Product Security Information Guide

OMNIC™ Paradigm Software | Version 2.3 | September 2023

Document valid through September 1, 2024

Introduction

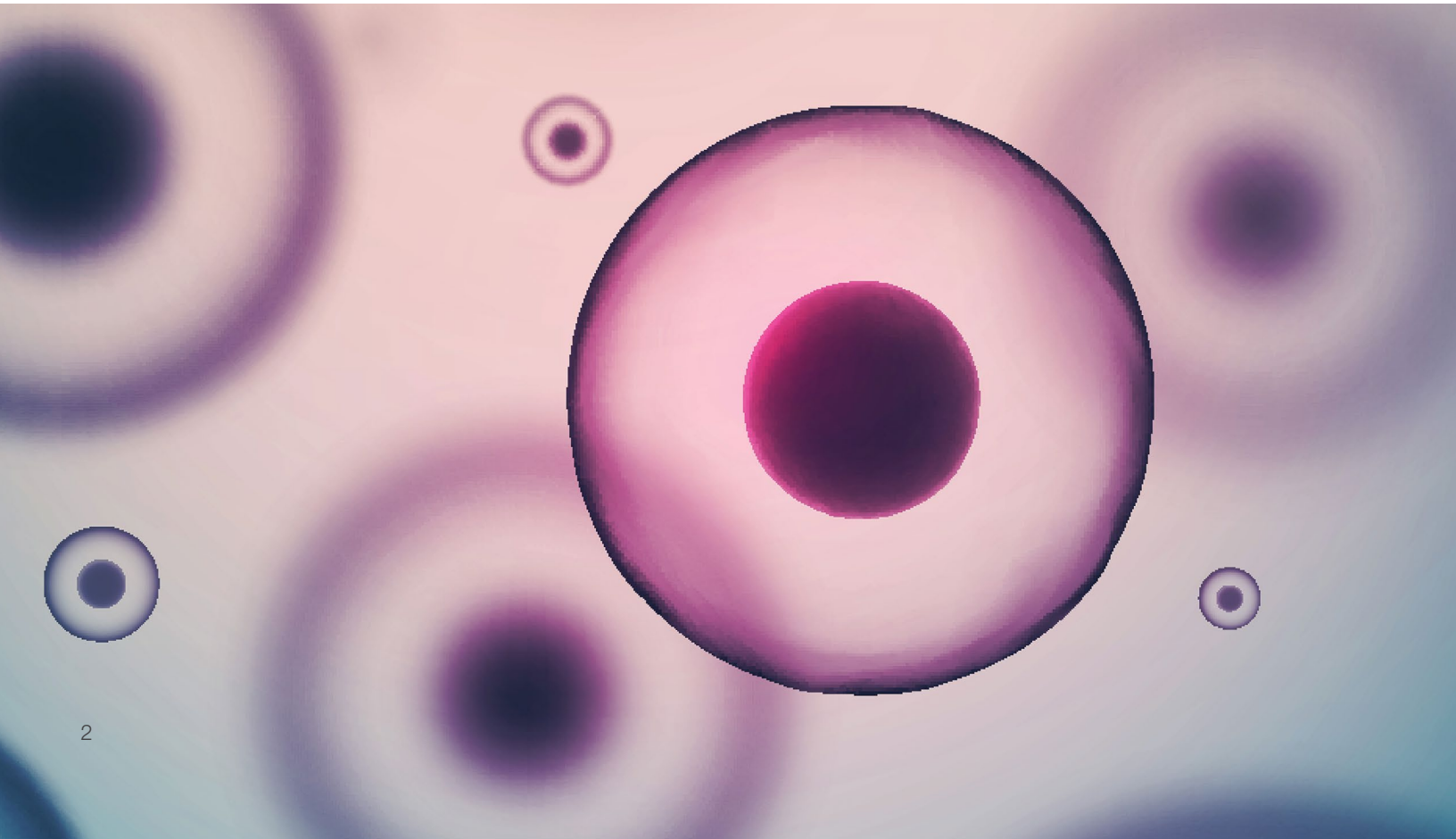
Thermo Fisher Scientific maintains a Cybersecurity Program, led by a dedicated Chief Information Security Officer (CISO), designed to safeguard the confidentiality, integrity, and availability of data and systems within our environment. Thermo Fisher Scientific supports a continuously improving security 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 OMNIC Paradigm Software Version 2.3 against intrusion or data compromise. This document applies only to OMNIC Paradigm Software Version 2.3 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, Thermo Fisher Scientific updates this Product Security Information Guide annually to ensure it contains current, accurate information. **This guide expires on September 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

