Product security information guide

Invitrogen EVOS S1000 Spatial Imaging System | January 2026

Document valid through January 31, 2027

Introduction

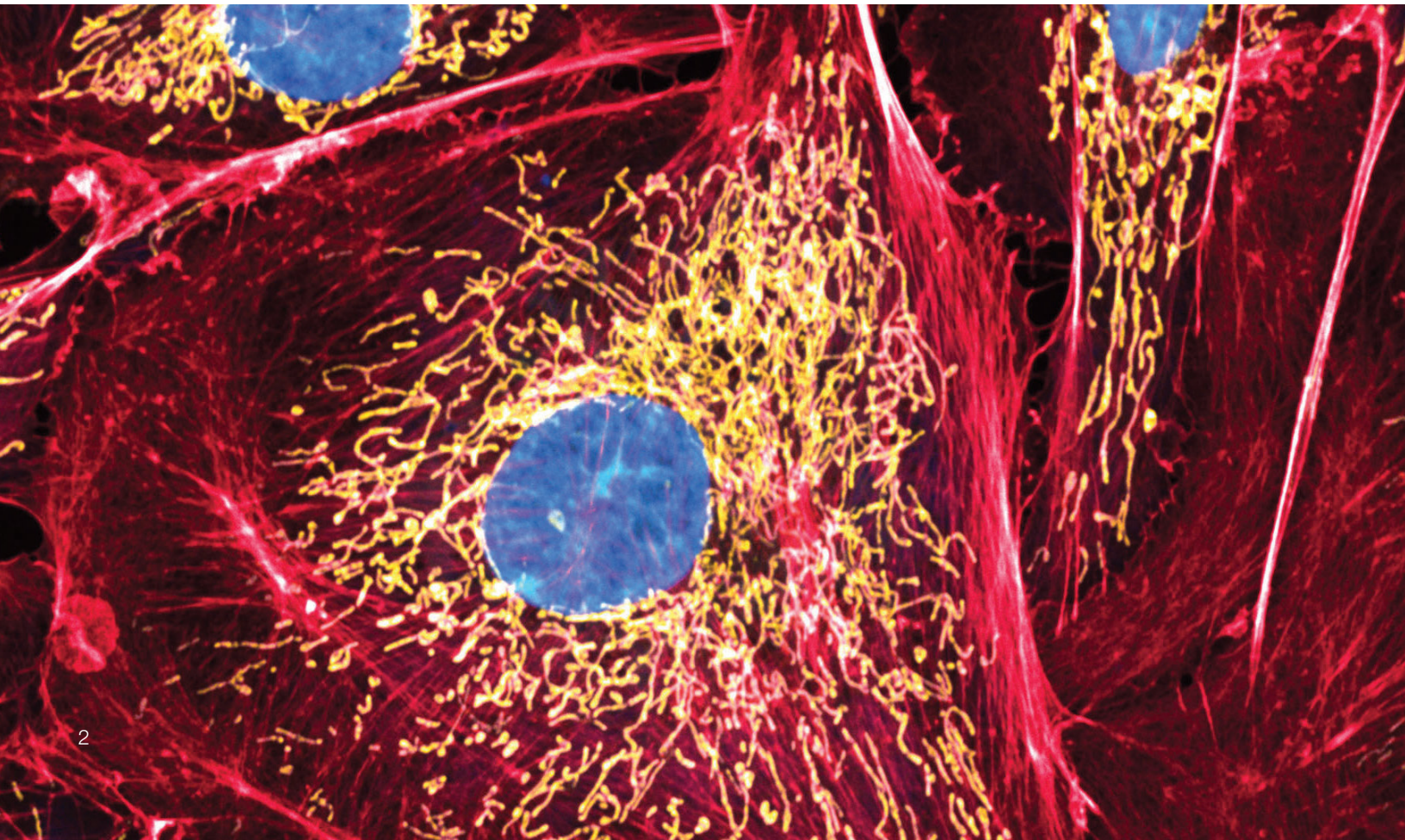
Thermo Fisher Scientific maintains a Cybersecurity Program which is designed to safeguard the confidentiality, integrity and availability of data and systems within our environment. Thermo Fisher supports a continuously improving security program model that has measures designed to focus on reducing 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 has implemented safeguards and protections designed to help protect the Invitrogen™ EVOS™ S1000 Spatial Imaging System against intrusion or data compromise. This document describes the various standards, controls and data security approaches and business practices that Thermo Fisher uses in this effort.

