Product Security Information Guide

Thermo Scientific™ Connect Edge Gateway | Version 1.0 | December 2023

Document valid through December 1, 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 protections designed to help protect the Connect Edge Gateway against intrusion or data compromise. This document applies only to Connect Edge Gateway Version 1.0 deployed within the customer's environment. It describes the various standards, controls, data security approaches and business practices that Thermo Fisher Scientific has employed for this configuration. This document does not apply to security features within the optional Thermo Fisher™ Connect Platform.

Due to the ever-changing cyber landscape, each Product Security Information Guide is updated annually to ensure accurate information is being provided to our customers. This guide expires **December 1, 2024.** Please contact 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"). 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 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

Thermo Fisher Scientific maintains a Cybersecurity Program that includes technical, administrative and physical safeguards designed to detect vulnerabilities and mitigate against potential threats. Controls include web application firewalls (WAFs), intrusion detection systems (IDSs), multiple 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.

Product overview

The Thermo Scientific Connect Edge Gateway Version 1.0 solution lets you connect devices to a digital ecosystem to enable data communication between lab instruments and the Thermo Fisher Connect Platform. The Connect Edge Gateway currently supports devices, such as refrigerators, incubators and freezers, allowing for customers to connect their various devices to a central solution. Once connected, device sensor, scientific, and operational health data may be shared in a standardized and traceable way, providing utilization and criticality data anytime, anywhere through the Thermo Fisher Connect Platform.

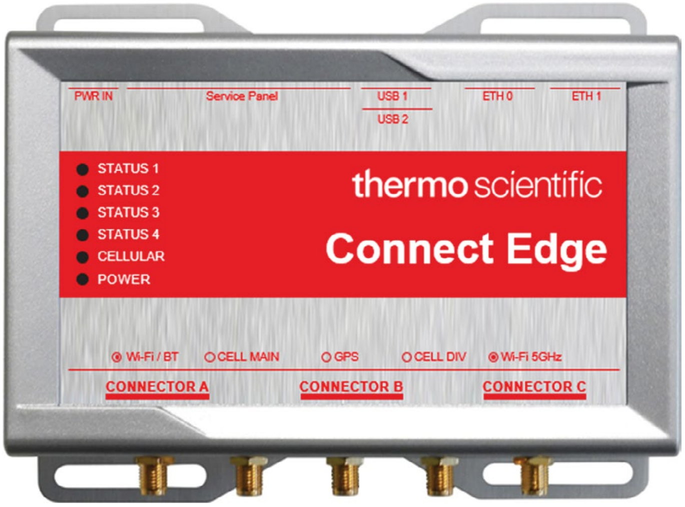


Figure 1: Connect Edge Gateway

Hardware specifications

The Connect Edge Gateway has the following hardware specifications:

- Texas Instruments™ Sitara™ processor AM3352 1GHz, 1 core
- 1GB RAM
- 8GB eMMC
- 4G LTE cellular, Wi-Fi/Bluetooth (model-dependent)

