Security White Paper

syngo Virtual Cockpit VA15A

The facts about the security of our products and solutions

siemens-healthineers.com/*syngo*-virtual-cockpit

SIEMENS Healthineers

Foreword

The Siemens Healthineers Product & Solution Security (PSS) program

At Siemens Healthineers, we are committed to working with you to address cybersecurity and privacy requirements. Our Product and Solution Security Office is responsible for our global program that focuses on addressing cybersecurity throughout the product lifecycle of our products.

Our program targets incorporating state of the art cybersecurity into our current and future products. We seek to protect the security of your data while, at the same time, providing measures to strengthen the resiliency of our products from cyber threats.

We comply with applicable security and privacy regulations from the US Department of Health and Human Services (HHS), including the Food and Drug Administration (FDA) and Office for Civil Rights (OCR), to help you meet your IT security and privacy obligations.

Vulnerability and incident management at Siemens Healthineers cooperates with government agencies and cybersecurity researchers concerning reported potential vulnerabilities.

Our communications policy strives for coordinated disclosure. We work in this way with our customers and other parties, when appropriate, in response to potential vulnerabilities and incidents in our products, no matter what the source.

Elements of our product and solution security program

- Providing information to facilitate secure configuration and use of our medical devices in your IT environment
- Conducting formal threat and risk analysis for our products
- Incorporating secure architecture, design and coding methodologies in our software development process
- Performing static code analysis of our products
- Conducting security testing of products under development as well as products already in the field
- Tailoring patch management to the medical device and depth of coverage chosen by you
- Monitoring security vulnerability to track reported third party components issues in our products
- Working with suppliers to address security throughout the supply chain
- Training of employees to provide knowledge consistent with their level of responsibilities regarding your data and device integrity.

Contacting Siemens Healthineers about product and solution security

Siemens Healthineers requests that any cybersecurity or privacy incidents are reported by email to: **productsecurity@siemens-healthineers.com**

For all other communication with Siemens Healthineers about product and solution security: **ProductTechnologyAssurance.dl@siemens-healthineers.com**

