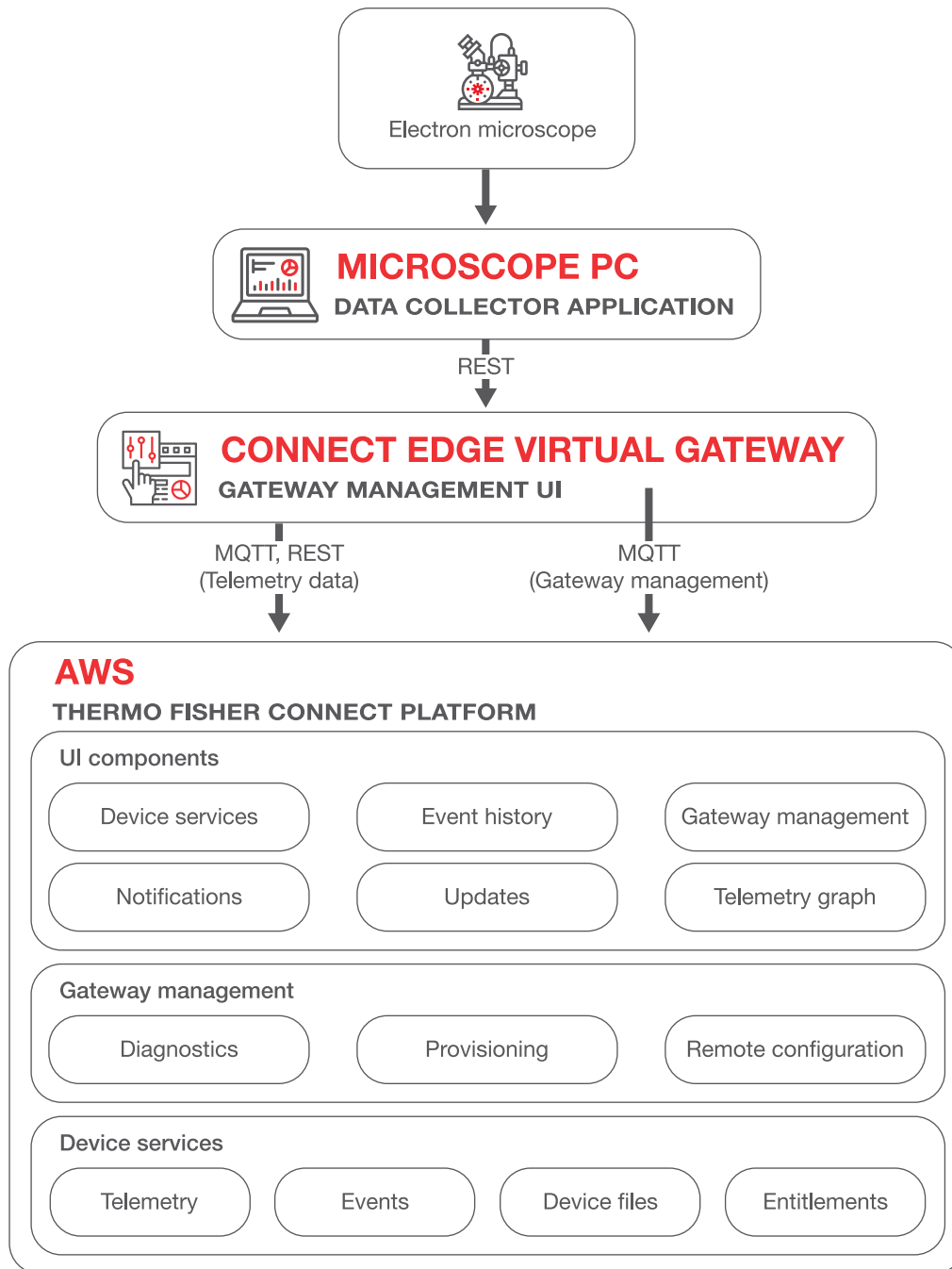