Due to the ever-changing cyber landscape, Thermo Fisher updates this product security information guide annually to maintain current and accurate information. This guide expires on **January 31, 2027.** Contact your account representative to get 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 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

The Invitrogen EVOS S1000 Spatial Imaging System is designed to deliver precision, ease of use and high-resolution imaging for tissue samples in life science research laboratories focusing on translational research. The system supports a range of transmitted light and fluorescence imaging applications for use in spatial proteomics research workflows.

The EVOS S1000 Spatial Imaging System is a widefield spectral imaging system that combines multiplex spectral fluorescence, transmitted brightfield and color brightfield detection. Coupled with the Invitrogen™ EVOS™ Imaging software, it provides seamless image processing, single-round spectral unmixing of up to 8-plex (+ nuclei detection) and powerful image visualization all within a user-friendly platform. The spectral unmixing software enables the EVOS S1000 Spatial Imaging System to image a single round of 9-plex multiplex immunofluorescence faster than instruments which rely on cyclic technology. The EVOS S1000 Spatial Imaging System can be used by scientists in the spatial biology field, including those specializing in cancer biology, histology, immunology, neurobiology and those who require highly resolved images.

Hardware specifications

- EVOS S1000 instrument
  - High-resolution LED-based imaging system
  - USB 3.0 port
- Operating Conditions
  - Temperature: 66° to 77°F (19° to 25°C)
  - Humidity: < 80% humidity (non-condensing)
- Dimensions (W x D x H)
  - 22 in. x 23 in. x 23 in. (56 cm x 58 cm x 58 cm)
- Weight
  - 118 lbs. (54 kg)
- Companion PC specifications
  - External Dell™ XE4 PC 12th generation Intel Core™ i9-12900 processor
  - 128GB DDR4 RAM
  - NVIDIA™ Quadro RTX™ A4000 graphics card
  - 2 x 8TB SSDs for data storage and 512GB SSD for the operating system
  - Support for USB memory stick, network drive and cloud storage
  - Output ports: 2 USB-A 2.0 ports, 4 USB-A 3.1 Gen 1 ports, 1 USB-C 3.1 Gen 2 port and an Ethernet port

System compatibility

The EVOS S1000 companion PC is compatible with the Microsoft™ Windows™ 10 IoT Enterprise LTSC (version 21H2) operating system. Upgrading the PCs to Windows 11 is not currently supported.

Microsoft may provide security updates for this operating system until January 2032, but Microsoft will not provide new features or technical support. Thermo Fisher recommends that customers maintain their existing Windows operating system and contact their support representative for assistance in updating, if necessary. For more information, please see Microsoft's Windows 10 - release information | Microsoft Learn.

Regulatory compliance

The EVOS S1000 Software Development team utilizes a Quality Management System (QMS) aligned with ISO 9001 standards that encompasses policies and procedures including, but not limited to, disaster recovery, data backup and recovery, business continuity, data security and change management procedures.

