Security quick reference guide

Thermo Scientific Smart-Vue Pro software
April 2026

Document valid through April 30, 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 has measures 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

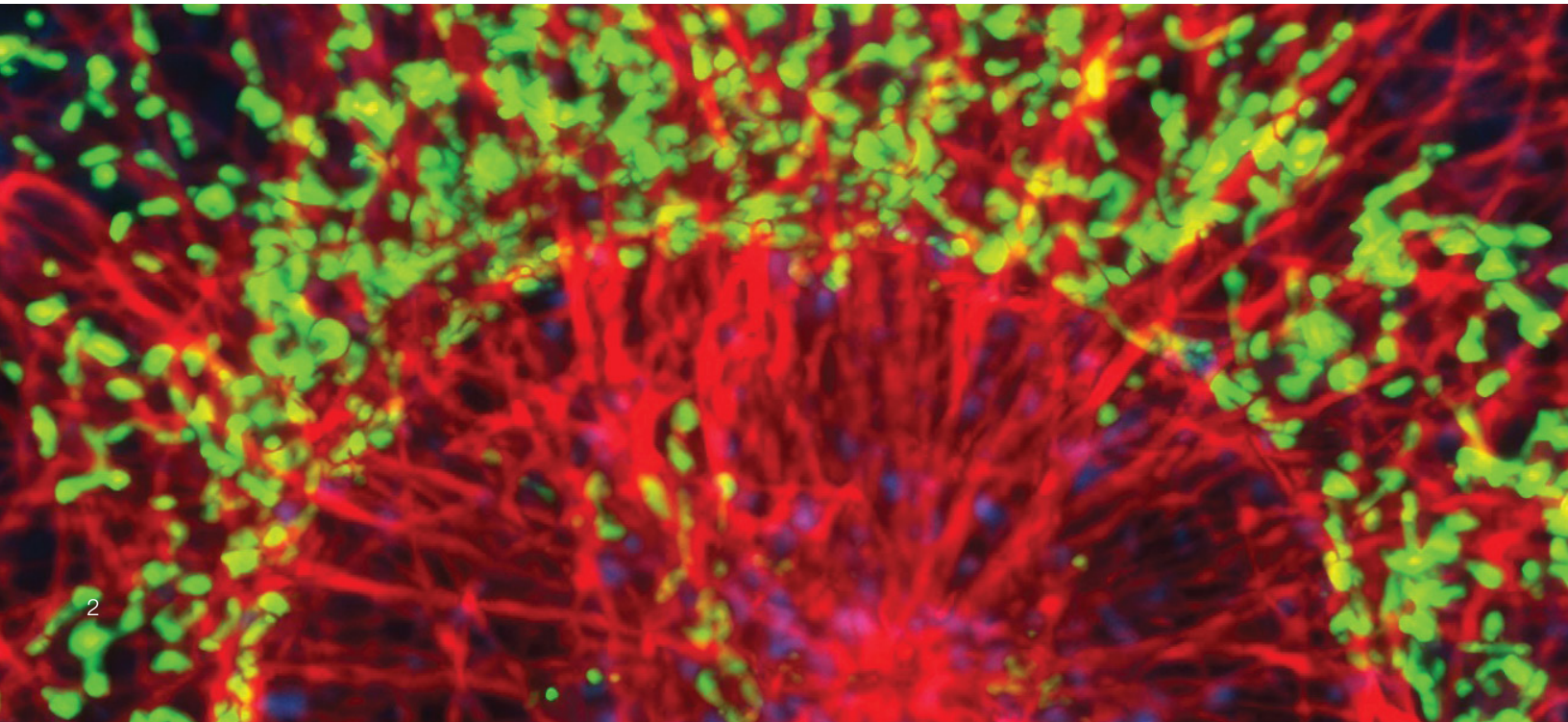
Thermo Fisher collaborates with a third-party partner to provide safeguards and protections that are designed to help protect the Thermo Scientific™ Smart-Vue™ Pro solution against intrusion or data compromise. Such third-party providers are independent and are not affiliates of Thermo Fisher Scientific. This document describes the various standards, controls, data security approaches and business practices that Thermo Fisher and the third-party partner use in this effort. Please contact your account representative for more information about the partnership between Thermo Fisher and the third-party partner.