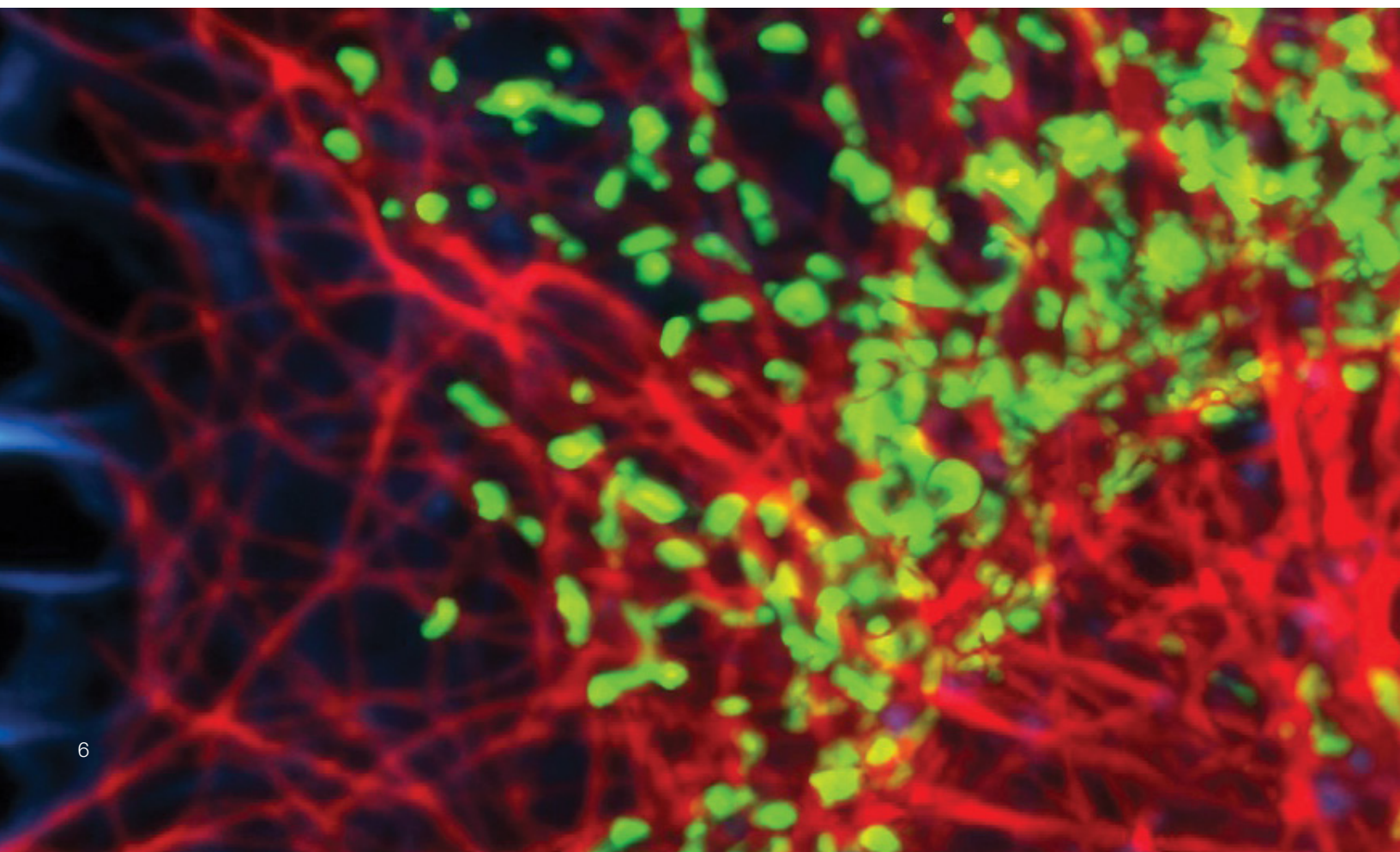