Jim Jacobson
Chief Product and Solution Security Officer
Siemens Healthineers

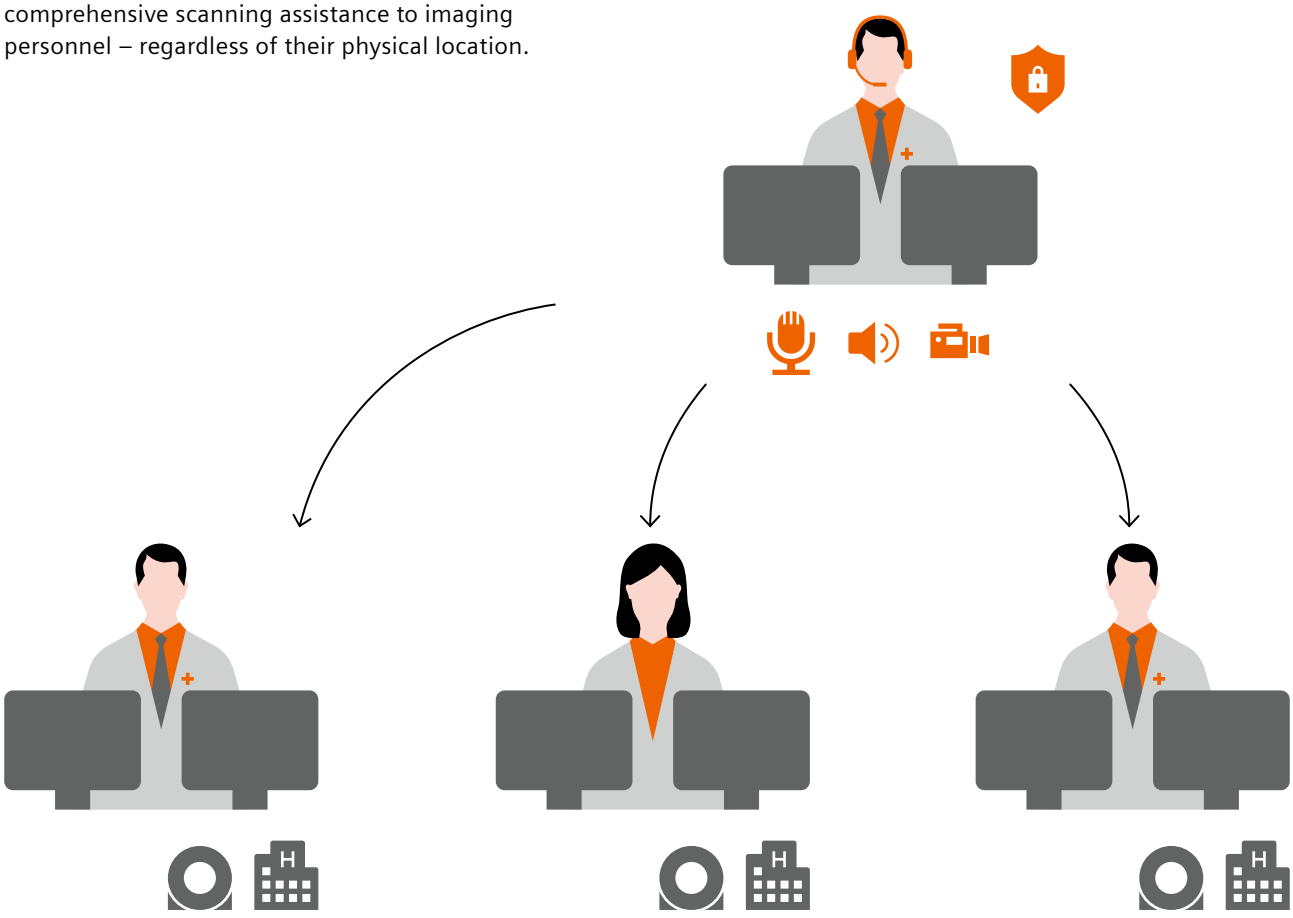
Contents

Basic Information

syngo Virtual Cockpit – Move knowledge, not staff.

Your software for remote scanning assistance.

syngo Virtual Cockpit enables you to provide comprehensive scanning assistance to imaging personnel – regardless of their physical location.



Core features

- Real-time knowledge sharing across teams and sites
- Live video, screen sharing, audio and chat functions
- One experienced technologist can collaborate with up to three scanning workplaces simultaneously

Operating systems

Server:

- Windows Server 2016
- Windows Server 2019
- Red Hat Enterprise Linux 7.9

Modality Clients:

- Microsoft Windows 10 (64bit)

Steering Clients:

- Microsoft Windows 10 (64bit)

Hardware specifications

Infrastructure/communication server:

- *syngo* Virtual Cockpit supports both physical or virtualized setups, the hardware specification for the *syngo* Virtual Cockpit Server depends on the setup chosen.
- The virtualized environment shall support hosting of Windows Server 2016 or Windows Server 2019 and Red Hat Linux 7.9 OS.

***syngo* Virtual Cockpit Modality and Steering clients:**

- USB-pluggable headset (with microphone) or speakerphone for VoIP-calls. [1]
- IP Cameras [1]: Up to two IP Cameras can be installed per scanner and placed in the operator room.

Please refer to the *syngo* Virtual Cockpit Data Sheet for more information and hardware requirements for server and clients.

[1] *Not part of the product.*

[2] *See Picture 2 and 3 in the "Shared Responsibilities" chapter below for more information about patching responsibilities.*

User account information

- *syngo* Virtual Cockpit user accounts can be local Windows user accounts, managed by the Security Accounts Manager (SAM), as well as Active Directory (AD) domain accounts. Therefore, *syngo* Virtual Cockpit users are authenticated by SAM or by AD.
- The system provides preconfigured Password Policies which can be customized by administrators.
- *syngo* Virtual Cockpit Communication Server provides account for administrative purposes – "root". The customer is responsible for "root" account adequate password policy.
- *syngo* Virtual Cockpit Communication Server provides account for remote service purposes – "aremote".

For details and configuration please refer to the Administration Manual.

Patching strategy

- Security patches of both server applications and the patches for the operating system on the communication server will be provided on a regular basis, after internal validation by Siemens Healthineers. The customer needs to take care that the operating system of the infrastructure server (Microsoft Windows) is updated on a regular basis. [2]
- Update policies are described in the Administration Manual and shall be followed to ensure an up-to-date setup of the environment.

