Security quick reference guide

Thermo Fisher™ Connect Platform, Individual Edition and Team Edition | version 1.0 | December 2023

Document valid through December 15, 2024

Introduction

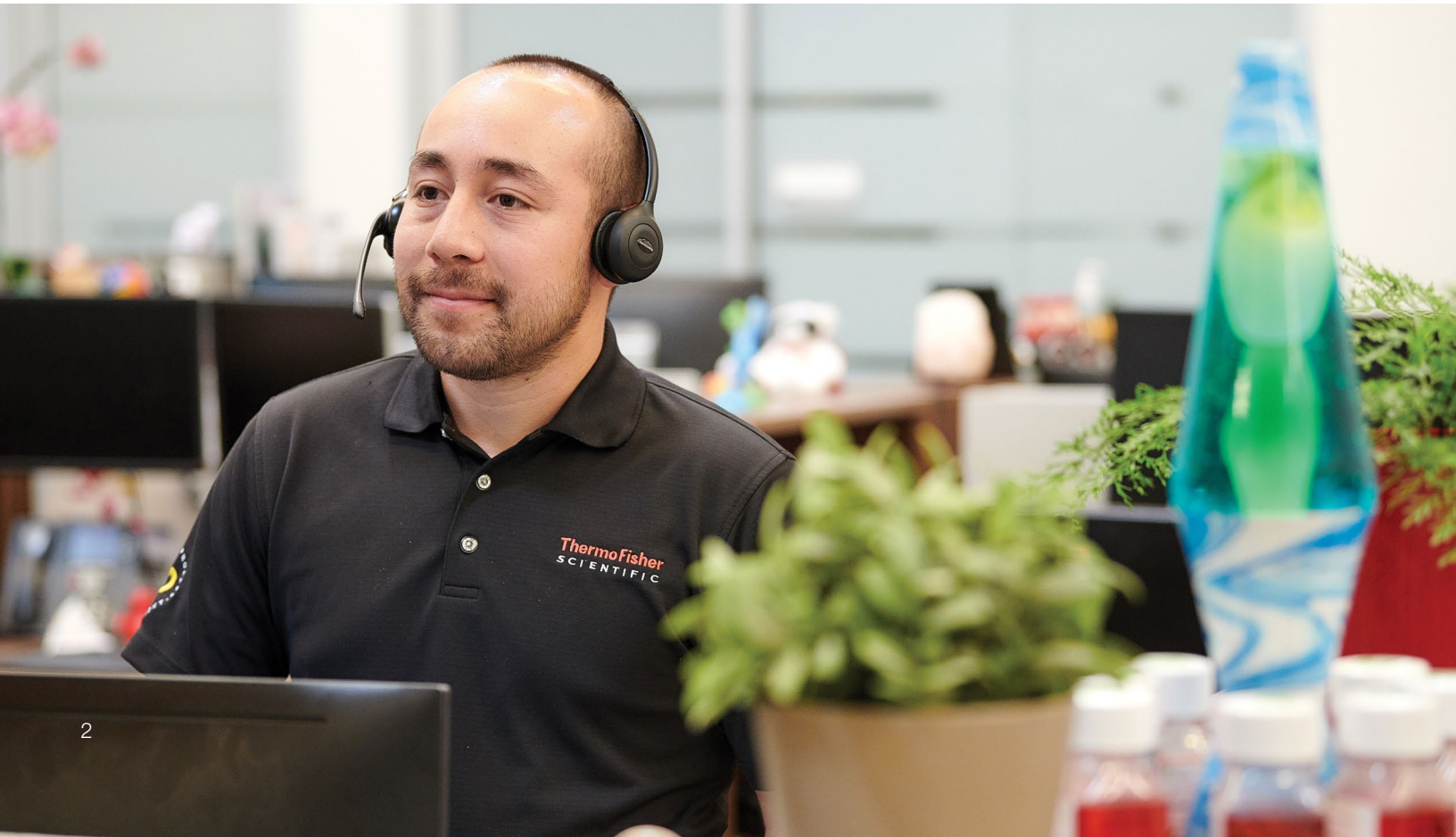
Thermo Fisher Scientific™ maintains a Cybersecurity Program, led by a dedicated Chief Information Security Officer (CISO), designed to safeguard the confidentiality, integrity and availability of data and systems within our environment. Thermo Fisher Scientific supports a continuously improving security 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 various safeguards and procedures designed to help protect the Connect Platform Individual and Team editions against intrusion and data compromise. The Connect Platform was designed and developed in collaboration with our Corporate Cybersecurity Program, which provides technical, administrative and physical safeguards for detecting vulnerabilities and addressing potential threats. Thermo Fisher Scientific's Cybersecurity Program has been certified as International Organization for Standards (ISO) 27001:2013-compliant.