Thermo Fisher relies, in part, on information provided by third-party providers regarding their security practices and does not independently verify all third-party controls. Responsibility for third-party components remains with the respective provider, subject to applicable agreements.

Due to the ever-changing cyber landscape, Thermo Fisher updates this security quick reference guide annually to maintain current and accurate information. This guide expires on **April 30, 2027.** Contact your account representative or visit our Information Security website to get 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" and/or "Thermo Fisher").

Additionally, this security quick reference 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 security quick reference guide will eliminate security risks, restore customer's systems, resolve issues related to any malicious code or achieve any other stated or intended results. Customers are solely responsible for evaluating and implementing appropriate security measures within their own environments and should not rely exclusively on this guide. The customer exclusively assumes all risk of utilizing or not utilizing any guidance described in this security quick reference 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.

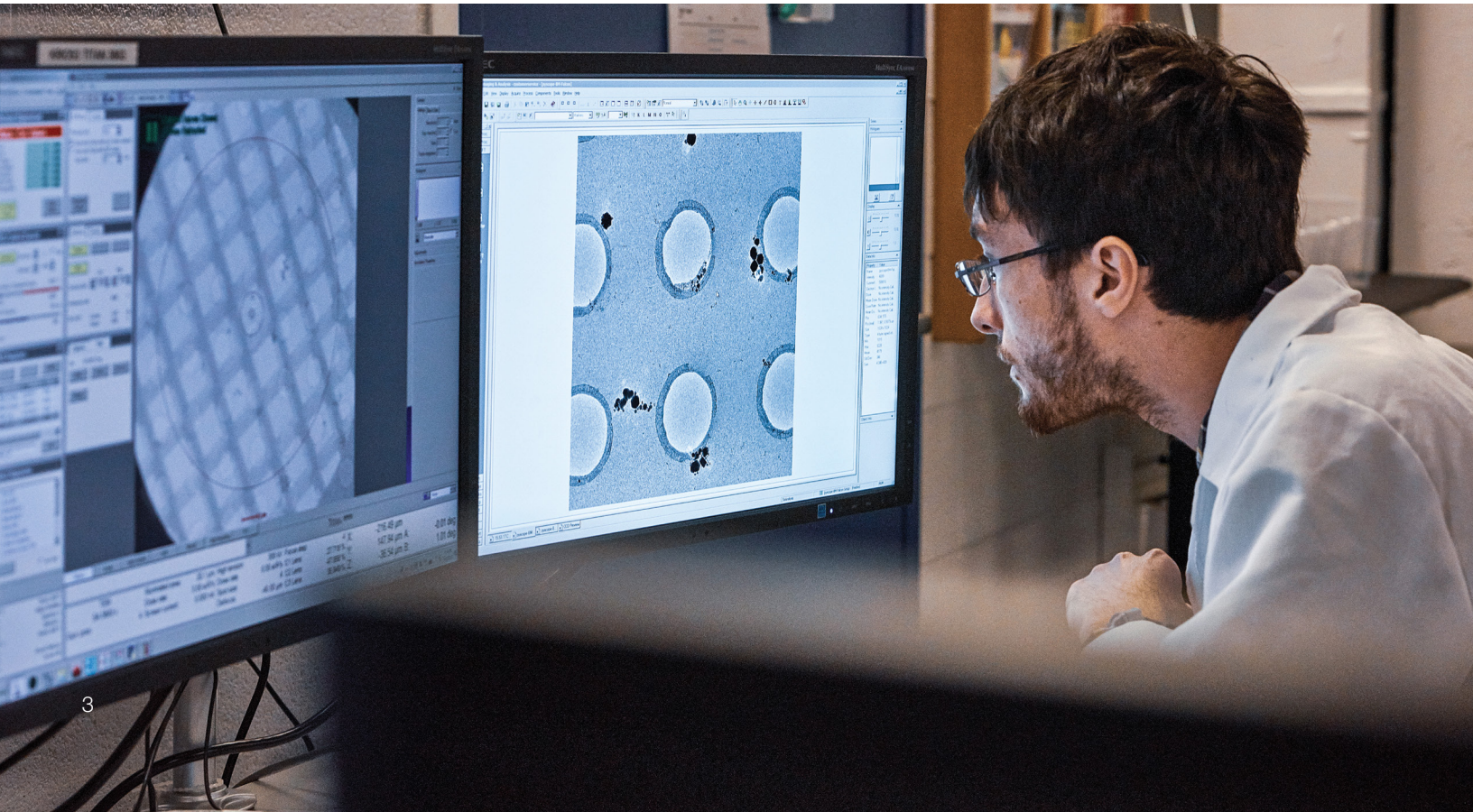
Thermo Fisher's Cybersecurity Program maintains an International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:2022 certification for the management of the following areas:

- 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™ Smart-Vue™ Pro solution is a remote environmental monitoring system designed to collect, store, visualize and alert on environmental data such as temperature and humidity. The solution integrates wireless monitoring devices, gateways, mobile applications and a centralized web-based application.

The Thermo Scientific Smart-Vue Pro supports both cloud-hosted and customer-managed (on-premises) deployments. The same core security mechanisms apply to both deployment models, with customers responsible for securing their own infrastructure in on-premises environments.

System components and data

Smart-Vue Pro consists of the following primary components:

- Smart-Vue Pro monitoring modules operating in LoRaWAN™ or Bluetooth™ Low Energy (BLE) modes;
- Smart-Vue Pro LoRaWAN gateways;
- Smart-Vue Pro web/mobile applications and application programming interfaces (APIs); and
- Amazon Web Services™ (AWS™)-hosted cloud infrastructure (only used for cloud deployments).

Certain components of the Smart-Vue Pro solution rely on third-party technologies and infrastructure. Thermo Fisher does not control all underlying third-party systems, and their availability, performance and security are subject to the respective third-party providers.

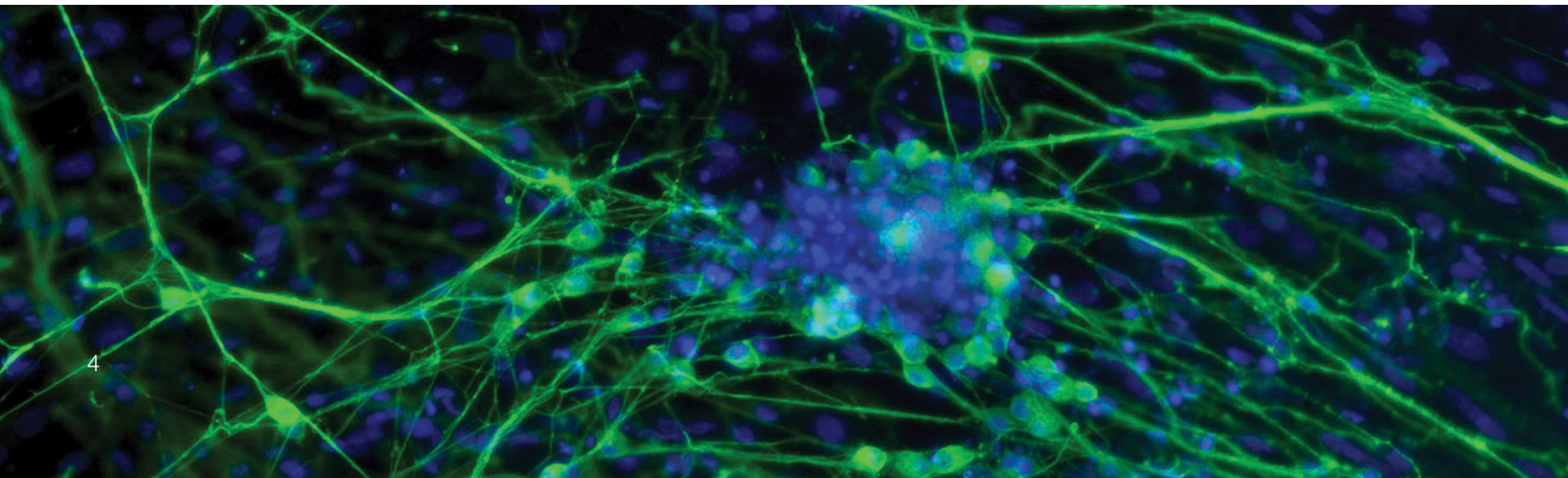
Third-party assets

The Smart-Vue Pro LoRaWAN gateway is based on hardware provided by MultiTech™ using the official AEP 6.x firmware. However, Thermo Fisher has its own firmware version based on the official firmware and includes several notable differences, such as default settings for simplicity and to help reduce potential configuration errors.

Additional changes made to the MultiTech firmware are as follows:

- Added a LoRaWAN server Test button in LoRaWAN page for connection verification;
- Preconfigured LoRa frequencies in LoRaWAN page with Thermo Fisher-supported frequencies;
- Preconfigured network interfaces to have a working fallback setup by default; and
- Preconfigured Wi-Fi settings to scan and list Wi-Fi networks upon first boot.