Cryptography usage

syngo Virtual Cockpit Infrastructure Server and Clients are based on Microsoft Windows as operating system. Windows has built-in functions for encryption, authentication and message hashing. A complete list of the algorithms used can be obtained from Microsoft TechNet. Those algorithms are used for encryption, authentication and message signing visible to the operator and to the hospital network.

For security relevant purposes we do fully support FIPS 140-2 algorithms. Those internal implementations are assumed to be identical to the standard implementations, but not necessarily FIPS 140-2 certified.

Handling of sensitive data

- *syngo* Virtual Cockpit does not process electronic Protected Health Information (ePHI).
- Processing of Personally Identifiable Information (PII) is limited to user names.
- Sensitive information (PHI/PII) might be present in user editable input fields or in the voice and video streams generated and processed. This information will be transferred over the customer network but not stored permanently. *syngo* Virtual Cockpit encrypts chat and Voice-over-IP conversations. [1]

Boundary Defense

Build in Microsoft Windows Firewall on the infrastructure server is used to minimize the network attack surface.

For optimized protection of sensitive data and operation of the system it must be deployed in a secure network environment, utilizing e.g. network segmentation, client access control and protection against access from public networks. Please see the related Secure Configuration and Hardening Guide.

Boundary defenses in the hospital should be multilayered relying on firewalls, proxies, DMZ and network based IDS and IPS, as well as physical protections.

Terms and Conditions

Please refer to local Siemens organization for Terms & Conditions related to Cybersecurity.

[1] *Encryption of the communication between syngo Virtual Cockpit Steering Client and scanner depends on the installed scanner types and their versions.*

Network Information

The *syngo* Virtual Cockpit server requires two static IP addresses, each IP Camera (not part of the product) requires one static IP address, for connection initiated by clients. Both IP standards, IPv4 and IPv6, are supported.