Figure 1: Connect Edge virtual gateway architecture diagram

Component glossary

Component	Definition
Electron microscopes	An instrument that uses electrons to create images that enable the visualization of extremely small molecules that cannot be seen with conventional light microscopes.
Microscope PC (MPC)	The PC used to support operation of the electron microscope and runs the Data Collector application.
Data Collector application	An application deployed on the MPC to communicate and transmit instrument telemetry data, events and files with the Connect Edge virtual gateway.
Connect Edge virtual gateway	The Connect Edge virtual gateway facilitates data communication, such as telemetry data and events, from the Data Collector application to the Thermo Fisher Connect Platform for data viewing and analysis. The Gateway Management user interface (UI) supports configuration of the Connect Edge virtual gateway.
Thermo Fisher Connect Platform	Instrument telemetry data, events and files from the Connect Edge virtual gateway may be transmitted to the Thermo Fisher Connect Platform for monitoring and analysis purposes.

Table 1: Component glossary



System access controls

Authentication & authorization

Authentication to the Connect Edge virtual gateway uses username and password credentials, prompting users to change the initial password upon first login. Authentication to the Thermo Fisher Connect Platform may be performed using either platform-managed user identities or federated authentication through the customer's identity provider, supporting OpenID™ Connect (OIDC) or Security Assertion Markup Language (SAML) protocols.

Administrative access to Thermo Fisher systems supporting the Connect Edge virtual gateway and Thermo Fisher Connect Platform requires multifactor authentication. Access to application servers and supporting infrastructure is restricted by Thermo Fisher to authorized personnel only.

Firewall and network controls

The Connect Edge virtual gateway is designed to initiate outbound network connections to the Thermo Fisher Connect Platform. Under normal operating conditions, inbound internet connections to the virtual gateway are not required.

Thermo Fisher recommends that customers configure firewall rules that allow only network traffic necessary for the operation of the Connect Edge virtual gateway, aligning with the customer's business, IT and security requirements.

Password management

The Connect Edge virtual gateway uses the authentication mechanisms of the underlying Windows OS. For authentication

to the local gateway management UI, passwords must satisfy the following requirements:

- Minimum of 8 characters;
- At least 1 uppercase character;
- At least 1 lowercase character;
- At least 1 numeric character; and
- At least 1 special character.

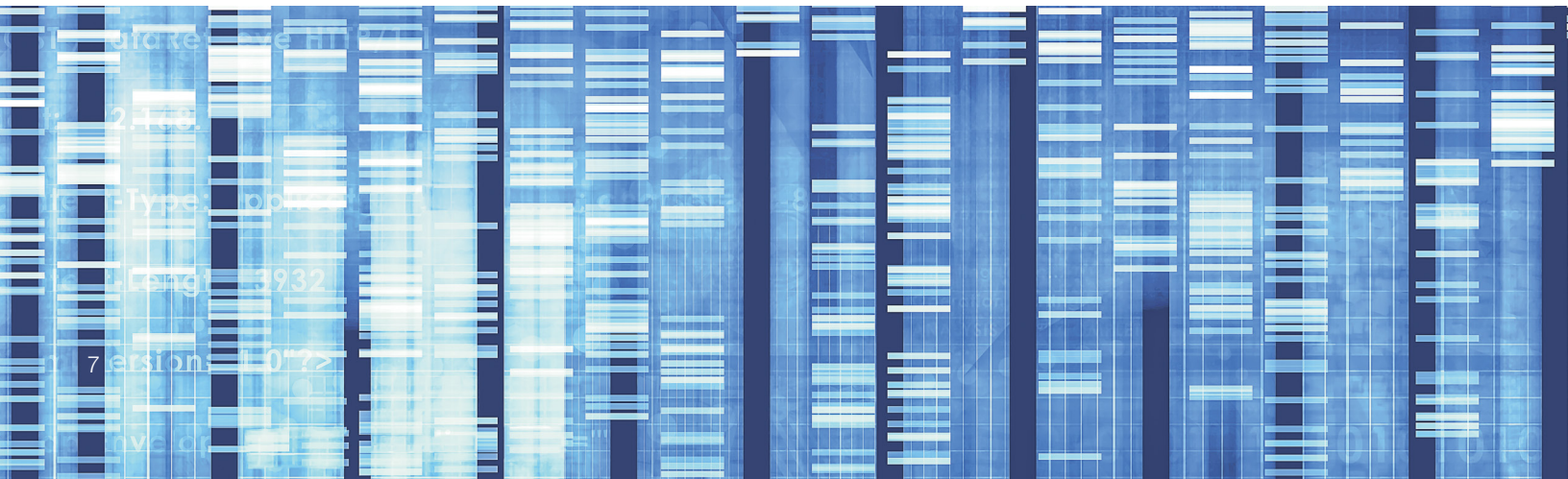
Customers are responsible for enforcing password complexity, expiration policies and account lockout thresholds at the operating system level in accordance with their organizational security and IT policies. Thermo Fisher recommends that password requirements align with industry standard practices.