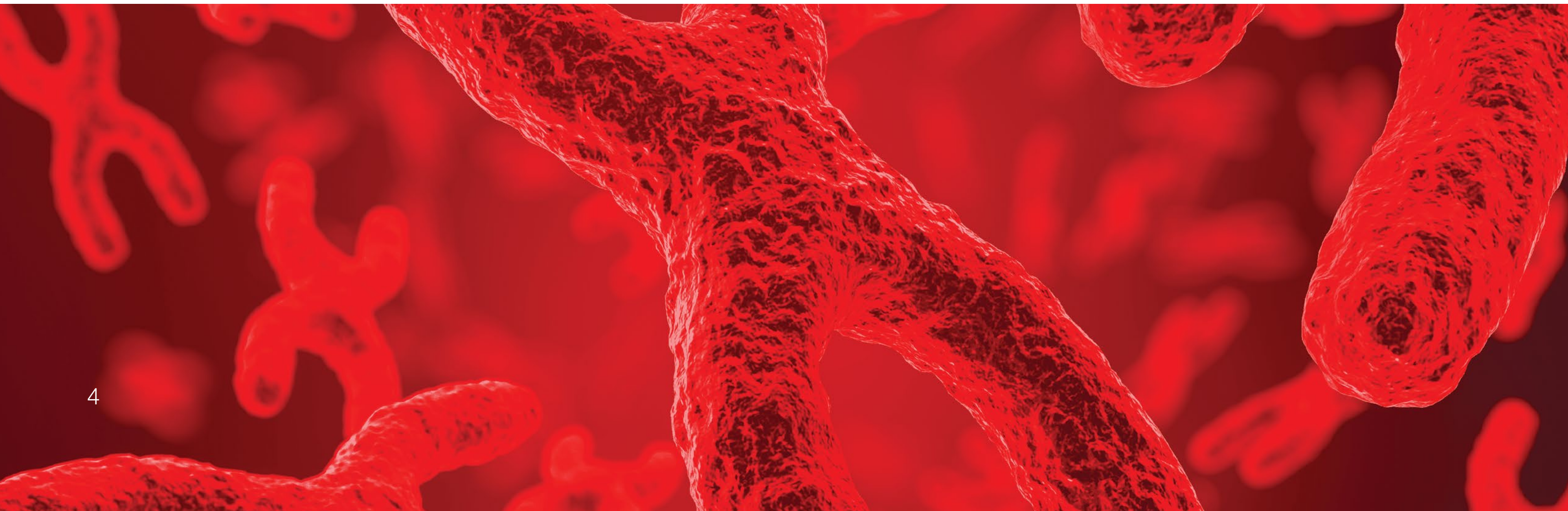
System compatibility

The Connect Edge Gateway runs a custom gateway image, Gateway Image TF_EDGE_10_12_1.0.0 or newer, which includes the following supported operating systems and software:

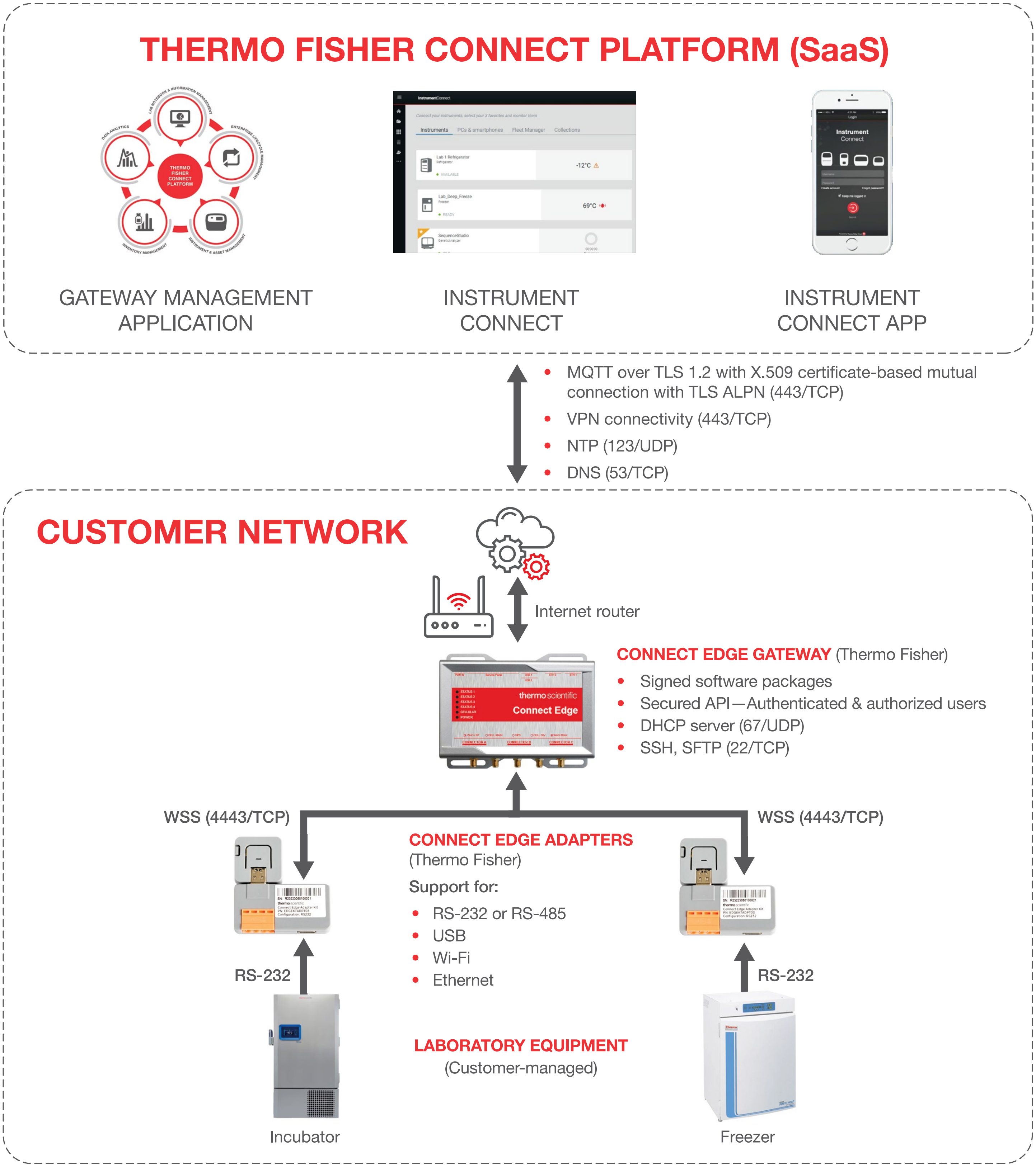
- Everyware™ Software Framework™ Version 7.2.3 or newer
- Everyware Linux™ operating system Version 27.1.0 or newer
- Everyware Cloud™ IoT Integration Platform Version 5.10.2 or newer