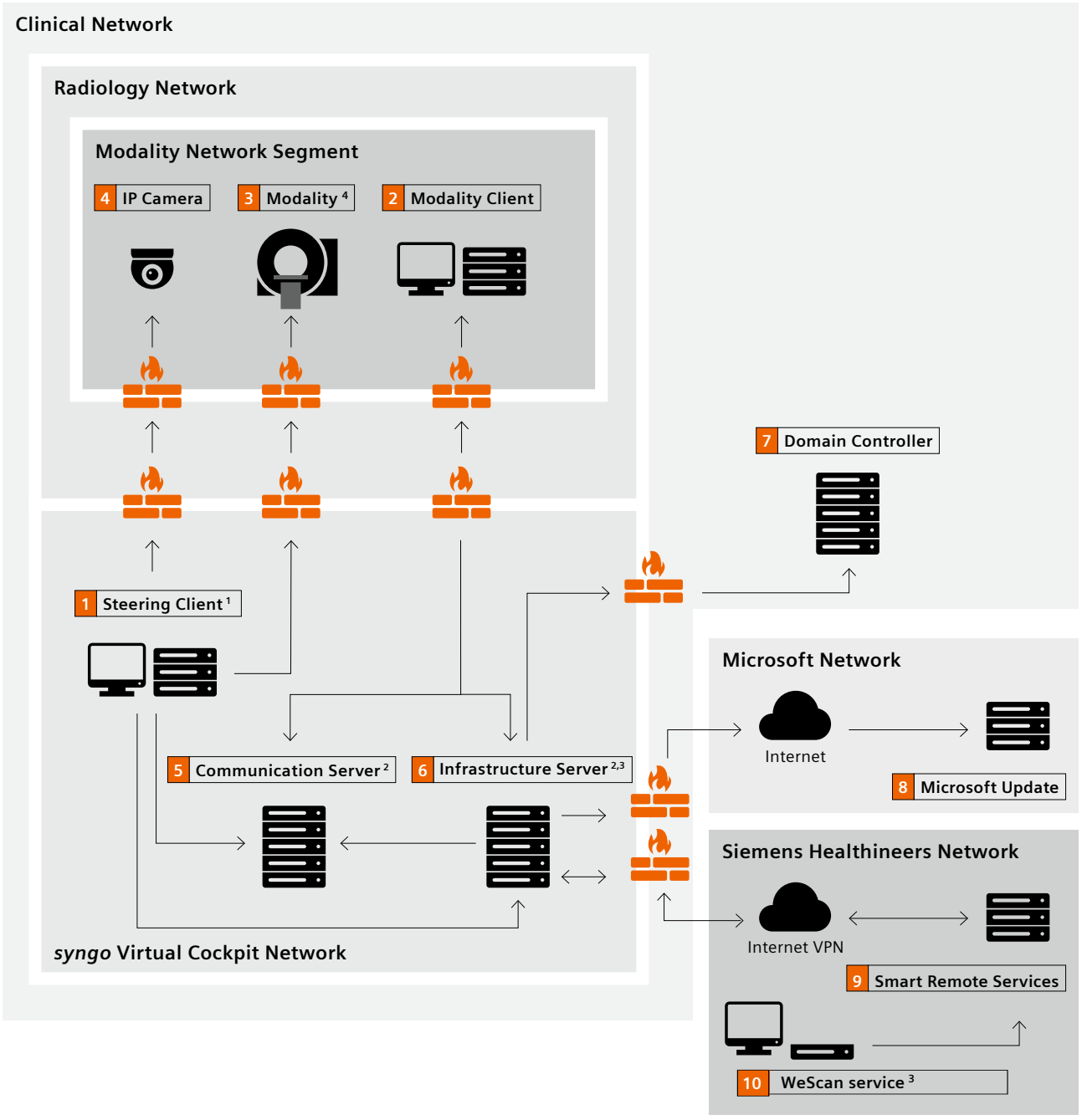


Figure 1:
Network Interfaces and recommended *syngo* Virtual Cockpit deployment in clinical network.

[1] *syngo Virtual Cockpit Steering Client can be deployed in clinical or radiology networks.*
[2] *syngo Virtual Cockpit Servers (Infrastructure and Communication server) can be part of clinical or radiology networks.*
[3] *WeScan service (optional) - requires steering client installation on Infrastructure server*
[4] *optional, integrated syngo Virtual Cockpit WEB client (e.g. MAGNETOM Free.Max)*

Identifier	Devices
1	Steering Client
2	Modality Client
3	Modality
4	IP Camera
5	Communication Server
6	Infrastructure Server
7	Domain Controller
8	Microsoft Update Server
9	Smart Remote Services

Service/ function	Source/ destination	Port number	Protocol
Modality (inbound)			
Expert-I (desktop duplication)	1 → 3	**5800** [1]**, 5900** [1]**, 5902** [2] **7443** [3]	VNC (over TCP) HTTPS (over TCP)
Camera (inbound)			
Camera streaming	1 → 4	**554** (configurable on camera)	RTSP (over TCP)
Communication server (inbound)			
Collaboration features (chat, VoIP)	1 → 5 2 → 5	**3334, 3478, 4001, 8089** **3478 , 20000-20199** [4]	TCP UDP
Authentication/User/Group/ Modality management	6 → 5	**3335** **4001, 4002**	HTTPS (over TCP) TCP
Maintenance/Administration (SSH)	6 → 5	**22**	SSH (over TCP)
Infrastructure server (inbound)			
Authentication	1 → 6 2 → 6	**553**	HTTPS (over TCP)
Administration Portal SRS (MSTS, Remote Desktop conn.) SRS (MNP) SRS (Event-Management) SRS (Remote Assist., TeamViewer)	9 → 6	**443** **3389** **8226** **13001** **11080**	HTTPS (over TCP) RDP (over TCP, UDP) TCP TCP TCP
Infrastructure server (outbound)			
SRS (MNP) SRS (Event-Management) SRS (FTP) SRS (Remote Assist.,TeamViewer) SRS (TeamViewer)	6 → 9	**8227, 8228** **12061** **20, 21** **8080** **5938** [5]	TCP TCP FTP (over TCP) TCP TCP, UDP
LDAP	6 → 7	**389**	LDAP (over TCP, UDP)
Microsoft Windows Server Update	6 → 8	**80** **443**	HTTP (over TCP) HTTPS (over TCP)

Table 1: List of Services, Protocols and Ports used by the product

[1] *Used by syngo classic based scanners (e.g. MAGNETOM Aera or SOMATOM Drive). 5800 is used for unattended login (if enabled), 5900 for invited login.*

[2] *Default port used by native/syngo based scanners (e.g. MAGNETOM Vida or MAGNETOM Sola).*

[3] *Default port used by Expert-I version 11.*

[4] *Optional, for better streaming performance.*

[5] *TeamViewer preferred port. If TeamViewer can't connect over port 5938, it will try to connect over TCP port 443 and then over port 80.*

Security Controls

Malware protection

Siemens Healthineers provides information on recommended virus protection software and general instructions on configuration.