Architecture diagram

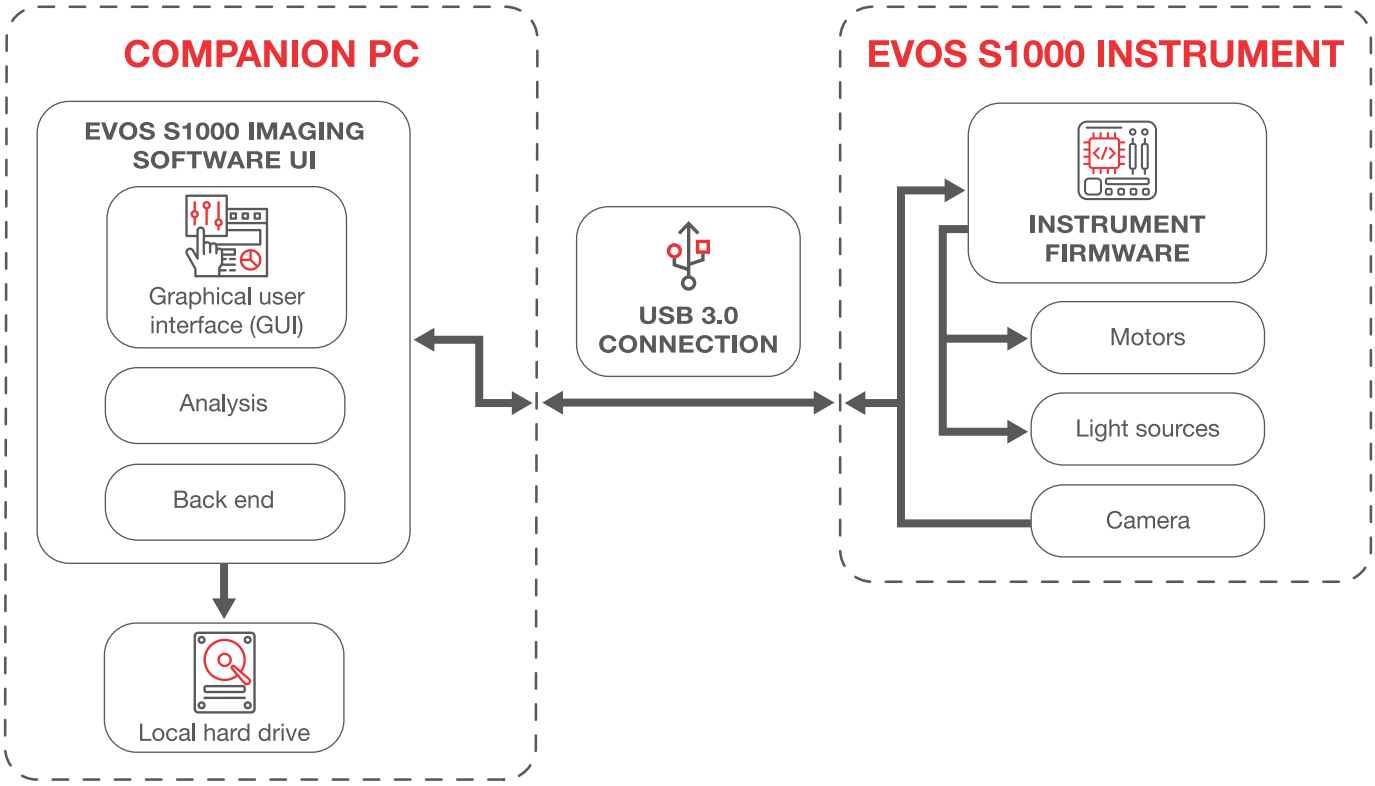


Figure 1: EVOS S1000 architecture diagram

Component glossary

The EVOS S1000 Spatial Imaging System features the following components (shown in the architecture diagram).

Component	Description
Companion PC	The instrument is controlled from a PC with the preinstalled EVOS S1000 Imaging software. The companion PC can be set up for a customer network environment (for example, network drive access). Thermo Fisher recommends limiting modifications to the companion PC to approved updates provided by Thermo Fisher to support reliable system operation.
EVOS S1000 imaging software	EVOS S1000 Imaging software controls the EVOS S1000 Spatial Imaging System. The software consists of a graphical user interface (GUI), back end and analysis library.
EVOS S1000 instrument	A USB 3.0 cable connects the instrument to the companion PC. The instrument consists of firmware running instrument light sources and motors and features a camera that provides images to the companion PC.