Logging

The Connect Edge virtual gateway and supporting services generate logs related to security events, including:

- Connection attempts (successful and unsuccessful); and
- Operational and system performance metrics.

Logs may be transmitted to Thermo Fisher support personnel through telemetry and support mechanisms. Access to such logs is restricted to authorized Thermo Fisher personnel only.



Data storage and encryption

Data encryption

Certain data generated from the electron microscopes may be transmitted through the Connect Edge virtual gateway to Thermo Fisher's Amazon Web Services™ (AWS™) environment using Amazon Simple Storage Service™ (Amazon S3™) buckets, for long-term data storage. Customers may enable a feature that caches certain files with less than 10MB to memory on the microscope PC to support faster backups.

Data transmitted between the Connect Edge virtual gateway and the Thermo Fisher Connect Platform is encrypted in transit using Transport Layer Security (TLS) version 1.2 with support for TLS 1.3 where available.

Certificates

The Connect Edge virtual gateway uses X.509 certificates to support establishment, authentication and encryption communications between the gateway and the Thermo Fisher Connect Platform. Thermo Fisher manages certificate renewal, rotation and revocation processes in accordance with applicable operational and security requirements.



Secure product development lifecycle

Secure software development training

Software development training is available to the Connect Edge virtual gateway 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 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 Connect Edge virtual gateway 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

The Connect Edge virtual gateway 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 used, 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 Connect Edge virtual gateway are

stored and maintained in a Thermo Fisher-approved artifact management solution. This provides visibility and control on developed software builds, enabling the Connect Edge virtual gateway product 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 Connect Edge virtual gateway product 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 Connect Edge virtual gateway 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 Edge virtual gateway product 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 Connect Edge virtual gateway product 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 Connect Edge virtual gateway against the Open Web Application Security Project's (OWASP) Top 10 IoT and Top 10 API lists. The team, comprised of trained penetration testers, uses 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