The customer is responsible for regularly updating virus patterns/definitions.

Virus protection software from following manufacturers is recommended for the *syngo* Virtual Cockpit Infrastructure Server:

- Trend Micro OfficeScan 12.0 or higher
- McAfee Endpoint Security 10.6 or higher
- Symantec Endpoint Protection 14.2 or higher
- Sophos Endpoint Security and Control 10.8 or higher
- Microsoft Defender 4.12 or higher

Whitelisting

syngo Virtual Cockpit Infrastructure Server supports Microsoft® Device Guard which is activated during installation of *syngo* Virtual Cockpit.

Controlled use of administrative privileges

Administrator rights are required to install/upgrade the servers. The first installation of the client needs to be carried out with administrator privileges. As long as certain prerequisites are not updated, the update can be installed with user privileges (for details see the Installation and Startup Manual). Running *syngo* Virtual Cockpit client application does not require administrator rights.

Administrative tasks or configuration changes can be performed in the Admin Portal on the infrastructure server. In order to access the Admin Portal the user needs to be added to the group “TeCoAdministrators”. Admin privileges on the infrastructure server are needed to grant these rights, but are not needed to access the Admin Portal.

Authentication

- For authentication and authorization, *syngo* Virtual Cockpit supports both, local (on server machine) users and LDAP defined users for user authentication.
- Only administrative users need access to the *syngo* Virtual Cockpit server.
- The system distinguishes between clinical and administrative roles. Clinical users do not require administrative privileges. Authorization as administrator is required for administrative tasks.

Security Scanning

Security scan is performed during development and release phase. No additional scans are done after installation.

Continuous Vulnerability Monitoring

Continuous vulnerability assessment and remediation is performed throughout the complete product lifecycle.

Hardening

- Hardening on the *syngo* Virtual Cockpit Infrastructure Server is performed based on the Security Technical Implementation Guidelines developed by Defense Information Systems Agency (DISA) U.S. department by upgrades and new installations using local policies.
- Hardening can be tailored to the site-specific needs by local or domain policies

Code, Data and Execution Integrity controls

- *syngo* Virtual Cockpit binaries' integrity is protected by vendor's cryptographic signature.
- Additionally, see “Whitelisting” and “Data protections controls”.

Network controls

- The system is designed to make limited use of network ports and protocols.
- Microsoft® Windows firewall is configured on the *syngo* Virtual Cockpit Infrastructure Server to block unwanted inbound network traffic. [1]
- Microsoft® Account Lockout policy Iis applied for local infrastructure server accounts.
- Siemens Healthineers recommends operating the system in a secured network environment, e.g. a separate network segment or a VPN. Inbound connections from the Internet are discouraged. Outbound connections should be limited by network or organizational policies for maintenance purposes only (e.g. OS patching). [2]

Physical Safeguards

The customer is responsible for the physical protection of the *syngo* Virtual Cockpit server, e.g. by a server room with access control. Please note that the *syngo* Virtual Cockpit server can contain sensitive data and should be protected against tampering and theft.

IP Camera protection

- IP Cameras are not part of the *syngo* Virtual Cockpit product. Selection, deployment and operation of the IP cameras is in the responsibility of the customer. This includes configuration and installing security patches. [3] *syngo* Virtual Cockpit Steering Clients connect directly to the cameras as can be seen in the network diagram in Figure 1.
- IP Cameras can process, store and provide access to privacy relevant sensitive content.
- The video stream is not encrypted by the product.

Therefore we recommend to:

- Limit access to the devices to the minimum network nodes and users.
- Deny any traffic from or to the public internet in the firewall.
- Establish continuous firmware patching process for your IP Cameras.
- Follow the vendor specific recommendations on secure camera operations.
- Use unprivileged IP camera account (streaming only) for integration with *syngo* Virtual Cockpit.
- Use only cameras providing state-of-the-art security capabilities, such as firewall and enabled centralized management of configuration, credentials and firmware updates.