Cybersecurity Program and leadership

Thermo Fisher Scientific maintains a Cybersecurity Program that includes technical, administrative, and physical safeguards designed to detect vulnerabilities and address 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

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

- NICOLET Summit™ X
- NICOLET Summit LITE
- NICOLET Summit PRO
- NICOLET iS5™
- NICOLET iS20™
- NICOLET iS50™

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 Scientific-provided computer dedicated to running OMNIC Paradigm Software. The hardware specifications are dependent on the spectrometer and its setup.

System compatibility

OMNIC Paradigm Software runs on the following supported operating systems:

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

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 you configure settings for access control, audit electronic records, and manage electronic signatures.
- The Audit Manager application lets you 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.

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

OMNIC Paradigm system architecture diagrams

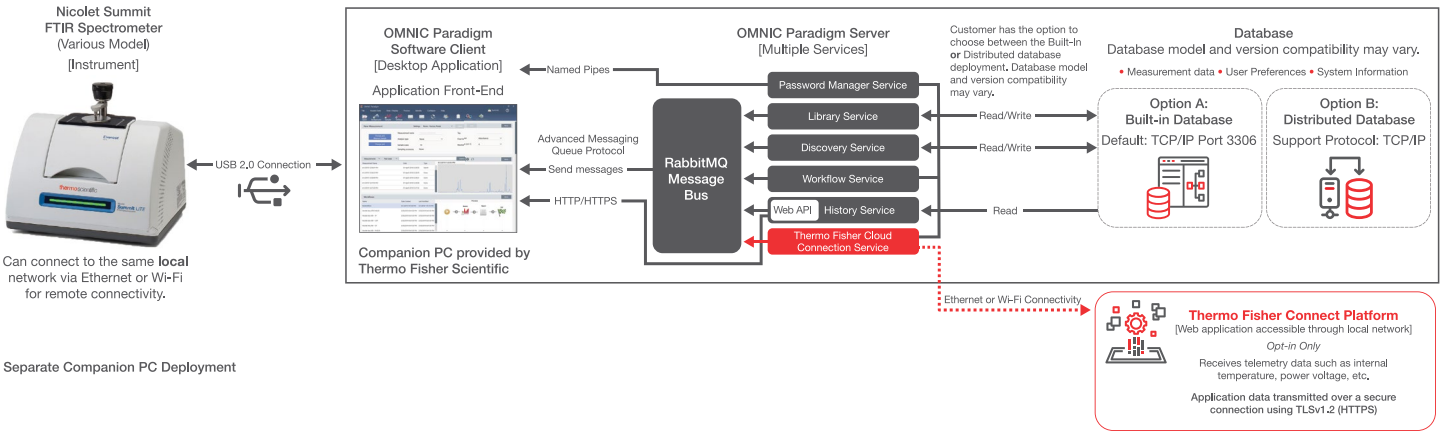


Figure 1: Separate companion PC deployment

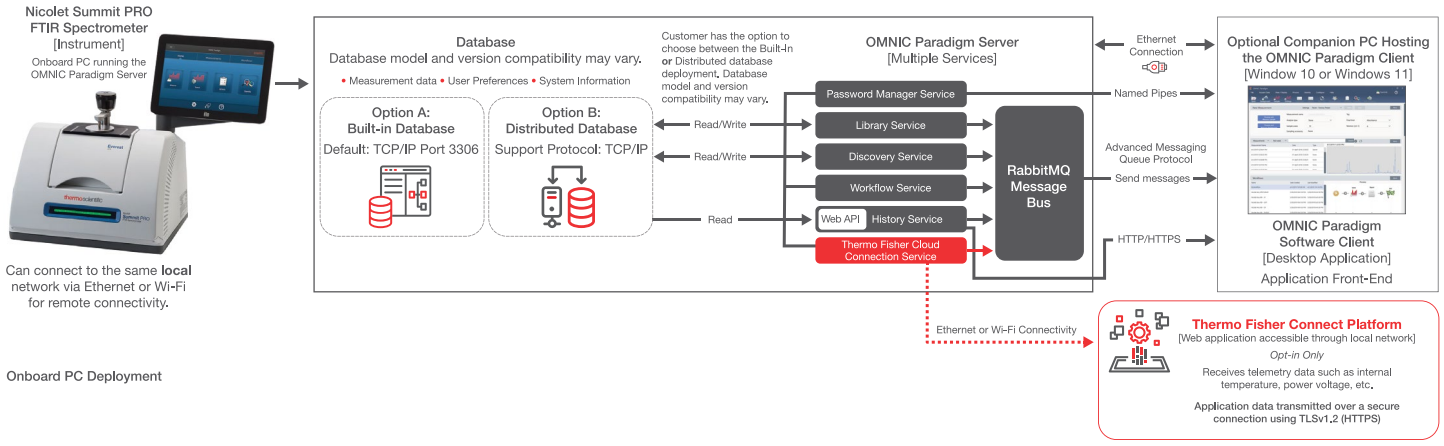


Figure 2: Onboard PC deployment

OMNIC Paradigm architecture diagrams component glossary

Component glossary

Component	Description
Companion Personal Computer (PC)	The Thermo Fisher Scientific-provided or customer-provided computer that hosts the complete OMNIC Paradigm Software application. Customers also can 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.
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 Hypertext Transfer Protocol (HTTP) to collect prior measurement data. While information being transmitted does not contain any sensitive data, including credentials or individually identifiable health information, any content transmitted over HTTP is compressed into binary form to obscure the 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 Scientific-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 Scientific 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 Scientific 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 Scientific-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 Scientific recommends configuring firewall rules to allow only necessary traffic to OMNIC Paradigm Software in accordance with the specific ports listed in the OMNIC Paradigm Software User Guide.

Password management

Strong password creation, structure, and renewal policies can help prevent unauthorized system access. 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.

Thermo Fisher Scientific recommends that password requirements follow organizational or industry best practices.

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 Scientific-managed and approved third-party remote support solution.

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

Logging

Auditing and recording system user activities and processes are critical security functions. 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 HTTP 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 hostname of the database, 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 Scientific recommends that customers restrict physical access to the instrument and companion PC to ensure a more 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 Scientific 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