Third-party assets

The Connect Edge Gateway utilizes hardware manufactured by Eurotech™, specifically the Internet of Things (IoT) Edge Gateway™. The Connect Edge Gateway operates the Everyware Software Framework (ESF) which runs on the Everyware Linux operating system. The ESF provides provisioning, monitoring and diagnostic capabilities for the Connect Edge Gateway, allowing for gateway and imaging configurations and package installations.



Connect Edge Gateway architecture diagram



THERMO FISHER CONNECT PLATFORM (SaaS)

GATEWAY MANAGEMENT APPLICATION

INSTRUMENT CONNECT

INSTRUMENT CONNECT APP

- MQTT over TLS 1.2 with X.509 certificate-based mutual connection with TLS ALPN (443/TCP)
- VPN connectivity (443/TCP)
- NTP (123/UDP)
- DNS (53/TCP)

CUSTOMER NETWORK

Internet router

CONNECT EDGE GATEWAY (Thermo Fisher)

- Signed software packages
- Secured API—Authenticated & authorized users
- DHCP server (67/UDP)
- SSH, SFTP (22/TCP)

WSS (4443/TCP)

WSS (4443/TCP)

CONNECT EDGE ADAPTERS
(Thermo Fisher)

Support for:

- RS-232 or RS-485
- USB
- Wi-Fi
- Ethernet

RS-232

RS-232

LABORATORY EQUIPMENT
(Customer-managed)

Incubator

Freezer

Figure 1: Connect Edge Gateway architecture

Secure connectivity

Connect Edge Gateway component connectivity

Hardware	Supported instruments	Connectivity offerings	Security considerations
Connect Edge IoT Gateway	The Connect Edge Gateway supports refrigerators, incubators, freezers, and ultra-low temperature freezers. Support for additional instrument types is planned in future releases.	Serial	The connection from laboratory equipment to the Connect Edge adapters supports RS-232 (the standard serial connectivity protocol), RS-485, Transistor-Transistor Logic (TTL) RS-232 and USB. Wi-Fi and Ethernet are also supported within the Connect Edge adapter, allowing for connectivity to the Connect Edge Gateway via wireless or Ethernet.
		Wi-Fi	The Connect Edge Gateway supports the following Wi-Fi authentication schemes: WEP, WPA, WPA2 and WPA2 Enterprise (802.1X). For customers who configure Wi-Fi authentication based on WPA2 Enterprise (802.1X), the supported protocols include EAP-TLS and PEAP MSCHAPv2. Thermo Fisher Scientific recommends that customers configure one of the supported Wi-Fi authentication schemes based on their business and IT requirements.
		Ethernet (TCP/IP)	The connection from the instrument to the Connect Edge Gateway can also leverage a direct Ethernet connection using the Connect Edge adapter.