Data protection controls

- Sensitive data is protected by role-based access control.
- The system provides auditing of its usage.
- Confidentiality and integrity of data is protected by encryption at rest and in transit. [4]
- The system provides backup and recovery capabilities for data in storages. The backups have to be carried out by the administrator.

Auditing/logging

System supports auditing/logging locally on the Infrastructure server or to a Syslog server. Only the administrator has access rights to the audit logs. Operating information, errors and usage data are logged.

Remote connectivity

Smart Remote Services connection performed using secured channel. The channel is used e.g. to download security patches and updates.

Incident response and management

Siemens has a 24/7 incident response team to react to any attacks to its systems. In case of suspected attacks,Siemens will work together with the incident response team of the cloud provider to analyze the issue, mitigate the effects of attacks and prevent malicious activity. The incident response teams follow established procedures for incident management, communication, and recovery. In case of a data breach involving institutional data, Siemens Healthineers will notify customers in compliance with the applicable data protection law and keep clear records about the incident and the response to it according to the Siemens privacy incident management process. If you suspect an attack or data breach, please contact the incident response team using the direct address: productcert@siemens.com

[1] *See Table 1 for details.*
[2] *See Figure 1 for recommended deployment, network segmentation and firewall setup.*
[3] *See Figure 2 about details of the patching responsibilites.*
[4] *Secure communication to modalities depends on the installed scanner and their versions.*