Thermo Fisher does not make any changes to MultiTech security rules and security implementations and relies on Multi-Tech Systems, Inc. to develop and provide any firmware updates, including security-related updates. Thermo Fisher does not control and is not responsible for the security, performance or availability of third-party firmware components. Only required firewall ports are opened, based on the customer's server configuration. Thermo Fisher makes every effort to keep our products current with respect to MultiTech updates. However, it does not guarantee the timing, availability or implementation of such updates.



Security certifications or regulatory standards

The Smart-Vue Pro software is designed to support customer efforts to comply with The U.S. Food and Drug Administration (FDA) 21 CFR Part 11 requirements for electronic records and electronic signature. However, compliance with 21 CFR Part 11 depends on the customer's specific implementation, configuration and use of the system, as well as procedural and administrative controls outside the scope of the software. Thermo Fisher does not represent or guarantee that use of the Smart-Vue Pro solution alone will result in compliance with 21 CFR Part 11.

Smart-Vue Pro is designed to provide full traceability through computer-generated and time-stamped audit trails that record user actions, data modifications and system events. Each entry should capture the unique user ID, date and time and should preserve prior values, where applicable, to support reconstruction of record history.

The system is designed to continuously record environmental conditions such as temperature and humidity, alarm events and user interactions. Records can be retained according to configured and defined policies and may be exported in human-readable and electronic formats suitable for regulatory review, if necessary. Customers are responsible for defining, implementing and maintaining appropriate data retention, review and archival policies in accordance with applicable regulatory requirements. Electronic signatures are intended to be linked to the associated record and include the printed name, date, time and signature.

By maintaining comprehensive performance history including environmental data and alarm acknowledgments, Smart-Vue Pro is intended to support customers in maintaining records for purposes such as training, internal quality reviews and regulatory audits. Such capabilities may assist customers in addressing data integrity, authenticity and reliability expectations under 21 CFR Part 11, but do not, by themselves, ensure compliance.

