Product security information guide

Thermo Scientific OMNIC Paradigm software | version 2.8 | July 2026

Document valid through July 31, 2027

Introduction

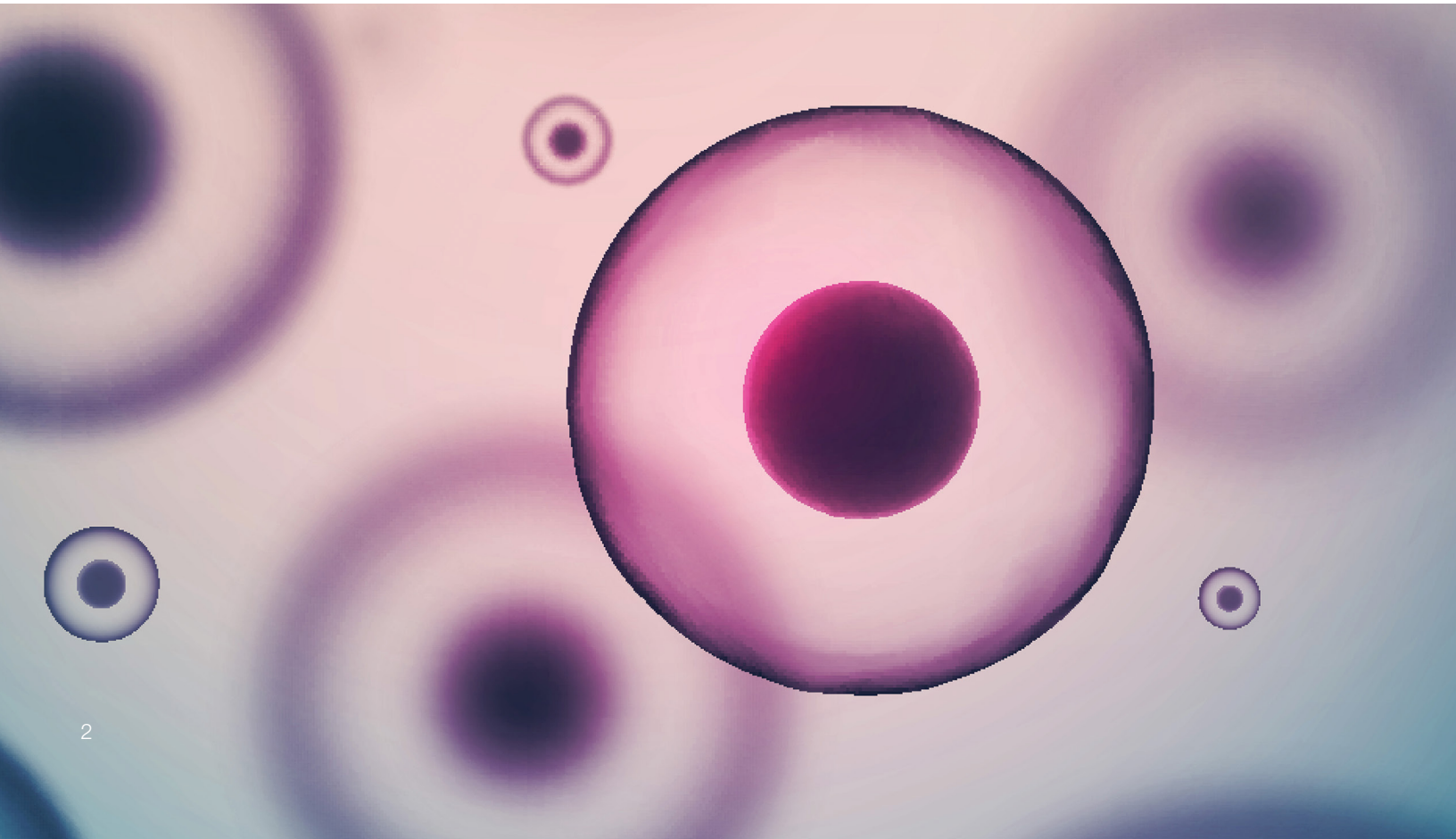
Thermo Fisher Scientific maintains a Cybersecurity Program which is designed to safeguard the confidentiality, integrity and availability of data and systems within our environment. Thermo Fisher supports a continuously improving security program model that is designed to focus on reducing risk, defending 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™ OMNIC™ Paradigm software version 2.8 against intrusion or data compromise. This document applies only to OMNIC Paradigm software version 2.8 deployed within the customer's environment. It describes the various standards, controls, data security approaches and business practices that Thermo Fisher 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, Thermo Fisher updates this product security information guide annually to ensure it contains current, accurate information. **This guide expires on July 31, 2027.** Contact your account representative or visit our information security website 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, 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.

