Medviso Software Security

2025-10-28

MEDVISO AB
Griffelvägen 3
SE-224 67 Lund
Sweden
support@medviso.com
https://www.medviso.com
P: +46-76-183 6442

Contents

1 General information

This document provides a structured disclosure of cybersecurity and IT security controls for the Medviso Segment software solutions Segment, Segment CMR, and Segment 3DPrint.

1.1 Purpose and scope

The measures described in this document are designed to meet the requirements of Regulation (EU) 2017/745 (MDR) Annex XV Chapter II §4.5, ensuring that personal data handled within the software remain protected against unauthorised access, disclosure, or loss.

1.2 Product usage and environment

The software is intended for use in hospital and clinical environments. It is compatible with standard medical-grade hardware, including medical image scanners, workstations, and PACS systems. The operating environment should adhere to national and EU regulations, such as GDPR, and provide physical security for the medical device via measures like regulated access and secure areas.

1.3 Standards, regulations, and compliance

Medviso maintains an internal information security management processes, which define responsibilities, access control governance, and escalation paths for security events, ensuring organisational alignment with the NIST Cybersecurity Framework and is fully compliant with the following regulations and standards pertaining to cyber and software security:

- General Data Protection Regulation (EU) 2016/679 (GDPR),
- Artificial Intelligence Act, Regulation (EU) 2024/1689 (AI Act), and
- DICOM standard PS 3.2.

2 Security features

2.1 Authentication, authorisation, and access control

Installing the software requires Administrator access on your computer. For your safety and the protection of patient data, we recommend enabling the built-in password feature in the Segment software. This password is linked to your Windows login, making access both secure and straightforward without adding extra steps to your workflow.

For organisations that use central user management systems, the software can also integrate with Active Directory. Only authorised staff will have access, and your organisation's existing security policies, such as password complexity and user permissions, will be applied automatically. This makes access both simpler and safer while ensuring patient data is protected.

2.2 Audit controls and logging

For support purposes, Segment software maintains a log of work sessions. The log **does not** contain any imaging data or patient information. The only identifiable information that is recorded is the computer's hostname and the license number used during the session. This enables our support team to assist you without requiring the transfer of imaging files, thereby reducing the risk of data exposure. To protect both your safety and your patients' privacy, the log file is stored per Windows user and log files older than 7 days are automatically deleted.

2.3 Data confidentiality and encryption

Segment software is deployed on local workstations and servers.

In accordance with the General Data Protection Regulation (GDPR), healthcare institutions remain the data controllers when using the software. Medviso acts only as a technical supplier and does not access, process, or store identifiable patient data during normal operation. No personal data leave the customer's IT environment, and temporary files created during analysis are removed when the session ends.

2.3.1 Data location

All data is stored according to the user's configuration. If any data is transmitted to Medviso, it is stored exclusively within the European Union, unless you have explicitly agreed otherwise.

2.4 Data integrity and validation

Segment software is downloaded via our secure HTTPS server. To ensure the integrity of the file and confirm it has not been tampered with, the MD5 checksum is provided for users

to verify.

Additionally, the we have implemented the following integrity measures:

- All software code is encrypted using the Advanced Encryption Standard (AES) cryptosystem before it is compiled into a software package via MATLAB Compiler, minimising the risk of reverse engineering.
- Licence keys and machine learning networks are encrypted using an XOR operation with a private key to reduce the risk of unauthorized access.
- Our website uses the Really Simple SSL plugin, which automatically detects the settings and configures the site to run over HTTPS, ensuring secure communication over a network.
- All installation files on our website are signed using a code signing certificate (PKCS#11) to authenticate their source.
- All uploads of files and data to our website, including program files or instructions for use, require a personal login and a connection to our local FTP server, which is password-protected.
- Our website host leverages advanced technology from Immunify360 to detect and protect against cyber-attacks and provides 24/7 monitoring of the hosting servers.

2.5 Data retention and disposal

Data from users is retained only for the duration of a support issue and is deleted thereafter.

3 System and network security

3.1 System requirements

Component	Minimum Requirement
CPU	Intel or AMD x86-64 processor with at least 4 logical cores
Memory	8 GB RAM (16 GB recommended)
Disk	Solid State Drive (SSD), minimum 5 GB free space
Operating System	Windows 10/11 (64-bit), Windows Server 2019
Graphics	DirectX and OpenGL compatible graphics card
Graphics (for AI)	CUDA-enabled NVIDIA GPU with 4 GB VRAM or more
GPU (for AI)	NVIDIA Ampere, Turing, Volta, or Pascal architecture
Third-party Software	Microsoft Word and Adobe Acrobat Reader (for full report functionality)
Peripherals	Standard keyboard, mouse, and display with suitable resolution for diagnostic use

3.1.1 General security requirements for the operating environment

- The operator is recommended to comply with all applicable national and EU regulations (e.g. GDPR).
- The operating environment should provide physical security for the medical device through measures such as:
  - Controlled and authenticated physical access enforced via appropriate technical measures (e.g. badges),
  - A physical security policy defining roles and access rights, including access to the medical device, and
  - Use of segregated, secure areas with appropriate access controls.
- The operating environment should implement appropriate security controls, including:
  - User access management (e.g. credentials for accessing software applications or devices, user access policies),
  - Antivirus and anti-malware protection,
  - Firewalls,

  - Application whitelisting and system hardening,
  - Exclusive use of genuine software, with prohibition of unauthorised or illegitimate software, and
  - Session management measures (e.g. session timeouts).