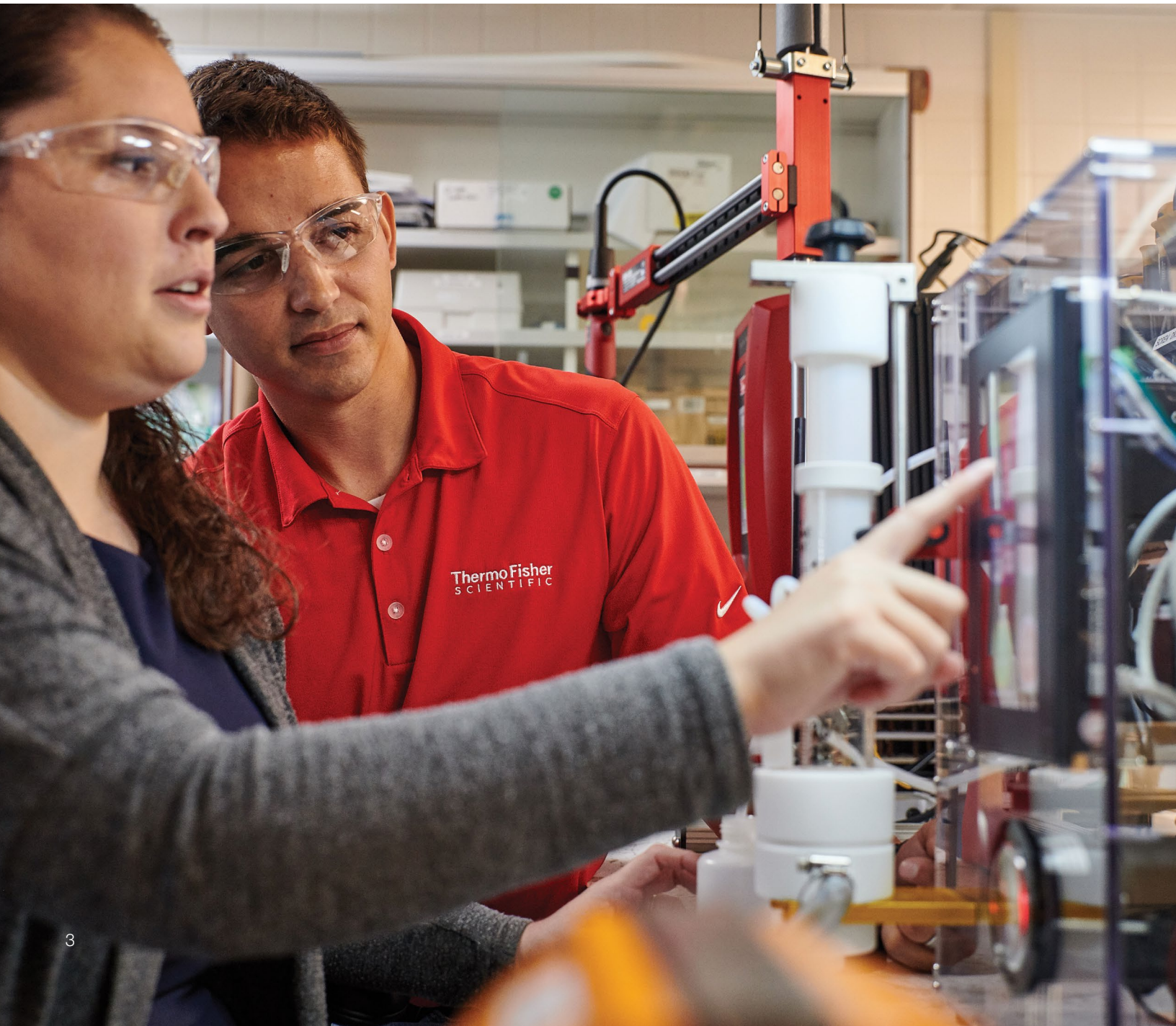
Due to the ever-changing cyber landscape, Security Quick Reference Guides are updated annually to ensure we provide accurate information to our customers. This guide expires on **December 15, 2024.** Please contact your account representative to obtain the latest published version.