Table 1: EVOS S1000 component glossary

System access controls

Authentication

The companion PC administers authentication to EVOS S1000 instrument and includes 4 user accounts: ABService, Administrator, INSTR-ADMIN and INSTR-USER.

- The ABService account is designated for service personnel and includes tools such as service and calibration software.
- The Administrator account is intended for customer IT staff to make system configuration changes, such as installing software updates, without modifying the customer's desktop environment.
- The INSTR-ADMIN account is reserved for the principal investigator or lab administrator to perform administrative tasks within the software application, such as installing updates.
- The INSTR-USER account is intended for standard operation of the software application.

Each account is provisioned with a default password. Users are required to change their password upon first login. Credentials for these 4 accounts are created during instrument setup and are the customer's responsibility to manage thereafter.

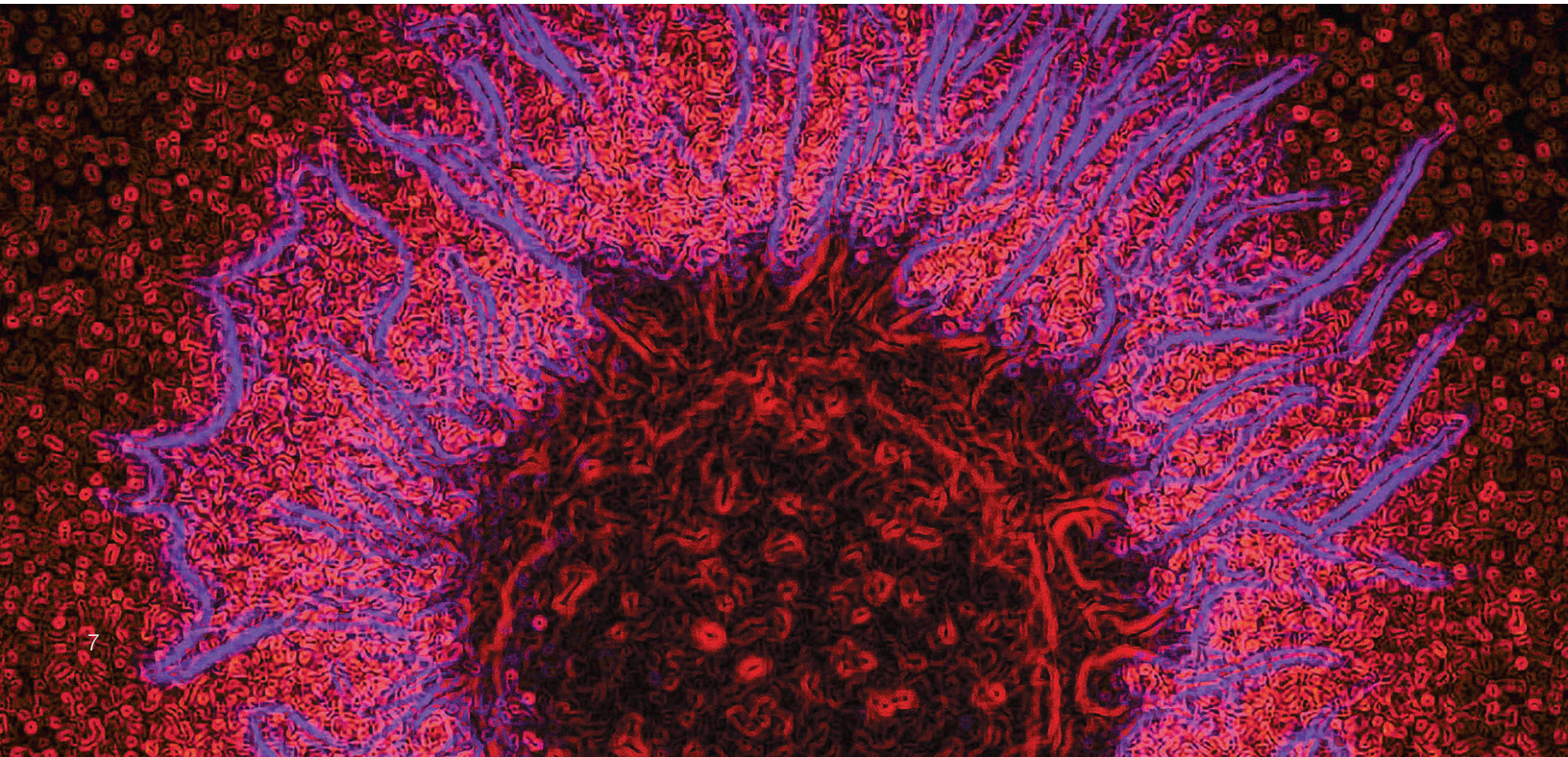
Authorization

The companion PC managing the EVOS S1000 instrument 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 follow the principle of least privilege, providing only the required system access needed to manage or use the EVOS S1000 Spatial Imaging System.

Firewall and network controls

The EVOS S1000 instrument does not require network connectivity for normal operation. Customers who wish to configure network connectivity can enable Windows Firewall on the companion PC.

In alignment with cybersecurity best practices, Thermo Fisher recommends implementing firewalls where applicable. Customers are permitted to configure firewall rules that allow only necessary traffic to and from the EVOS S1000 companion PC, aligning with business and IT requirements.



Thermo Fisher recommends maintaining network hardening practices on relevant infrastructure supporting the use of the EVOS S1000 Spatial Imaging System.

Password management

Customers are responsible for managing computer access passwords for user accounts in accordance with their internal policies as applicable. Thermo Fisher does not retain copies of customer-created passwords during initial user account setup.

Thermo Fisher recommends that password requirements follow industry standard practices.

Remote support

Customers initiate remote support for the EVOS S1000 Spatial Imaging System 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. For more information about this solution, please refer to our security flyer.

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

Logging

The EVOS S1000 Spatial Imaging System logs multiple types of activities, including instrument information (such as serial number and software/firmware version), application events, communication between the instrument and the software application and warning and error messages. These logs assist in evaluating system performance and documenting specific instrument and software tasks.