- The operating environment should ensure control and security of network traffic via:
  - Network segmentation,
  - Traffic filtering, and
  - Data encryption.

- For workstations connected to the medical device, recommended security measures include:
  - Operating system hardening and application whitelisting,
  - Memory protection measures to prevent unauthorised code execution,
  - Compatibility of the medical device software with security solutions designed to counter malicious code,
  - Use of strong passwords, and
  - Installation of only those software programmes necessary for the intended use of the operating environment.

- In cases where the operating environment integrates multiple medical devices or other systems, measures to limit the propagation of an attack may include:
  - Partitioning mechanisms and network/traffic segmentation, and
  - Software integrity checks and device authentication mechanisms.

- To maintain an appropriate security posture of both the operating environment and the medical device, provisions for version and update management are recommended.
- Elements of the operating environment that interact with (e.g. other devices) or are required for the operation of the medical device (e.g. the operating system) should ensure interoperability and should not impair the specified performance of the medical device.

3.2 Software Bill of Materials (SBOM)

Third-party software used in the Segment software are listed below, along with their specifications:

3.2.1 Software items used in all Segment software

Table 2: MATLAB Compiler Runtime (MCR)

Supplier Name	MathWorks
Component Name	MATLAB Compiler Runtime (MCR)
Component Version	R2022a
License	Proprietary, distributed by MathWorks
Other Unique Identifiers	Runtime environment for precompiled MATLAB code used by Segment software
Dependency Relationship	Required runtime for MATLAB-based modules within Segment software; dependent on Windows 10/11, 64-bit
Author of SBOM Data	Medviso

Table 3: Visual Studio C++ Redistributable

Supplier Name	Microsoft
Component Name	Visual Studio C++ Redistributable
Component Version	2015–2022
License	Microsoft Software License Terms
Other Unique Identifiers	Installs Microsoft C and C++ runtime libraries; required for Sectra PACS image transfer to Segment software
Dependency Relationship	Required by Segment software for Sectra PACS integration
Author of SBOM Data	Medviso

Table 4: DCMTK Library

Supplier Name	OFFIS – Institute for Information Technology
Component Name	DCMTK Library
Component Version	3.6.6
License	BSD-style open source
Other Unique Identifiers	Open-source DICOM toolkit for handling PACS communications
Dependency Relationship	Used by Segment software to send/receive/search DICOM files and convert formats
Author of SBOM Data	Medviso

Table 5: NSSM Service

Supplier Name	Iain Patterson
Component Name	NSSM Service
Component Version	2.24
License	GPL v2 open source
Other Unique Identifiers	Non-Sucking Service Manager for Windows services
Dependency Relationship	Ensures Segment Server services are monitored and restarted if they stop unexpectedly
Author of SBOM Data	Medviso

Table 6: MATLAB function nanconv

Supplier Name	Benjamin Kraus
Component Name	MATLAB function nanconv
Component Version	1.1.0.0
License	MATLAB File Exchange open-source license
Other Unique Identifiers	Open-source MATLAB function for 1D/2D convolution ignoring NaN values
Dependency Relationship	Embedded in Segment software to handle image data with missing values
Author of SBOM Data	Medviso

Table 7: MATLAB function xml2struct

Supplier Name	Wouter Falkena
Component Name	MATLAB function xml2struct
Component Version	1.8.0.0
License	MATLAB File Exchange open-source license
Other Unique Identifiers	Open-source MATLAB function to convert XML files into MATLAB structures
Dependency Relationship	Used in Segment software for parsing XML configuration and metadata
Author of SBOM Data	Medviso

Table 8: MATLAB function findjobj

Supplier Name	Yair Altman
Component Name	MATLAB function findjobj
Component Version	1.53.0.1
License	MATLAB File Exchange open-source license
Other Unique Identifiers	Open-source MATLAB function to access Java objects in GUI handles
Dependency Relationship	Used in Segment software to customize GUI components
Author of SBOM Data	Medviso

Table 9: Smart card library pkcs11-tool

Supplier Name	Olaf Kirch, OpenSC (open source)
Component Name	Smart card library pkcs11-tool
Component Version	0.21.0.0
License	LGPL (OpenSC open-source license)
Other Unique Identifiers	Facilitates use of PIV/smart cards for authentication and digital signatures
Dependency Relationship	Used by Segment software to authenticate users and secure data
Author of SBOM Data	Medviso

Table 10: OpenSSL

Supplier Name	The OpenSSL Project
Component Name	OpenSSL
Component Version	1.1.1w
License	OpenSSL License and SSLeay License (Apache-style)
Other Unique Identifiers	Library for encryption, signing, and certificate validation
Dependency Relationship	Used to validate user signatures in Segment software
Author of SBOM Data	Medviso