Product overview

OMNIC Paradigm software is a cutting-edge package for molecular spectroscopy and microscopy that is designed to ease collecting, analyzing and interpreting data. It also allows customers to work remotely and collaborate with colleagues globally. The OMNIC Paradigm software is compatible with the following Fourier-transform infrared (FTIR) spectrometers:

- Nicolet™ Summit™ X
- Nicolet Summit LITE
- Nicolet Summit PRO
- Nicolet S5
- Nicolet iS20
- Nicolet iS50
- Nicolet iN5
- Nicolet Apex

Hardware specifications

Please refer to the Thermo Fisher Scientific Knowledge 1 website topic about Nicolet Spectrometers to locate the hardware specifications for the Thermo Fisher-provided computer dedicated to running OMNIC Paradigm software. The hardware specifications are dependent on the spectrometer and its setup.

System compatibility

OMNIC Paradigm software is compatible with the following supported operating systems:

- Microsoft™ Windows™ 10 when running on the companion PC or the embedded instrument PC; and
- Microsoft Windows 11 when running on the companion PC.

Thermo Fisher recommends that customers utilizing a companion PC running Windows 10 upgrade to Windows 11 at their earliest convenience. If a companion PC was purchased from Thermo Fisher, please contact your dedicated Sales Representative for more information on upgrading to Windows 11.

Note: The embedded computer within the Nicolet Summit **does not** currently support Windows 11. MariaDB™ is the default database used to store information produced from OMNIC Paradigm software. Microsoft SQL Server™, Amazon Aurora™ or Oracle™ databases also can be used. Customers are responsible for provisioning and configuring the database according to the instructions provided in the OMNIC Paradigm Software User Guide for the specific software version in use.

Regulatory compliance

The Security Suite add-on software provides enhanced capabilities to help protect the security and integrity of the data produced by OMNIC Paradigm software to help comply with the requirements of 21 CFR Part 11. There are two primary applications that comprise the Security Suite software: Security Administration and Audit Manager.

- The Security Administration application lets customers configure settings for access control, audit electronic records and manage electronic signatures.
- The Audit Manager application lets customers view logged security events (such as when a user logged on or when data was saved, for example), create reports and store logged events in the Audit Manager database. Audit trail capabilities for tagging, including tags created in workflows, are also supported through the Audit Manager application.

Please contact your Thermo Fisher Sales Representative for more information about purchasing Security Suite software.