By default, log files produced by the EVOS S1000 Spatial Imaging System are stored locally with customer-managed access. A troubleshooting package (.zip file) can be generated through the EVOS S1000 Spatial Imaging Software by navigating to **Settings > Service > Create Troubleshoot Package.** This package can then be shared with Thermo Fisher technical service personnel to support troubleshooting activities.

Data storage and encryption methods

By default, data generated from results on the EVOS S1000 instrument is stored on the companion PC. Customers can enable encryption capabilities through Microsoft BitLocker™ to encrypt data at rest. BitLocker leverages the Trusted Platform Module chip within the PC and supports AES-128 encryption by default, with the option to configure AES-256 to meet organizational requirements.

Note: Running BitLocker concurrently with instrument operation may result in system errors. Customers should refer to Microsoft Windows documentation for guidance on configuring BitLocker encryption, available under the Windows Support pages for "Windows security, safety, and privacy."

Secure product development lifecycle

Secure software development training

Software development training is available to the EVOS S1000 Product 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 employee, and Thermo Fisher regularly has educational programs to share best practices and to raise awareness of cybersecurity threats. Thermo Fisher accomplishes this through a security awareness training program, including regular exercises and periodic cyber-event simulations.

Product security assessments

Products, instruments, software and devices undergo customized 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 EVOS S1000 Product 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

EVOS S1000 source code is stored in a Thermo Fisher-approved version control solution that contains built-in redundancy to support data loss prevention. Continuous integration is in use, automating the implementation of changes made to the code.

Artifact management

Software artifacts including, but not limited to, executables, images and libraries for EVOS S1000 are stored and maintained in a Thermo Fisher-approved artifact management solution. This provides visibility and control on developed software builds, enabling the EVOS S1000 Product 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 EVOS S1000 Product Development team utilizes a Thermo Fisher-approved static analysis tool to scan code repositories. This tool helps identify potential security defects, maintain code quality and integrity and allow for the prompt review and prioritization of security alerts for remediation based on criticality and a business risk management process.