3.2.2 Software items used in Segment 3DPrint only

Table 11: IDTF Converter

Supplier Name	Alexandre Gramfort
Component Name	IDTF Converter
Component Version	v1.2.851.0
License	GPL (open source)
Other Unique Identifiers	Converts 2D MATLAB mesh images to 3D PDF images
Dependency Relationship	Embedded in Segment software for 3D visualization output
Author of SBOM Data	Medviso

Table 12: Remesh

Supplier Name	geometry4Sharp Open-source project
Component Name	Remesh
Component Version	Head revision 2024-06-14
License	Boost Software License 1.0 (permissive open-source)
Other Unique Identifiers	C# library for geometric computing and 3D mesh manipulation
Dependency Relationship	Improves 3D experience in Segment software
Author of SBOM Data	Medviso

3.3 Network communication

The following table summarises the network connections, protocols, data types, and security measures used by Segment software.

Table 13: Network communication

Application	**Protocol / Standard**	**Source → Destination**	**Port / Scheme**	**Data Type / Purpose & Security Measures**
Segment Server	DICOM	External DICOM node → Segment software	TCP/IP, port 104 (configurable)	Medical images and metadata; within customer firewall; antivirus protection
Query Retrieve	DICOM (findscu, movescu)	PACS → Segment CMR	TCP/IP	Medical images and metadata; within customer firewall; antivirus protection
Send to PACS	DICOM	Segment software → PACS	TCP/IP	Medical images and metadata; within customer firewall; antivirus protection
License Server	TCP	Segment software → Medviso License Server	Port 443 (HTTPS)	License validation; encrypted communication; logging
Sectra PACS Connection	IDS Imaging API	Sectra PACS → Segment software	Windows pipes	Medical images and metadata; within customer firewall; antivirus protection; login required

3.4 Adding MATLAB website to network firewall

If your organisation operates a network firewall, you must allow connections to the MathWorks servers to install the MATLAB Runtime (which is included with the software) during the installation process.

The MathWorks installer requires access to the following servers and ports:

- `login.mathworks.com`
- `services.mathworks.com`
- TCP ports 80 and 443

Ensure your firewall allows connections to these domains over ports 80 and 443. Since these servers use dynamic IP addresses, they cannot be whitelisted by IP – use the domain names instead. More information on unblocking connections is available at the link below.

Source: *Why do I get a connection error when installing or activating MATLAB or other MathWorks products?*

3.5 Adding licence server to network firewall

If your organisation operates a network firewall, access must be permitted to the Medviso Licence Server to enable verification and updating of the software licence.

Segment software contacts Medviso Licence Server on the following address and port:

- URL: `https://medviso.com`
- Port: 443

4 Protection and safeguards

4.1 Malware protection and vulnerability management

Segment software incorporates measures to minimise the risk of malware infection and ensure prompt handling of potential software vulnerabilities. The following practices are recommended:

- **Antivirus compatibility:** Segment software has been tested with common antivirus and anti-malware solutions. Users should ensure their antivirus software is active and kept up-to-date.
- **Secure software updates:** Updates are distributed exclusively via official Medviso channels. Users should install updates promptly to prevent exposure to potential vulnerabilities.
- **Vulnerability reporting and mitigation:** Any suspected software vulnerability should be reported to Medviso via support@medviso.com. Medviso reviews reports promptly and issues updates or mitigations as necessary.
- **Version control:** Users are encouraged to operate the latest verified version of the software. Older versions may lack important security updates and are more vulnerable to potential threats.
- **Security awareness:** Users should avoid downloading software or files from untrusted sources and follow best practices for network security.
- **Internal security testing:** Medviso regularly performs internal security assessments and testing to identify and remediate vulnerabilities before release, ensuring compliance with relevant regulatory standards.

Medviso continuously monitors publicly available cybersecurity advisories and relevant software-component vulnerability databases. Software updates are cryptographically signed and automatically verified by the application prior to installation to ensure authenticity and integrity. In the unlikely event of a suspected or confirmed data-security breach, Medviso promptly investigates the issue, contains any impact, and informs affected customers without undue delay. Corrective updates or mitigations are distributed through the official, verified Medviso channels. All incidents are reviewed internally to ensure appropriate corrective and preventive actions are implemented.

4.2 Security guidance for users (shared responsibility)

This guidance helps users manage cybersecurity risks related to patient data, as described in the Instructions for Use (IFU), section *Safety Instructions*. Following these recommendations can help reduce the residual risks:

- Exposure of patient data / integrity violation.
- User gets incorrect information from user manual.
- Computer virus on users' computers where software is installed on.

4.2.1 Your responsibilities

To keep patient data secure, you should:

- De-identify or pseudonymise patient data before uploading or sharing
- Follow your organisation's IT security policies
- Only give access to authorised personnel
- Report any suspected security incidents immediately

4.2.2 Local security measures to implement

Ensure that your workstation and network are protected by:

- Firewall and antivirus/anti-malware software
- Full-disk encryption and secure backups
- Role-based access control for sensitive data
- Secure network connections (VPN, HTTPS)
- Physical security for computers and servers handling patient data