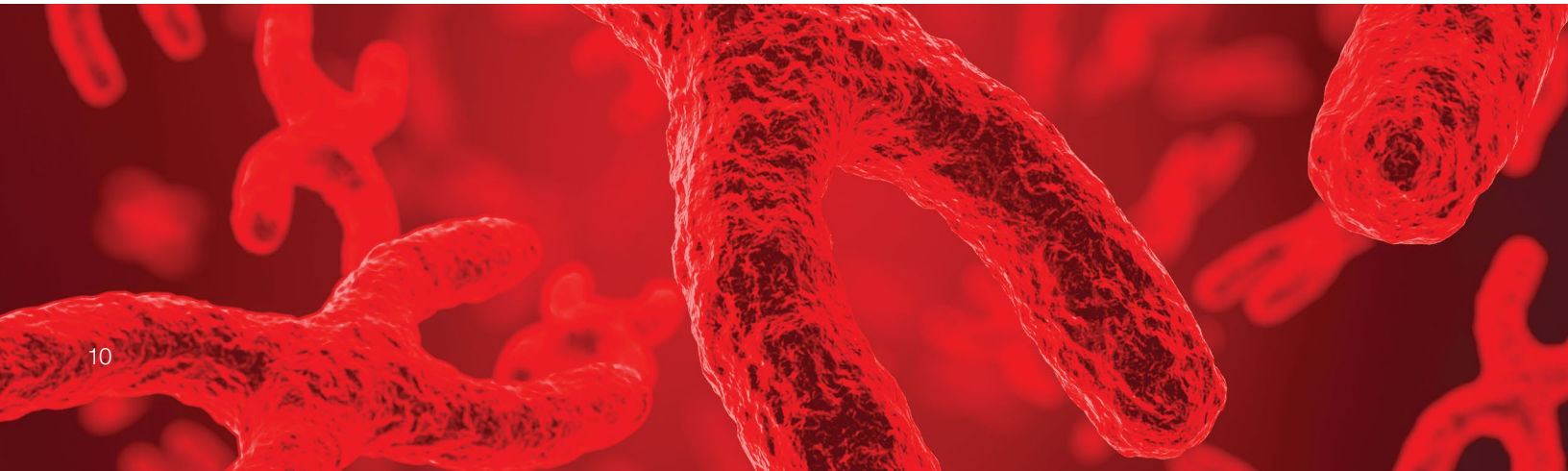
Assets	Secure connection
OMNIC Paradigm Server to Software Client	The three primary services that connect the OMNIC Paradigm Server with the OMNIC Paradigm client are RabbitMQ Message Bus, Password Manager Service, and a web API exposed by the History Service. AMQP, named pipes, and HTTP are the protocols 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 Scientific 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 Scientific 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



Ports and protocols

Various system services are used to run OMNIC Paradigm Software. A complete list of the services, with a description of each service, can be found within the OMNIC Paradigm Software User Guide.

Thermo Fisher Scientific recommends closing any unused ports to limit connections and follow industry standards and best practices. Thermo Fisher Scientific also recommends confirming that the ports listed in the OMNIC Paradigm Software User Guide allow traffic if issues arise while connecting to a spectrometer.

Data encryption methods

Encryption at rest

By default, the data generated from OMNIC Paradigm Software is stored in the local MariaDB. Thermo Fisher Scientific recommends that customers enable encryption capabilities offered within MariaDB or the database of their choosing 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.

Secure product development lifecycle

Secure software development training

The OMNIC Paradigm Software Product Development team completes secure software development training to further 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 Product Development team reviews, evaluates, and prioritizes security assessment findings for remediation and acts on them based on criticality.

Source code management

OMNIC Paradigm Software source code is stored in a Thermo Fisher Scientific-approved version control solution that has no public exposure or access and 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 OMNIC Paradigm Software Product Development team stores and maintains software artifacts including, but not limited to, executables, images, and libraries 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 OMNIC Paradigm Software 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. Conducting a static analysis scan benefits our customers by evaluating code quality and integrity through the increased efficiency of code reviews. The development team reviews and prioritizes security alerts for remediation based on criticality.

Peer code reviews

The OMNIC Paradigm Software Product Development team conducts manual peer reviews of code before testing and deployment into a product. Manual code reviews provide benefit by accounting for the overall context and business logic in which the code was developed, which supplements findings from the static analysis tool.

Penetration tests

Thermo Fisher Scientific’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 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. Assessments of third-party vendors and service providers are critical 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 OMNIC Paradigm Software 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. The team evaluates and schedules updates containing fixes to critical and high-priority vulnerabilities for immediate remediation.

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

Disaster recovery and business continuity

OMNIC Paradigm Software has data backup capabilities to prevent data loss and aid in restoring normal functionality. Thermo Fisher Scientific suggests that customers leverage these backup capabilities and include them in Disaster Recovery plans and testing in accordance with their policies. Thermo Fisher Scientific 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 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 Scientific-provided computers as well as the onboard computer associated with Nicolet Summit Pro instruments.
- Disabling Microsoft PowerShell™ on Thermo Fisher Scientific-provided computers.
- Installation of Microsoft Windows Defender™ as the default antivirus solution for the onboard computer.

Thermo Fisher Scientific 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 Scientific'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

269-363500A