Table 1: Connect Edge Gateway component connectivity

Services, ports and protocols

Services	Ports	Network context
• Hypertext Transfer Protocol Secure (HTTPS) • Virtual Private Network (VPN) • Message Queue Telemetry Transport (MQTT)	443/TCP	Internet
• Secure Shell Protocol (SSH) • SSH File Transfer Protocol (SFTP)	22/TCP	Customer network
Network Time Protocol (NTP)	123/UDP	Internet
Domain Name System (DNS)	53/TCP	Internet or customer network
Dynamic Host Configuration Protocol (DHCP) server	67/UDP	Customer network
HTTPS, HTTPS over WSS	443, 4443/TCP	Customer network

Table 2: Connect Edge Gateway assets and secure connections

Various system services are used to run and manage the Connect Edge Gateway. Key services that can be configured by the customer are listed in Table 2.

Thermo Fisher Scientific recommends maintaining the native encryption mechanisms in use and encrypting network traffic wherever technologically feasible. Thermo Fisher Scientific also recommends closing any unused ports to limit connections and to follow industry standards and best practices.

Access controls

Authentication

The Connect Edge Gateway authenticates users leveraging username and password and prompts users to change the initial password at the first login. Please refer to the Connect Edge Gateway User Manual for the initial credentials to configure network settings.

Note: A customer must have a valid support agreement to access the Connect Edge Gateway User Manual. If you have questions, please contact Connect Edge Support for more information.

Authorization

The Connect Edge Gateway leverages role-based access control (RBAC) to grant permissions and access to required users, where roles are configurable to meet necessary business requirements. Thermo Fisher Scientific configures role assignments to use the principle of least privilege based on the need to manage and support the Connect Edge Gateway.

Firewall and network controls

The Connect Edge Gateway uses the Linux™-native utility **iptables** to block and allow traffic. Ethernet is available as the default network configuration for the Connect Edge Gateway. The gateway also has Wi-Fi capabilities, which are disabled by default. If the Connect Edge Gateway is unable to establish a connection with the Gateway Management endpoint during boot-up, then Wi-Fi will be temporarily enabled.

For IP assignment of the Connect Edge Gateway, Thermo Fisher Scientific recommends that customers reserve a dedicated IP address within their network configuration for consistent communication with the gateway adapters. For IP assignment of the devices connected to the Connect Edge Gateway, Thermo Fisher Scientific recommends that customers utilize the gateway's DHCP client mode as this is the default configuration. In addition, Thermo Fisher Scientific recommends that customers reserve IP addresses to be used by the gateway's DHCP client mode within their own network. Please contact Connect Edge Support for any additional questions on supporting advanced network configurations.

Password management

The Connect Edge Gateway user interface (UI) requires the use of passwords for user authentication. Upon initial authentication, a password change is required. All user account passwords must meet the following requirements:

- 12 to 80 characters in length
- At least 1 uppercase letter
- At least 1 lowercase letter
- At least 1 numeral
- At least 1 special character

All local web UI passwords are stored on the Linux file system and encrypted.

Logging

The Connect Edge Gateway logs multiple types of activities, capturing specific user actions and system performance anomalies. A combination of Linux-native tools and utilities are used for system logging and auditing, such as security enhanced (SE) Linux as well as the auditd (writes audit records to storage) and systemd-journald (collects and stores logging data) services.

By default, log files produced from the Connect Edge Gateway are stored locally and will be transmitted to the Thermo Fisher Connect Platform using MQTT over TLS v1.2.

Encryption

Hypertext Transfer Protocol Secure (HTTPS)

For HTTPS communications, TLS v1.2 encrypts the connection between the Connect Edge Gateway and the MQTT broker, as well as the WSS connection between the Connect Edge Gateway and the gateway adapters.