Vulnerability and patch management

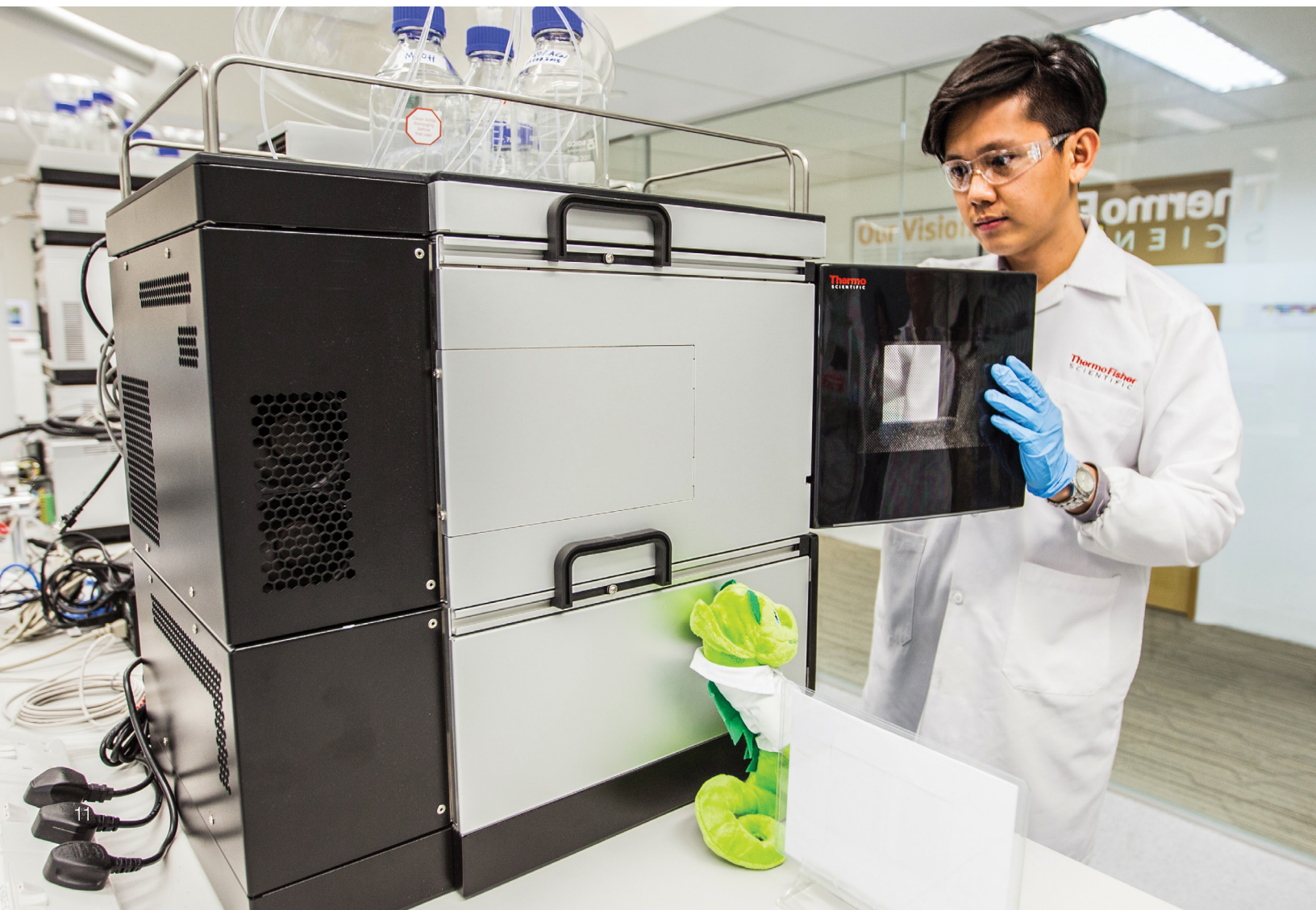
The Connect Edge virtual gateway Product Development team tests and validates security updates and system patches throughout the lifecycle of the product and deploys them to the impacted environments based on criticality and a business risk management process. Updates are communicated through product release notes and applied by Thermo Fisher support personnel in accordance with supported deployment procedures.

Thermo Fisher also recommends that customers utilize our [Reporting Security Issues form](#) to report suspected or potential security issues.

Service handling

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

Please contact your local Thermo Fisher Technical Support representative with questions or concerns pertaining to the Connect Edge virtual gateway.



 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 Web Services, Amazon Simple Storage Service, Amazon S3 and AWS are trademarks of Amazon Technologies, Inc. Docker is a trademark of Docker, Inc. Linux is a trademark owned by Linus Torvalds and administered by Linux Mark Institute. Microsoft and Windows are trademarks of Microsoft Corporation. OpenID is a trademark of OpenID Foundation. Rancher is a trademark of SUSE Inc. Amazon Technologies, Inc., Docker, Inc., Linux Mark Institute, Microsoft Corporation, Open ID Foundation and SUSE Inc. trademarks may be registered and/or used in the U.S. and other countries.