Architecture diagram

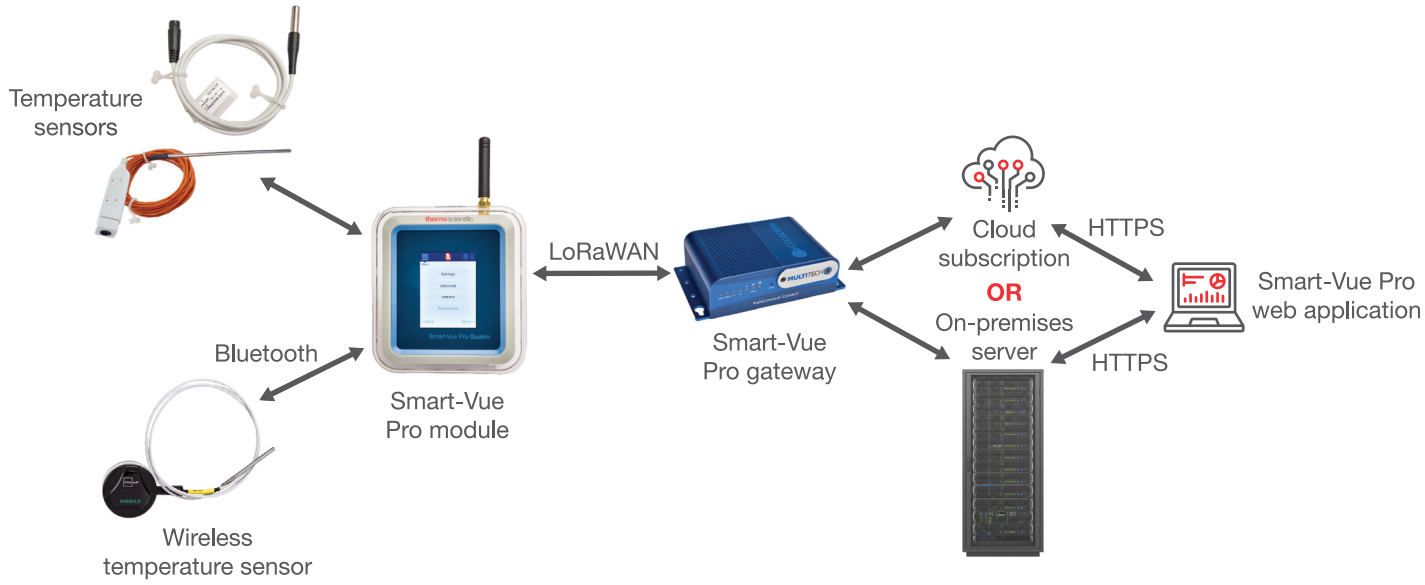


Figure 1: Smart-Vue Pro architecture diagram

Comprehensive security controls

Authentication & authorization

Authentication to the Smart-Vue Pro web application is designed to be administered through an industry-standard OAuth 2.0 identity server using OpenID™ Connect. Users must authenticate with valid credentials to access the platform. Authentication effectiveness depends on proper configuration, credential management and endpoint security.

The Smart-Vue Pro solution leverages role-based access control (RBAC) to grant permissions and access levels to authorized users, where roles are configurable to meet necessary business requirements. Access controls are implemented based on configured roles and system settings and may vary depending on customer configuration.

Password management

The Smart-Vue Pro server authentication is designed to enforce the following password controls. Configuration of these controls may vary based on deployment settings and customer requirements. Additional controls can be applied to meet enhanced customer requirements. Typical password controls include:

- Minimum password length of 8 characters
- A combination of uppercase and lowercase letters, numbers and special characters
- Account lockout after 3 unsuccessful login attempts
- Password reset required following account lockout

Smart-Vue Pro modules are designed not to store user passwords. PIN codes entered on device screens are validated locally using a proprietary hash-based mechanism intended to be unique to each customer.