Message Queue Telemetry Transport (MQTT)

The IoT Connectivity Software Development Kit (SDK) uses TCP/IP (IP port 443) to establish a MQTT connection, allowing simple device data streaming (such as telemetry, status or event data) and remote command communication. MQTT provides advantages for device connectivity because of its low bandwidth requirements and publish/subscribe architecture. It is designed to provide embedded connectivity between applications and middleware on one side and networks and communications on the other side.

Certificates

The Connect Edge Gateway utilizes an X.509 device certificate to establish and authenticate the MQTT communication from the gateway to Thermo Fisher Connect Platform. This certificate generates a token, which is exchanged with the Thermo Fisher Connect Platform to obtain the device identity and credentials.

Secure development lifecycle

Secure software development training

Software development training is available to the Connect Edge Gateway Product Development team, allowing them to reinforce their knowledge of secure coding principles and 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, 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 the complexity of these component interactions. The assessment may include technical review, focused testing of identified components and regulatory review, if applicable. The Connect Edge Gateway Product Development team reviews, evaluates and prioritizes security assessment findings for remediation and acts on them based on criticality.

Source code management

The Connect Edge Gateway source code is stored in a Thermo Fisher Scientific-approved and internally facing version control solution that 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

The creation of software artifacts including, but not limited to, executables, images and libraries for the Connect Edge Gateway 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 Connect Edge Gateway 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. The Product Development team reviews and prioritizes security alerts for remediation based on criticality.

Peer code reviews

Manual peer reviews of code are conducted by the Connect Edge Gateway Product Development team before testing and deployment. Manual code reviews account 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 Connect Edge Gateway Product Development team uses a Thermo Fisher Scientific-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 fully scanned for security vulnerabilities and resilience to outside influence prior to product release. The Product Development team reviews and prioritizes findings from the scans for remediation based on criticality.

Architecture review

Thermo Fisher Scientific performs a security architecture review on the Connect Edge Gateway as part of the product security assessment. Led by product security architects, the assessment consists of understanding the major components involved in the Connect Edge Gateway, their interactions and connections and determining how security can be impacted based on the technology and configurations in use. Feedback and findings are considered and prioritized for remediation by the Connect Edge Gateway Product Development team based on their criticality.

Penetration tests

Thermo Fisher Scientific's Penetration Testing team tests core components of the Connect Edge Gateway against the Open Web Application Security Project's (OWASP) Top 10 IoT and OWASP's Top 10 API lists. The team is comprised of trained penetration testers who use technical and non-technical approaches to identify vulnerabilities during product development.

Vendor assessments

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

Product security maintenance

Vulnerability and patch management

The Connect Edge 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. Updates which contain fixes to critical and high vulnerabilities are evaluated and scheduled for remediation. Security patches are released as a software update to the Connect Edge Gateway. Upon receiving customer approval, the Connect Edge Gateway software updates can be applied remotely from the Thermo Fisher Connect Platform.

Thermo Fisher Scientific does not recommend that customers independently install security patches to the Connect Edge device as this can cause the device to fall out of vendor support per the guidelines stated in the Master Service Agreement (MSA). Please contact Connect Edge Support for assistance with deploying a patch to the Connect Edge Gateway.

Thermo Fisher Scientific also recommends that customers report suspected or potential security issues to our Cybersecurity Program.

