Powered by *syngo* MI Apps VB21

Symbia SPECT and SPECT/CT

System Security

Protect your most important assets

—today and in the future.

siemens.com/mi

SIEMENS Healthineers

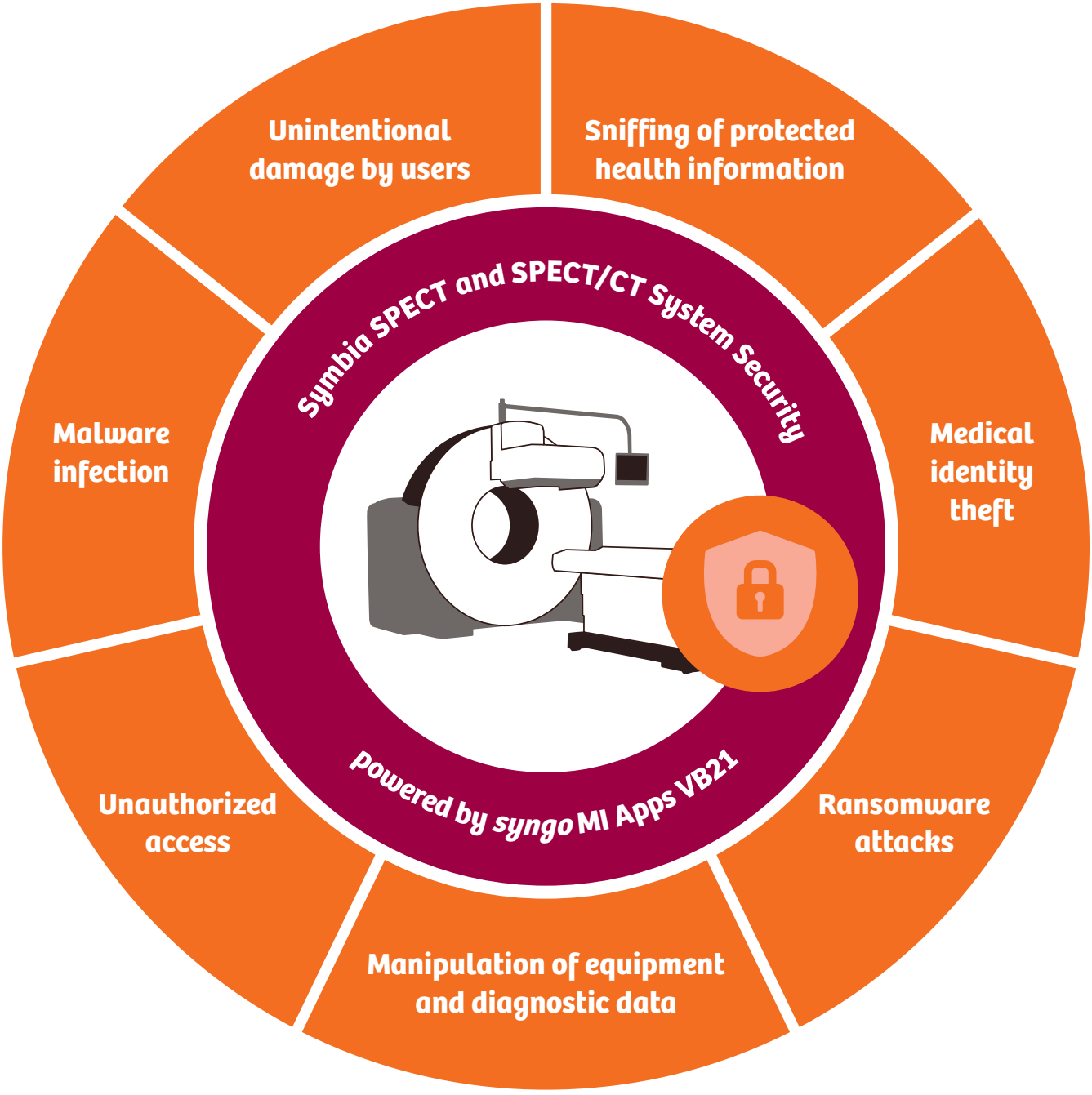
Symbia SPECT and SPECT/CT System Security

Protect your most important assets — today and in the future.

Addressing the threat of cyberattacks on healthcare facilities has become a strategic issue for organizations of every size. Widely publicized data breaches have raised concerns for healthcare providers, as well as fueled patient interest over how personal information is handled. These growing pressures have triggered the need for more secure medical imaging technology in order to better protect against internal and external threats that can negatively impact patient care, compromise regulatory compliance, cause financial loss, and damage credibility.