The information contained in this Security Quick Reference 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 customer that any of the methods or suggestions described in this Security Quick Reference 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 Security Quick Reference Guide.



Product information

The Thermo Fisher Connect Platform Individual and Team editions deliver a robust suite of digital capabilities designed to enhance laboratory efficiency for managers and technicians. Individual and Team editions are supported by Amazon™ Web Services™ (AWS) Virtual Private Cloud™ (VPC) infrastructure and provide secure, cloud-based data storage, scientific analysis applications and peer collaboration tools to simplify data analysis and enable greater data visibility.



Comprehensive security controls

Authentication and authorization

OpenID Connect (OIDC) manages authentication on Connect Platform Individual and Team editions, supported by SAP™ Customer Data Cloud™ (CDC). Two login methods exist:

- Direct login: Users can establish their system identities directly within the Connect Platform Individual and Team editions.
- Federated login: Connect Platform Team edition supports federated login through a customer identity provider (IdP) on either OIDC or Security Assertion Markup Language (SAML) protocols. Thermo Fisher Scientific's Customer Identity Platform (CIP) team can configure a trust relationship with the customers' IdP upon request, providing two options:
  - Domain-based authentication: All users from the customer's IdP can authenticate to the platform.
  - Specific-user authentication: This option restricts the authentication to a predefined list of users.

Please contact your Thermo Fisher Scientific business representative for more information on configuring your IdP with the Connect Platform.

For internal colleagues, Thermo Fisher Scientific limits access to application servers and infrastructure to authorized personnel only. For example, administrative access to the AWS console, which manages Connect Platform Individual and Team editions' infrastructure, requires multifactor authentication (MFA).

Cloud security

Thermo Fisher Scientific has implemented a security control framework allowing for automated adoption of the cloud while maintaining security safeguards. This solution simultaneously monitors and governs thousands of controls across our AWS accounts.

Our Cloud Governance and Incident Detection and Response programs focus on the cloud security control framework. The Cloud Governance program implements procedures and utilizes automated tools to detect incorrectly configured cloud resources, while the Incident Detection and Response program enforces the deployment of security tools to identify suspicious behavior at the cloud- and server-instance levels. Alerts from the security tools are directly sent to the appropriate response team for triage.

Network and endpoint security

Thermo Fisher Scientific manages Connect Platform Individual and Team editions' network security using virtual private clouds (VPCs), network access control lists (NACLs) and security groups (SGs) to restrict network access, only allowing necessary communication. Public subnets host only external services, while private subnets host internal services and infrastructure, such as databases that are not publicly accessible.

The Connect Platform Individual and Team editions utilize AWS to host infrastructure. AWS provides distributed denial-of-service (DDoS) protection called AWS Shield™ that safeguards all Thermo Fisher Scientific-hosted services, including the Connect Platform Individual and Team editions. Additionally, the protection is further enhanced by scalability features such as elastic load balancers and auto-scaling groups to handle spikes in traffic.

Connect Platform Individual and Team editions are supported by virtual machines that leverage endpoint detection and response (EDR) tools. These tools detect, prevent and assist in response to sophisticated intrusion methods that could bypass traditional antivirus solutions.