OMNIC Paradigm system architecture diagrams

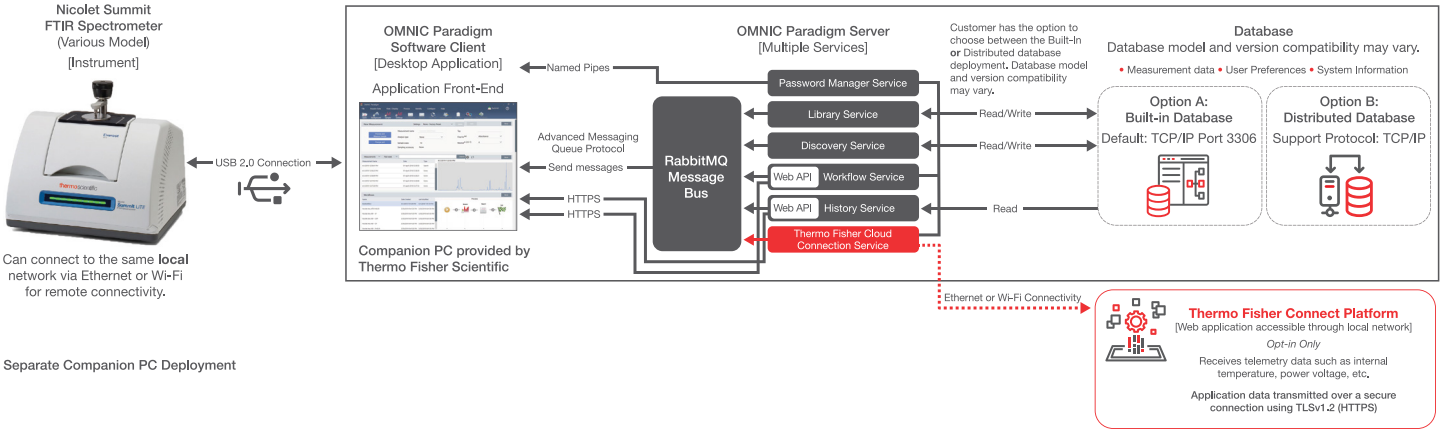


Figure 1: Separate companion PC deployment

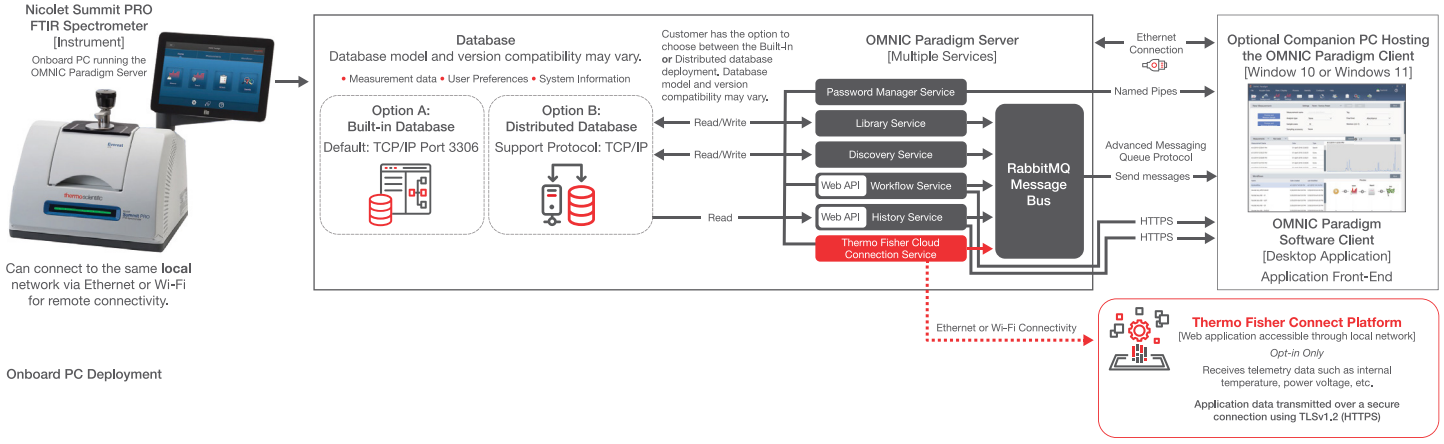


Figure 2: Onboard PC deployment

OMNIC Paradigm architecture diagrams component glossary

Component glossary

Component	Description
Companion personal computer (PC)	The Thermo Fisher-provided or customer-provided computer that hosts the complete OMNIC Paradigm software application. Customers can also utilize the companion PC to run the OMNIC Paradigm software client depending on the instrument setup and system configuration.
OMNIC Paradigm software client	Desktop application for OMNIC Paradigm software, supported on Windows 10 or Windows 11 when run on the companion PC.
OMNIC Paradigm server	Comprised of multiple services that transmit data to the application interface as well as read/write data to the built-in or distributed database. These services include the Password Manager service, Library service, Discovery service, Workflow service, History service and the Thermo Fisher Cloud Connection service.
RabbitMQ™ message bus	A messaging broker that acts as a common platform to send and receive messages between the OMNIC Paradigm software client and the back-end services using the Advanced Messaging Queue Protocol (AMQP).
Password Manager service	Provides credentials to the other back-end services using named pipes to allow for connection to the RabbitMQ message bus and the database.
Library service	Used to create, edit and search spectral libraries.
Discovery service	Automatically detects the instrument available on the network, allowing the customer to select the instrument they want to connect to.
Workflow service	Used to create, edit and run OMNIC Paradigm workflows. Customers can also utilize the Web API exposed over Hypertext Transfer Protocol Secure (HTTPS) to initiate and control OMNIC Paradigm workflows.
History service	Used to gather previous measurement data from the database, such as spectral data and results of quantitative analysis. The History service utilizes a web application programming interface (API) connection over HTTPS to collect prior measurement data.
Thermo Fisher Cloud Connection service	Used for those customers that opt in to send telemetry data, such as internal temperature and power voltages, to the Thermo Fisher Connect Platform.
Database	Stores information, including measurement data, user preferences and system information pertaining to OMNIC Paradigm software. Customers can use the built-in MariaDB database or configure a compatible alternative, such as SQL Server, Aurora or Oracle database, to meet their business needs.
Thermo Fisher Connect Platform	An optional component: Customers can opt in to send telemetry data to the Thermo Fisher Connect Platform to analyze data anytime, anywhere. Security features within the Thermo Fisher Connect Platform are not in scope for this document.

Table 1: Component glossary

System access controls

Authentication

Authentication to OMNIC Paradigm software and the spectrometers is administered via domain authentication or standard Windows authentication on the Thermo Fisher-provided computer or the embedded PC. The default mechanism utilizes standard local Windows authentication to access OMNIC Paradigm software. Customers can use their own devices to manage the software; however, the customer is responsible for configuring authentication in accordance with their policies and procedures.