Symbia™ SPECT and SPECT/CT System Security builds on our long-term experience in developing solutions to harden and defend your imaging systems and IT infrastructure.

Comprising a bundle of solutions that enable you to confront primary IT cybersecurity factors, Symbia SPECT and SPECT/CT System Security helps you manage and mitigate the risks of unauthorized system access, exposure of health information, and manipulation of your medical equipment.


Unintentional damage by users
Sniffing of protected health information
Medical identity theft
Ransomware attacks
Manipulation of equipment and diagnostic data
Unauthorized access
Malware infection
Symbia SPECT and SPECT/CT System Security
Powered by syngo MI Apps VB21

As part of our commitment to helping you achieve the level of security and privacy you require, a number of options are available to ensure your software is up-to-date throughout the lifecycle of your new and installed Symbia systems.

Understanding security is not an option. Symbia System Security Basic is a standard feature in our *syngo*® MI Apps VB21 software. For increased protection, we also offer *syngo* Security Package, which provides additional tools for strengthening your IT environment and imaging systems.

Basic

Standard with *syngo* MI Apps VB21

Hardened operating software

- Uses a hardened Windows® version that enables firewalls and restricts network communication to the clinically relevant DICOM nodes (for example, PACS and RIS)

Strong passwords

- Increases your level of protection with stronger user passwords in compliance with your organization's password policy

Whitelisting software protection

- Allows only applications defined for use on your medical device to run, which helps prevent external parties from manipulating system code and running dangerous applications

Trusted nodes

- Reduces the risk of data manipulation by authenticating predefined secure medical devices in your network (for example, PACS servers)

syngo Security Package

Greater confidence with an added level of protection

User management

- Defines individual user accounts and protects scanner access with a strong user password. This helps prevent unauthorized usage and enables the audit trail function.

Audit trail

- Enables evaluation of who is accessing protected health information (PHI). Recording audit trail entries is required for compliance with the U.S. Health Insurance Portability and Accountability Act (HIPAA).

Functional roles

- Supports the creation of individual privileges and restricts scanner usage according to your organization's defined user hierarchy

Patient groups

- Limits user access to specific patients, which helps safeguard sensitive patient information (for example, data of VIP patients)

DICOM encryption

- Transmits encrypted health data confidentially via secure DICOM

Security for all your systems

SPECT/CT

- Symbia Intevo Bold™
- Symbia Intevo™
- Symbia T Series

Secure your entire family of Symbia systems

Improved confidentiality
Protected health information is not disclosed to unauthorized persons.

Data integrity
Protected health information cannot be altered or deleted by unauthorized person.

SPECT

- Symbia Evo™
- Symbia Evo Excel
- Symbia S
- Symbia E

Workplaces

- MI Workplace
- Symbia.net

Secure data access
Sensitive information stored on the medical device can only be accessed by authorized persons.

Integrated accountability
Any modifications to information can be attributed to the person responsible.

Assured authenticity
User identities can be verified any time.

Enhanced authentication
Supports PKI (public key infrastructure) user authentication.

On account of certain regional limitations of sales rights and service availability, we cannot guarantee that all products included in this brochure are available through the Siemens Healthcare sales organization worldwide. Availability and packaging may vary by country and are subject to change without prior notice.

Some/All of the features and products described herein may not be available in all countries. The information this document contains general technical descriptions of specifications and options, as well as, standard and optional features which do not always have to be present in individual cases.

Siemens Healthcare reserves the right to modify design, packaging, specifications and options described herein without prior notice. Please contact your local Siemens Healthcare sales representative for the most current information.

"Siemens Healthineers" is considered a brand name. Its use is not intended to represent the legal entity to which this product is registered. Please contact your local Siemens organization for further details.

Siemens Healthineers Headquarters
Siemens Healthcare GmbH
Henkestr. 127
91052 Erlangen, Germany
Phone: +49 9131 84-0
siemens-healthineers.com

Published by
Siemens Medical Solutions USA, Inc.
Molecular Imaging
2501 North Barrington Road
Hoffman Estates, IL 60192
USA
Phone: +1 847 304-7700
siemens.com/mi

Order No. A91MI-10467-C1-7600 | Printed in USA | MI-3569.TM.JV.TW.1000 |