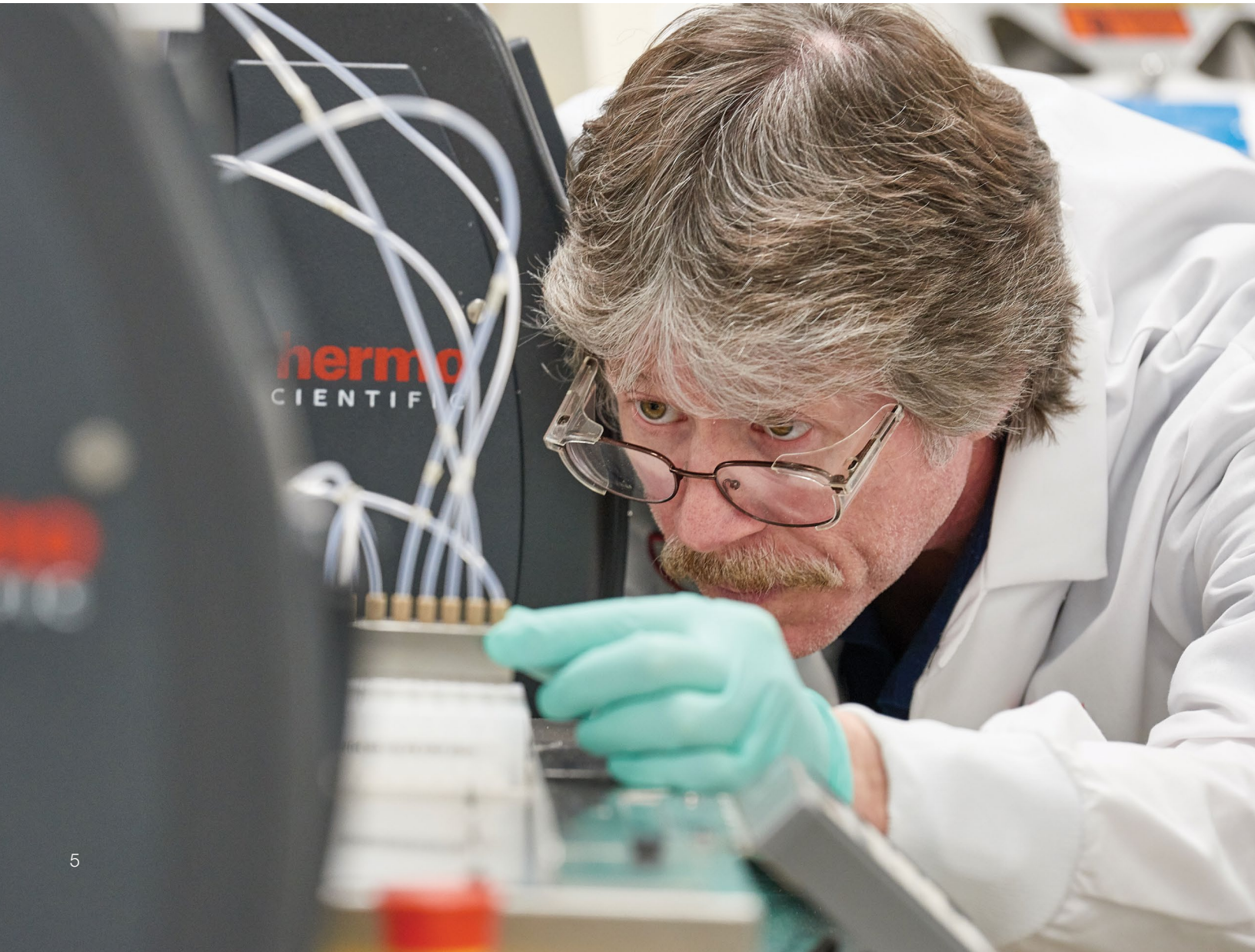
Data encryption methods

Encryption at rest

Thermo Fisher Scientific stores device and customer-uploaded data to the Connect Platform Individual and Team editions primarily in AWS Simple Storage Service™ (S3). The data stored in S3 is encrypted using AWS S3 server-side encryption that utilizes 256-bit Advanced Encryption Standard (AES-256). Other database and storage services leverage native AWS encryption mechanisms. Backups that contain any customer data are also encrypted at rest.

Encryption in transit

Data uploaded from an instrument or a user to the Connect Platform Individual and Team editions is encrypted in transit. Web and mobile clients accessing data in the cloud use Hypertext Transport Protocol (HTTP) over Transport Layer Security (TLS), otherwise known as HTTPS, utilizing 256-bit encryption. For Internet-of-Things (IoT) connected devices that integrate with the Connect Platform, both Message Queueing Telemetry Transport (MQTT) over TLS protocols and HTTPS are used to secure communications.