Shared Responsibilities

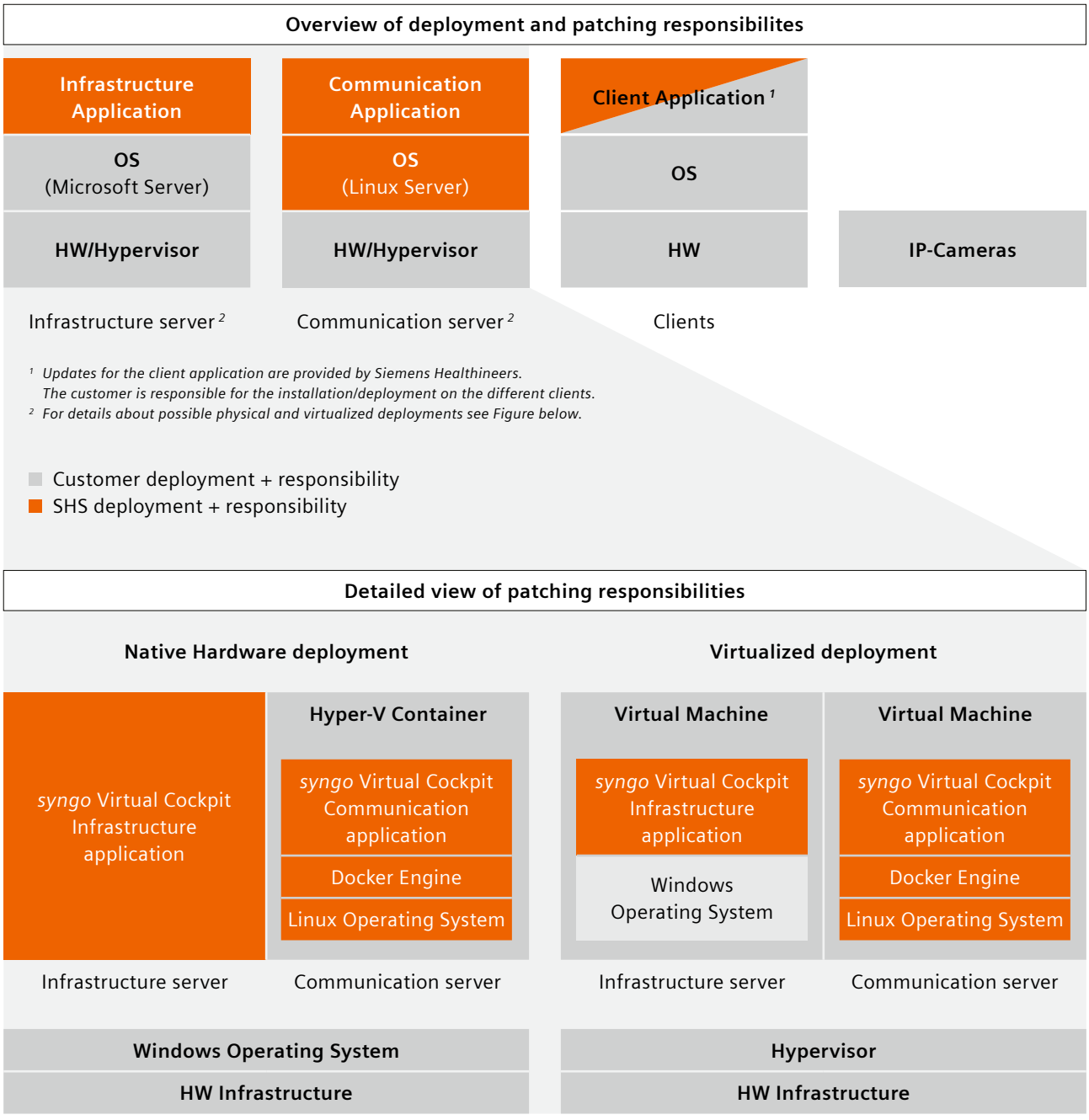


Figure 2:
Overview and detailed physical/virtualized server deployment and patching responsibilities.

Software Bill of Materials

The following table lists ALL third-party technologies used

Vendor name	Component name	Component version	Description/ use
Microsoft	Windows Server 2016	Standard Edition, English US	*syngo* Virtual Cockpit Infrastructure Server Operating System
Microsoft	Windows Server 2019	Standard Edition, English US	*syngo* Virtual Cockpit Infrastructure Server Operating System
Microsoft	Windows Installer XML	3.11.1	Installation automation
James Newton-King	Newtonsoft.Json	12.0.3	JSON serialization/deserialization
FastViewer	Universal Collaboration	sVC UC V 2.1	Communication (chat and voice over IP) between *syngo* Virtual Cockpit clients
Siemens Healthineers	Helix	Trunk 2104	Licensing and several service function-ality for use in *syngo* Virtual Cockpit
Red Hat	Red Hat Enterprise Linux (RHEL)	7.9	*syngo* Virtual Cockpit Communication Server Operating System
Docker	Docker Engine	1.13.1	Virtualization technology – containerization
Flexera Software	FlexNet Publisher	2018 R2	Product Licensing
Microsoft	.NET Framework	4.7.2	.NET runtime platform
Microsoft	Entity Framework	6.1.3	Object Relational Mapper
Microsoft	VC++ Runtime	2017, 2013	Runtime components of Visual C++ Libraries
Microsoft	AspNetWebStack	3.2.7	Source code repository for open source ASP.NET products
Microsoft	NuGet Package: Microsoft HTTP Client Libraries	2.2.29	Microsoft HTTP Client Libraries
Microsoft	NuGet Package: Microsoft. Web.Administration	7.0.0	.NET Core version of the Microsoft Web Administration assembly
Sam Harwell	NuGet Package: Antlr3.Runtime	3.5.1	Used in WeScan
Paul Seal	Password Generator	2.0.5	Used in WeScan
Siemens Healthineers	SHUI native	1.10.0	Siemens Healthineers UI
Siemens Healthineers	SHUI	1.14.0	Siemens Healthineers UI
Microsoft	WebGrease	1.6.0	Used in WeScan

Software Bill of Materials

Vendor name	Component name	Component version	Description/ use
SSH.NET	NuGet Package SSH.NET	2016.1.0	PowerShell Module for automating tasks on remote systems using SSH Used to access FV virtual machine remotely during the collaboration server update and to send remote commands to Communication server
Alexander Iacobciuc	NuGet Package: WebEye.Controls.Wpf	1.0.6	FFmpeg-based stream player control
Siemens Healthineers	Sy Angular	12.1.0	Used in *syngo* VirtualCockpit WebClient
Konrad Mattheis	NuGet Package: XAMLMarkupExtensions	1.9.0	A base class for nested markup extensions and a collection of useful extensions for WPF
XAMLMarkupExtensions	NuGet Package: WpfLocalizeExtension	3.6.1	Way to localize any type of DependencyProperties or native Properties
Mark Heath	NuGet Package: Naudio	1.10.0	Open source audio API for .NET
Microsoft	NuGet Package: Microsoft .AspNet.WebPages	3.2.7	Used in WeSca
Microsoft	IIS URL Rewrite	2.1/7.2	Microsoft URL Rewrite Module 2.0 for IIS 7
Carlos Perez	Posh-SSH	2.2	PowerShell Module for automating tasks on remote systems using SSH Used to access FV virtual machine remotely during the collaboration server update and to send remote commands to Communication server