System hardening

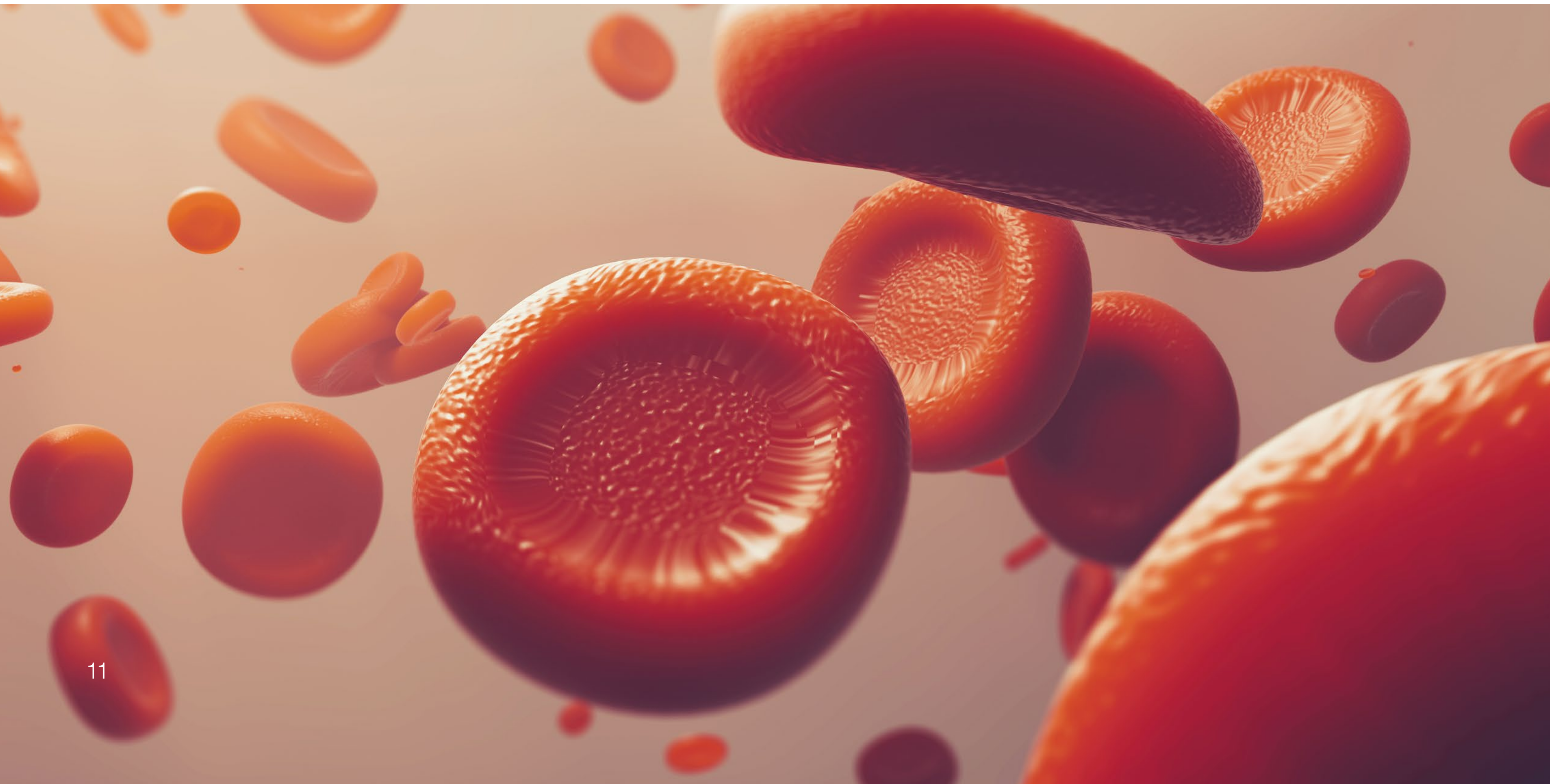
System hardening can mitigate the potential exploitation of system vulnerabilities and can prevent potential threats.

Prior to product deployment, security hardening practices are applied to the Connect Edge Gateway to further enhance its overall security, including disabling the Connect Edge Gateway SD slot.

Service handling

Product-specific support and global training serve as critical components to deploying and supporting IoT gateway devices. Thermo Fisher Scientific's experienced team of professionals use a global, follow-the-sun approach for technical assistance and rapid escalation if critical issues should arise.

Please contact Connect Edge Support with questions or concerns pertaining to the Connect Edge Gateway.



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

For Research Use Only. Not for use in diagnostic procedures. ©2023 Thermo Fisher Scientific Inc. All rights reserved.

Eurotech Internet of Things Edge Gateway is a trademark of Eurotech S.p.A. Everyware Cloud, Everyware Linux and Everyware Software Framework are trademarks of Everyware Worldwide Inc. Linux is a trademark administered by LMI Oregon, LLC. Sitara is a trademark of Texas Instruments Incorporated. All other trademarks are the property of Thermo Fisher Scientific and its subsidiaries unless otherwise specified.