Customers can also use domain authentication to authenticate users through their domain credentials. OMNIC Paradigm software validates the user-provided credentials on domain controllers on the customer's network. Once the domain controller performs the validation, the user authenticates into OMNIC Paradigm software. For customers using domain authentication with the Security Suite software, role-based access control can be leveraged to assign specific permissions to validated users.

Although OMNIC Paradigm software can run using the Windows administrator account, Thermo Fisher recommends that a standard Windows user account be configured to manage OMNIC Paradigm software to limit permissions in accordance with the principle of least privilege. Please refer to the Authorization section for more information about the principle of least privilege.

Authorization

Using Security Suite, OMNIC Paradigm software leverages role-based access control (RBAC) to grant permissions and access to authorized users, where roles are configurable to meet necessary business requirements. Thermo Fisher recommends that role assignments be configured using the principle of least privilege providing only required system access needed to manage OMNIC Paradigm software and the supported instruments.

Firewall/network controls

Installation of OMNIC Paradigm software includes updates to the firewall configuration on the customer-provided or Thermo Fisher-provided PC to allow the connection between the OMNIC Paradigm client and the back-end services. No additional firewall modifications are required for the function of the OMNIC Paradigm software. A complete list of the back-end services and their corresponding ports can be found within the OMNIC Paradigm Software User Guide.

Thermo Fisher recommends configuring firewall rules to allow necessary traffic to OMNIC Paradigm software in accordance with the specific ports listed in the OMNIC Paradigm Software User Guide.

Additionally, Thermo Fisher recommends closing any unused ports to limit connections and follow industry standard practices and business requirements.

Password management

Thermo Fisher recommends that password requirements follow industry standard practices. For customers leveraging the standard Windows authentication mechanism, OMNIC Paradigm software provides functionality for configuring passwords adherent to organizational security requirements. For customers leveraging domain authentication, the password policy requirements are those set by the customer's domain controllers.

During OMNIC Paradigm software installation, the installer resets the root password for RabbitMQ and MariaDB, silently prompting the software to create strong, randomly generated passwords to access these critical back-end services.

Remote support

Customers initiate remote support for OMNIC Paradigm software and the supporting instrument by contacting technical support in their region. If the technical support representative recommends that troubleshooting can be provided remotely, the representative will establish a remote session with the customer using a Thermo Fisher-managed and approved third-party remote support solution.

Thermo Fisher maintains internal policies and procedures that govern the secure storage, retention and disposal of any customer data obtained through a remote support session.