Abbreviations

AD	Active Directory
AES	Advanced Encryption Standard
BIOS	Basic Input Output System
DES	Data Encryption Standard
DISA	Defense Information Systems Agency
DMZ	Demilitarized Zone
DoS	Denial of Service
ePHI	Electronic Protected Health Information
FDA	Food and Drug Administration
FIPS	Federal Information Processing Standards
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HIMSS	Healthcare Information and Management Systems Society
HTTP	Hypertext Transfer Protocol
HTTPS	HTTP Secure
IEC	International Electrotechnical Commission
IIS	Internet Information Services
LDAP	Lightweight Directory Access Protocol
MD5	Message Digest 5
MDS²	Manufacturer Disclosure Statement for Medical Device Security
NEMA	National Electrical Manufacturers Association
NTP	Network Time Protocol
OCR	Office for Civil Rights
PHI	Protected Health Information
PII	Personally Identifiable Information
RPC	Remote Procedure Call
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SRS	Siemens Remote Services
SW	Software
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VPN	Virtual Private Network

Disclaimer according IEC 80001-1

1-1 The Device has the capability to be connected to a medical IT-network which is managed under full responsibility of the operating responsible organization. It is assumed that the responsible organization assigns a Medical IT-Network Risk Manager to perform IT-Risk Management (see IEC 80001-1:2010/EN 80001-1:2011) for IT-networks incorporating medical devices.

1-2 This statement describes Device-specific IT-networking safety and security capabilities. It is not a responsibility agreement according to IEC 80001-1:2010/EN 80001-1:2011.

1-3 Any modification of the platform, the software or the interfaces of the Device – unless authorized and approved by Siemens Healthcare GmbH – voids all warranties, liabilities, assertions and contracts.

1-4 The responsible organization acknowledges that the Device's underlying standard computer with operating system is to some extent vulnerable to typical attacks like e.g. malware or denial-of-service.

1-5 Unintended consequences (like e.g. misuse/loss/corruption) of data not under control of the Device e.g. after electronic communication from the Device to some IT-network or to some storage, are under the responsibility of the responsible organization.

1-6 Unauthorized use of the external connections or storage media of the Device can cause hazards regarding the availability and information security of all components of the medical IT-network. The responsible organization must ensure – through technical and/or organizational measures – that only authorized use of the external connections and storage media is permitted.

International Electrotechnical Commission Glossary (extract)
Responsible organization:
Entity accountable for the use and maintenance of a medical IT-network.

Statement on FDA Cybersecurity Guidance

Siemens Healthineers will follow cybersecurity guidance issued by the FDA as appropriate. Siemens Healthineers recognizes the principle described in FDA cybersecurity guidance that an effective cybersecurity framework is a shared responsibility among multiple stakeholders (e.g., medical device manufacturers, health care facilities, patients and providers), and is committed to drawing on its innovation, engineering and pioneering skills in collective efforts designed to prevent, detect and respond to new and emerging cybersecurity threats. While FDA cybersecurity guidance is informative as to adopting a risk-based approach to addressing potential patient harm, it is not binding and alternative approaches may be used to satisfy FDA regulatory requirements.

The representations contained in this White Paper are designed to describe Siemens Healthineers' approach to cybersecurity of its medical devices and to disclose the security capabilities of the devices/systems described herein. Neither Siemens Healthineers nor any medical device manufacturer can warrant that its systems will be invulnerable to cyberattack. Siemens Healthineers makes no representation or warranty that its cybersecurity efforts will ensure that its medical devices/systems will be error-free or secure against cyberattack.

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

Legal Manufacturer
Siemens Healthcare GmbH
Henkestr. 127
91052 Erlangen, Germany

Published by Siemens Healthcare GmbH · online pdf · unrestricted · 0921 ·