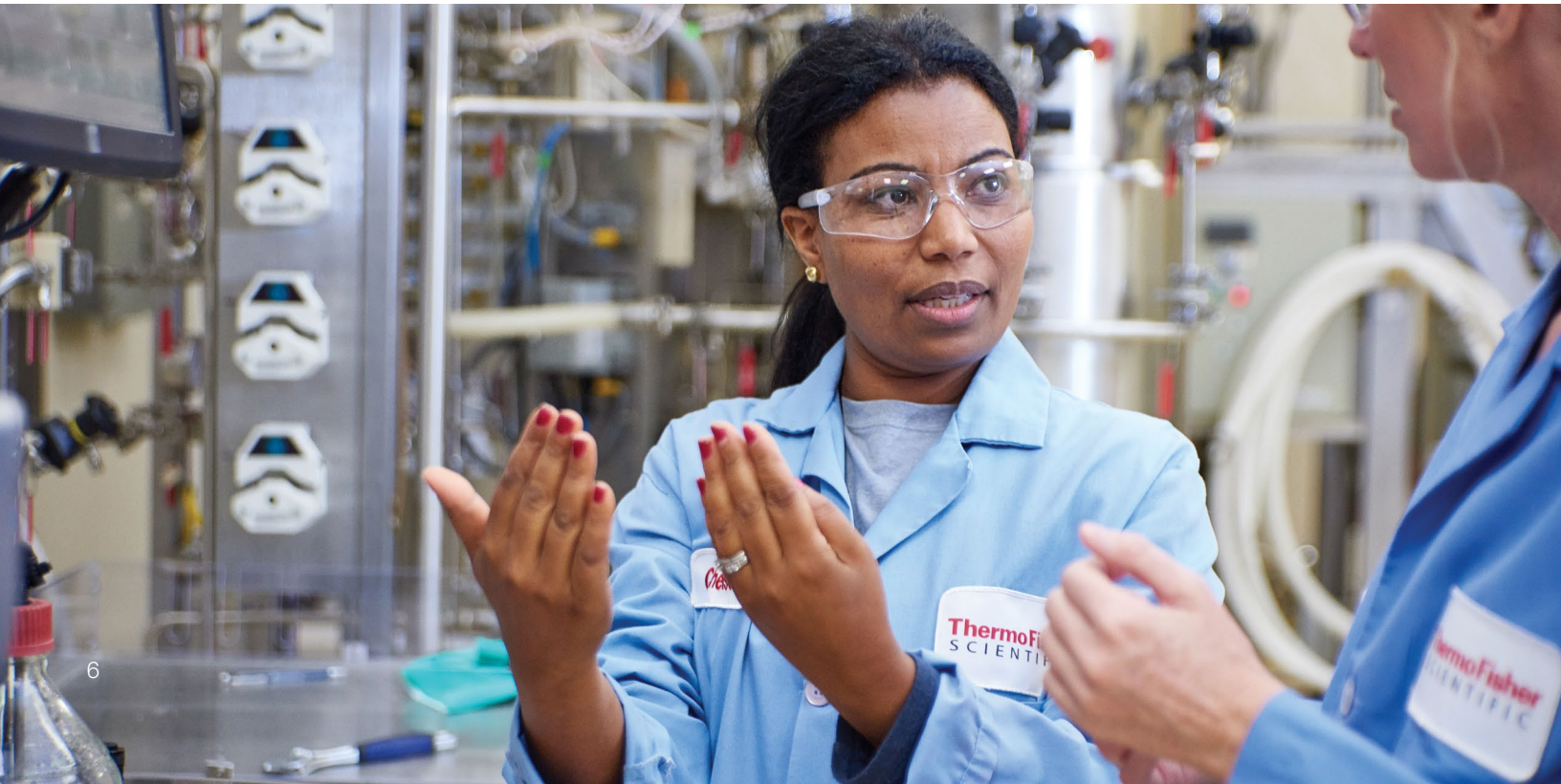
Secure product development lifecycle

Products, instruments, software and devices are subject to 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 Product Development team reviews, evaluates and prioritizes security assessment findings for remediation and acts on them based on criticality.

Additional security measures employed by the Connect Platform Product Development team as part of the product security assessment include storing source code in a Thermo Fisher Scientific-approved version control solution that is only internally accessible and contains built-in redundancy. Software artifacts are maintained in an artifact management solutions that provides visibility and control of developed software builds. The solution leverages static analysis and dynamic analysis tools to scan code repositories as well as web applications and application programming interfaces (APIs), where applicable, for potential security vulnerabilities.

Thermo Fisher Scientific follows a standardized change control process that requires supervisor, application owner and Quality Assurance governance approvals. The Connect Platform Product Development team, in accordance with Thermo Fisher Scientific policies, follows documented standard operating procedures for application and infrastructure management. Health check tools and alarms for resource utilization and logging monitor application and infrastructure health.

The Connect Platform Product Development team employs separate development, test, staging and production environments. The lower environments, including development, test and staging, are not publicly accessible and require the use of a virtual private network (VPN) for secure access. Updates for security and system patches are tested, validated and prioritized based on criticality prior to being deployed to impacted environments.



Questions? Please visit **thermofisher.com/connect** if you would like to learn more or have questions.

To request support for Connect Platform Individual and Team editions, sign into **https://apps.thermofisher.com** and click the Feedback button located near the bottom-right corner.

FL80986-EN1223