Logging

OMNIC Paradigm software logs multiple types of activities, including user actions, software system events and instrument events to evaluate system performance and document specific user tasks. In addition, OMNIC Paradigm software uses a built-in event store as the auditing mechanism to track and monitor activities, particularly for data acquisition and processing-related events.

Secure connectivity

Separate companion PC deployment

Separate companion PC application connectivity

Assets	Secure connection
OMNIC Paradigm server to software client	The three primary services that connect the OMNIC Paradigm server with the OMNIC Paradigm client are RabbitMQ message bus, Password Manager service and a web API exposed by the History service. AMQP, named pipes and HTTPS are the protocols used to transmit data from the server to the OMNIC Paradigm software client, all occurring within the companion PC.
OMNIC Paradigm server to built-in database	The OMNIC Paradigm server connects to the built-in database through a TCP/IP connection. The Password Manager service within the OMNIC Paradigm server manages the credentials used to connect to the built-in database. Please reference the "System Compatibility" section for a complete list of compatible databases.
OMNIC Paradigm server to distributed database	Customers can configure the OMNIC Paradigm server to connect to their chosen distributed database through a TCP/IP connection. Currently, the OMNIC Paradigm server can only support a TCP/IP connection, requiring the database hostname, the desired TCP/IP port and valid credentials. The OMNIC Paradigm server supports the use of Integrated Windows Authentication (IWA).

Table 2: Separate companion PC application connectivity

Separate companion PC hardware connectivity

Assets	Secure connection
Companion PC to instrument	The instrument connects to the companion PC through a direct USB 2.0 connection where OMNIC Paradigm software performs data analysis entirely on the companion PC. Thermo Fisher recommends that customers restrict physical access to the instrument and companion PC to ensure a stable and secure connection.
Companion PC to Thermo Fisher Connect Platform	The companion PC can connect to the Thermo Fisher Connect Platform through an Ethernet or Wi-Fi connection. Customers can opt in to send telemetry data (such as internal temperatures and power voltages) to the Thermo Fisher Connect Platform, but the connection is not required for normal functionality of OMNIC Paradigm software. Thermo Fisher recommends that customers configure wireless connectivity to leverage either the WPA2 or WPA3 standard for authentication if establishing a connection through Wi-Fi.

Table 3: Separate companion PC hardware connectivity

Onboard PC deployment

Onboard PC application connectivity

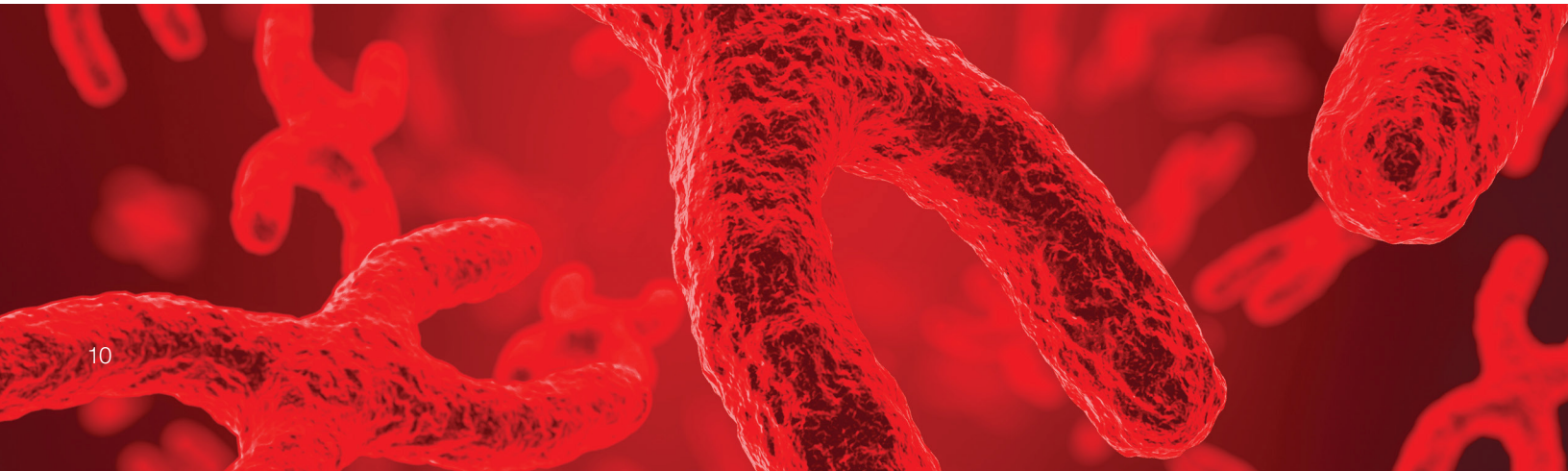
Assets	Secure connection
OMNIC Paradigm server to software client	The three primary services that connect the OMNIC Paradigm server with the OMNIC Paradigm software client are RabbitMQ message bus, Password Manager service and a web API exposed by the History service. AMQP, named pipes and HTTPS are the protocols used to transmit data from the embedded PC running the OMNIC Paradigm server to the OMNIC Paradigm software client on the external companion PC.
OMNIC Paradigm server to built-in database	OMNIC Paradigm server connects to the built-in database through a TCP/IP connection. The Password Manager service within the OMNIC Paradigm server manages the credentials used to connect to the built-in database. Please reference the “System Compatibility” section for a complete list of compatible databases.
OMNIC Paradigm server to distributed database	Customers can configure the OMNIC Paradigm server to connect to a distributed database of their choosing through a TCP/IP connection, requiring the hostname of the database, the desired TCP/IP port and valid credentials. The OMNIC Paradigm Server supports the use of IWA.