Logging

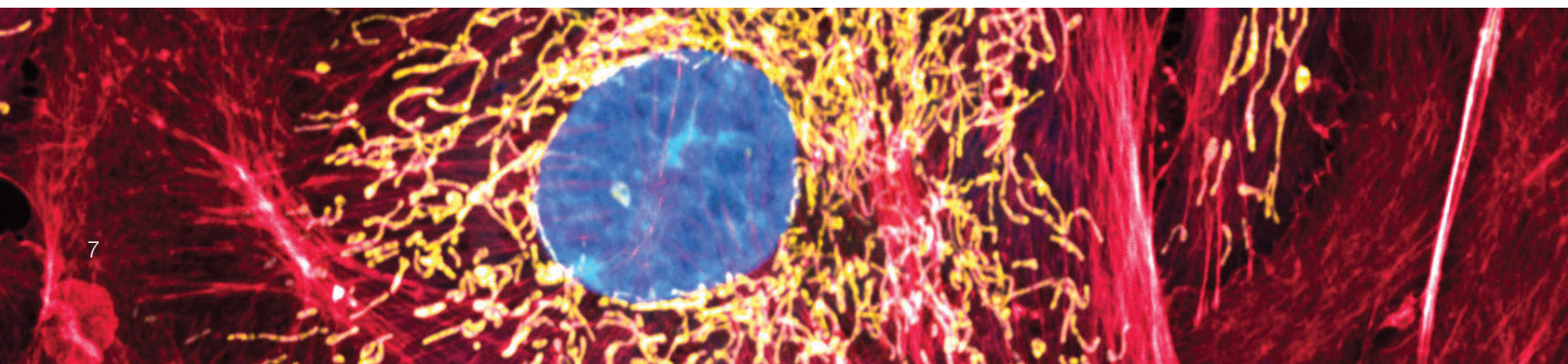
The Smart-Vue Pro solution is designed to log multiple types of activities, including audit trail information for user actions and system events. Audit records may include data modification events, user identifiers and timestamps. Smart-Vue Pro is designed not to intentionally transmit or store personal health information (PHI) or personally identifiable information (PII) in audit logs. However, the presence of such data may depend on customer configuration, user input or integration with external system.

Infrastructure and system logs may be aggregated and stored by our third-party partner with access managed by them in accordance with that provider's controls and policies. Thermo Fisher does not control third-party log storage environments and is not responsible for the security, availability or management of such third-party systems.

Network & endpoint security

For cloud deployments, the Smart-Vue Pro solution leverages AWS to host the supporting infrastructure. AWS is an independent third-party provider, and certain infrastructure and security controls are implemented and managed by AWS in accordance with its own policies and shared responsibility model.

Smart-Vue Pro production systems are hosted within an Amazon Virtual Private Cloud™ (Amazon VPC™) where network access is designed to be restricted such that only front-end services and device endpoints are externally accessible, based on system configuration. Network access is managed using AWS security groups and firewall rules that are configured to only allow required traffic.



In addition, AWS provides various services, including their threat monitoring service, Amazon GuardDuty™ and web application firewall (WAF) service, which may be used to support the protection of Smart-Vue Pro web applications and application programming interfaces (APIs).

For on-premises deployment, customers are responsible for configuring and managing their network controls. In accordance with cybersecurity best practices, Thermo Fisher recommends the use of firewalls, where applicable. Customers are permitted to configure firewall rules that allow only necessary traffic to and from Smart-Vue Pro infrastructure, aligning with business and IT requirements.

Antivirus/anti-malware

The cloud infrastructure supporting the Smart-Vue Pro software leverages an antivirus solution intended to help detect and mitigate malicious software using signature-based indicators of compromise through its threat database. The solution provides capabilities for real-time and on-demand scanning against file-based threats.

For on-premises deployments, Thermo Fisher recommends that customers implement and manage an antivirus solution in alignment with their business and IT requirements. If any technical issues arise, please contact your local Thermo Fisher support representative.

Data encryption

Data packets captured by the sensors and transmitted to the module communicate to the Smart-Vue Pro cloud infrastructure or on-premises server using either a LoRaWAN gateway or Bluetooth. If customers decide to communicate using the LoRaWAN gateway, the data packets are designed to be signed and encrypted using Advanced Encryption Standard (AES)-128. If the customer decides to use Bluetooth, the data packets are not encrypted. Customers are responsible for selecting communication methods and configurations appropriate to their security requirements. Thermo Fisher recommends that customers apply encryption controls in accordance with industry standard practices, where applicable.