Peer code reviews

The EVOS S1000 Product Development team conducts manual peer reviews of code before testing and deployment to help assess adherence to coding standards and design requirements. These reviews provide additional insight 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 EVOS S1000 Spatial Imaging System against the Open Worldwide Application Security Project (OWASP) Top 10 Internet-of-Things (IoT) list. The team, comprised of trained penetration testers, uses 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

Antivirus/anti-malware

The companion PC is equipped with Microsoft Defender™ to provide protection against malicious software. Thermo Fisher recommends that customers schedule virus and malware scans during a designated maintenance window when the EVOS S1000 instrument is not in use.

To ensure optimal performance, customers should not install additional applications, apply unauthorized Windows operating system updates, or run other applications concurrently with the EVOS S1000 Imaging software. Running unapproved software or making configuration changes may lead to a non-validated system environment and adversely affect the stability of the EVOS S1000 Spatial Imaging System.

Vulnerability and patch management

The EVOS S1000 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 and a business risk management process.

Thermo Fisher recommends testing and applying patches to impacted EVOS S1000 versions upon notification to help keep systems up to date and minimize risks associated with vulnerabilities. Updates are available at thermofisher.com/software-downloads.

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

Disaster recovery and business continuity

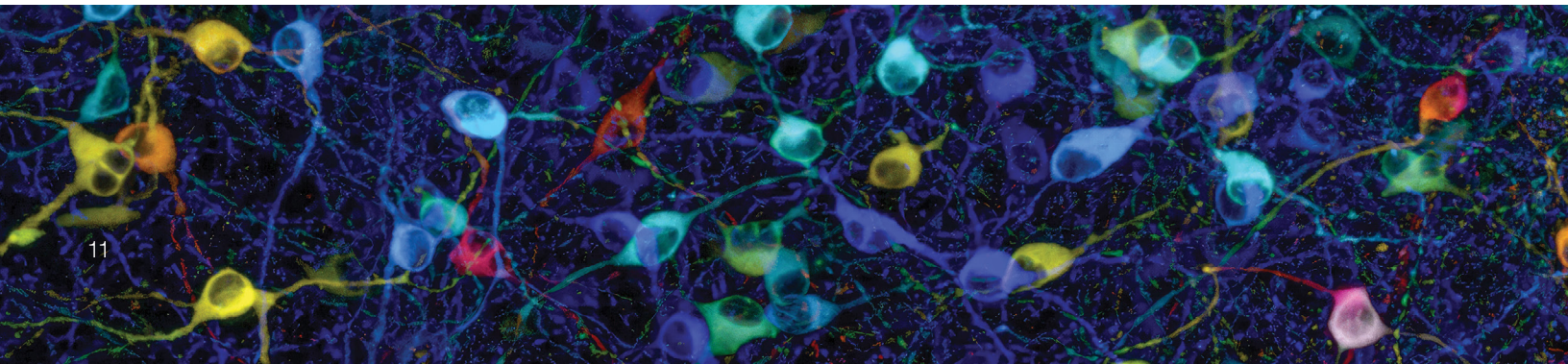
The companion PC has data backup capabilities to prevent data loss and aid in restoring normal functionality. Thermo Fisher suggests that customers leverage these backup capabilities and include them in disaster recovery plans and testing in accordance with their policies. Thermo Fisher also suggests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

Service handling

Application-specific support and global training serve as critical components to maintaining and supporting the EVOS S1000 Spatial Imaging System. 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.

For the latest service and support information, customers can visit EVOS Cell Imaging System Services, thermofisher.com/support or the Services Central portal. These resources provide worldwide contact telephone numbers, product support materials (including FAQs, software, patches and updates), training for many applications and instruments, order and web support and product documentation such as user guides, manuals, protocols, Certificates of Analysis and Safety Data Sheets (SDSs).

Note: For an SDS related to reagents and chemicals supplied by other manufacturers, customers should contact the respective manufacturer directly.



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