Table 4: Onboard PC application connectivity

Onboard PC hardware connectivity

Assets	Secure connection
Instrument with embedded PC to companion PC	An external companion PC can be connected to an instrument with an embedded PC through an Ethernet connection. This allows customers to host the OMNIC Paradigm software client on the external PC for data analysis as well as connect the instrument to the customer’s network for remote connectivity, if desired. Thermo Fisher recommends that customers restrict physical access to the instrument and companion PC to ensure a stable and secure connection.
Instrument with embedded PC to Thermo Fisher Connect Platform	The instrument with an embedded PC can connect to the Thermo Fisher Connect Platform through an Ethernet or Wi-Fi connection. Customers can opt in to send telemetry data (such as internal temperatures and power voltages) to the Thermo Fisher Connect Platform, but the connection is not required for normal functionality of OMNIC Paradigm software. Thermo Fisher recommends that customers configure wireless connectivity to leverage either the WPA2 or WPA3 standard for authentication if establishing a connection through Wi-Fi.

Table 5: Onboard PC hardware connectivity



Data encryption methods

Encryption at rest

By default, the data generated from OMNIC Paradigm software is stored in the local MariaDB. Thermo Fisher recommends that customers enable encryption capabilities offered within MariaDB or the database they choose to encrypt data at rest. Refer to instructions in the vendor-specific documentation for configuring encryption mechanisms for the selected database.

Encryption in transit

Data produced from OMNIC Paradigm software is transferred from the instrument to the companion PC or onboard computer via RabbitMQ. The RabbitMQ connection delivers traffic using Secure Sockets Layer (SSL)/Transport Layer Security (TLS) encryption. Telemetry data sent from OMNIC Paradigm software to the Thermo Fisher Connect Platform uses a secure HTTPS connection, leveraging TLS encryption version 1.2.

Certificates

OMNIC Paradigm software version 2.8 supports customers who want to import an existing SSL certificate through the OMNIC Paradigm configuration utility. This service is intended for administrator use only. The default configurations should be utilized unless the customer's organizational policy states otherwise.

Secure product development lifecycle

Secure software development training

Software development training is available to the OMNIC Paradigm 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 colleague, and regularly educate and share industry leading 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 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 OMNIC Paradigm 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 OMNIC Paradigm software are stored and maintained in a Thermo Fisher-approved artifact management solution. This provides visibility and control on developed software builds, enabling the OMNIC Paradigm 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 OMNIC Paradigm Software Development team utilizes a Thermo Fisher-approved static analysis tool that scans code repositories during each code commit. This tool helps identify potential security defects, maintain code quality and integrity and allow for prompt review and prioritization of security alerts for remediation based on criticality and a business risk management process.