Transmitted data being sent to and from the Smart-Vue Pro cloud platform communicates over Secure Socket Layer (SSL) connection using Transport Layer Security (TLS) v1.2.

Secure product development lifecycle

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 Smart-Vue Pro Product Management team reviews, evaluates and prioritizes security assessment findings based on criticality and a business risk management process and directs these findings to the third-party partner. Remediation activities are dependent on the third-party provider and applicable agreements.

Additional security measures may include leveraging a static analysis tool to scan code repositories, web applications and APIs, where applicable, as well as the third-party partner penetration testing to identify potential security vulnerabilities. The scope, frequency and results of such testing may vary and are not guaranteed.

The third-party partner develops and provides security updates and system patches throughout the lifecycle of the product and deploys them to the impacted environments based on factors such as criticality and a business risk management process. Software updates are typically released on a semiannual basis. Critical and high-severity security patches may be provided to customers as needed, based on risk and availability. Thermo Fisher does not guarantee the availability, timing or completeness of any security updates or patches.

For cloud deployments, Thermo Fisher generally provides advance notification of planned updates, after which customers may be required to take action such as downloading and installing the update. For on-premises deployments, updates may be performed onsite by a Thermo Fisher field service engineer.

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

Disaster recovery and business continuity

The Smart-Vue Pro solution includes data backup capabilities designed to reduce the risk of data loss and support the restoration of system functionality. Smart-Vue Pro is designed to provide notifications to customers when alarms are triggered, subject to system configuration and connectivity. The minimum time between incident detection and the initiation of investigation and potential service restart is 15 minutes. Accordingly, the optimal achievable Recovery Time Objective (RTO) is 15 minutes.

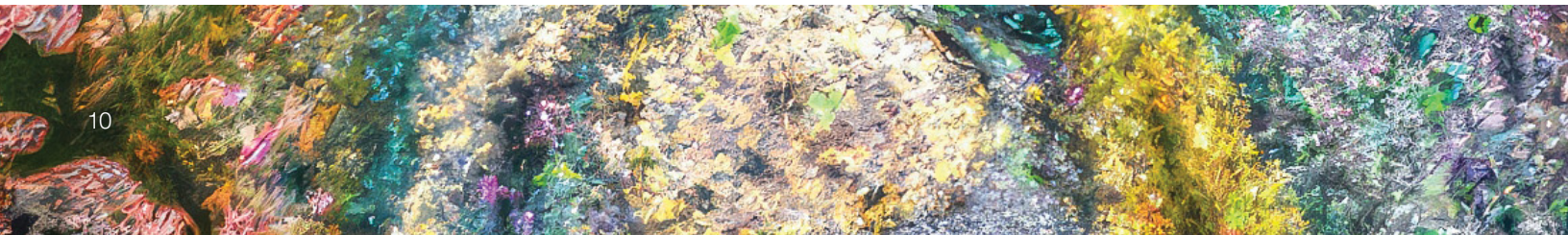
For cloud deployments, databases are typically backed up using AWS native backup services. Backups may occur multiple times per day and retention periods are up to 31 days. Backups are tested regularly to help ensure data integrity. Smart-Vue Pro databases hosted on AWS are backed up every 4 hours which makes the Recovery Point Objective (RPO) 4 hours. In the event of severe database corruption, the most recent backup may be used to restore the Smart-Vue Pro instance. Backup availability and restoration outcomes are not guaranteed and depend on system conditions and third-party services.

For on-premises deployments, customers are responsible for managing data backups in alignment with their business and IT requirements.

Service handling

Application-specific support and global training are intended to support the operation and use of the Smart-Vue Pro solution. 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.

Customers can request support for Smart-Vue Pro by contacting their local Thermo Fisher support representative.



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

CIS-SQRG-SVP-001