Peer code reviews

The OMNIC Paradigm Software Development team conducts manual peer reviews of code before testing and deployment. These reviews provide additional insights into the overall context and business logic of the code, complementing the information gathered from the static analysis tool.

Penetration tests

Thermo Fisher's Penetration Testing team tests core components of the Nicolet Summit and OMNIC Paradigm software against the Open Worldwide Application Security Project (OWASP) Top 10 Internet-of-Things (IoT) list. The team, comprised of trained penetration testers, 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

Vulnerability and patch management

The OMNIC Paradigm Software 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.

Thermo Fisher recommends validating and applying patches to impacted OMNIC Paradigm software versions upon notification, keeping applicable systems up to date and minimizing risk associated with vulnerabilities. Thermo Fisher recommends that customers utilize our Reporting Security Issues form to report suspected or potential security issues.

Disaster recovery and business continuity

OMNIC Paradigm software has data backup capabilities to prevent data loss and aid in restoring normal functionality. Thermo Fisher suggests that customers leverage these backup capabilities and include them in Disaster Recovery plans and testing in accordance with their policies. Thermo Fisher also suggests performing regular file system and database backups with laboratory managers and IT administrators in accordance with policy.

System hardening

System hardening, a critical security function, can mitigate potential exploitation of system vulnerabilities and prevent potential threats. The OMNIC Paradigm Software Development team uses system hardening practices prior to deployment, including:

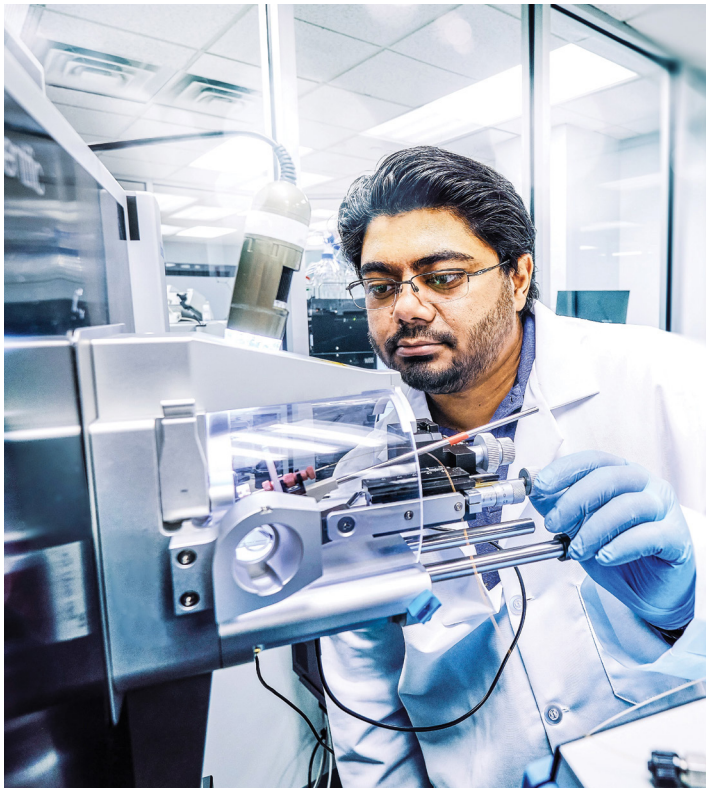
- Running Windows 10 hardening scripts derived from the Center for Internet Security (CIS) hardening guides on Thermo Fisher-provided computers as well as the onboard computer associated with Nicolet Summit Pro instruments;
- Disabling Microsoft PowerShell™ on Thermo Fisher-provided computers; and
- Installation of Microsoft Windows Defender™ as the default antivirus solution for the onboard computer.

Thermo Fisher recommends maintaining operating systems and network hardening practices on relevant infrastructure supporting the use of OMNIC Paradigm software.

Service handling

Application-specific support and training serve as critical components to deploying and supporting your spectrometer and associated software. 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.

Technical support for OMNIC Paradigm is provided through Unity Lab Services. Customers can engage Unity Lab Services by submitting a technical support request ticket through the Services Central web portal (login required).



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

269-366500C