White paper

Kinectus – Remote connectivity solution for ultrasound

Security concept

siemens-healthineers.com/ultrasound

Remote connectivity has become a vital component in the modern world of technology where companies and organizations need to provide remote technical support and application support to their customers. Kinectus is a custom development on Amazon Web Services (AWS) providing a channel for Siemens Healthineers Ultrasound service to respond to customer requests for reactive and interactive services, such as remote technical support and remote applications support.

This solution has been designed to provide a secure and efficient way to connect and to troubleshoot customer systems while keeping data safe. This white paper contains information about different security measures implemented in Kinectus, including security measures in the remote service delivery process, security measures in applications software, security measures for data in transit, security measures in infrastructure and protection against malicious attacks.

SIEMENS Healthineers

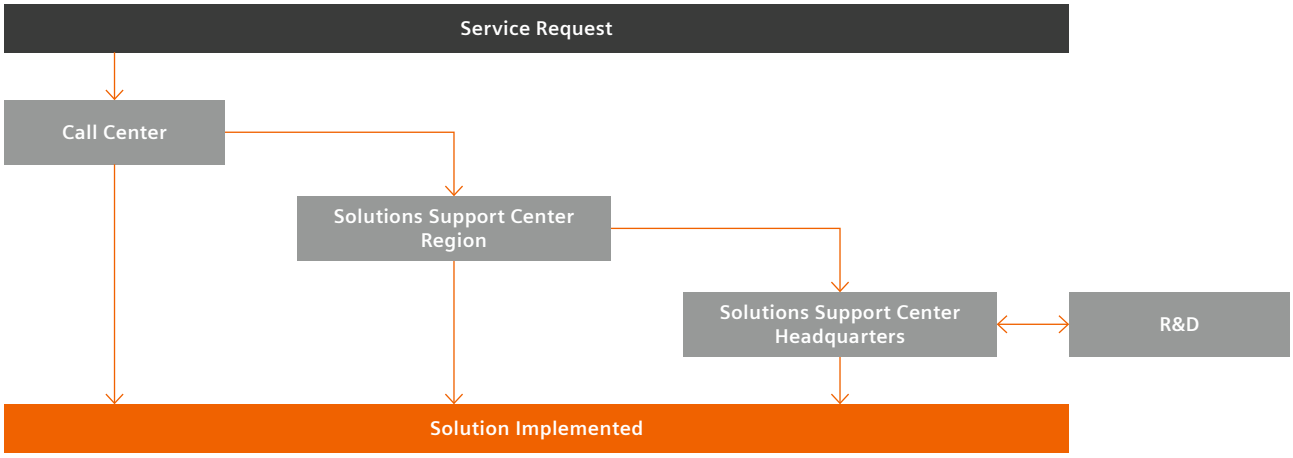

Figure 1: Service escalation process

Security measures in the remote service delivery process

Kinectus enables the Siemens Healthineers Ultrasound service organization to provide remote technical and applications support. The service escalation process follows a multi-step approach that provides remote trouble-shooting and expert support for Siemens Healthineers ultrasound products (Figure 1).

The service engineers from the Regional Solutions Support center provide second-level support and access customer systems remotely for early diagnosis and trouble-shooting. In addition, a service engineer from the Headquarters Solution Support team may also access customer systems remotely to provide support on issues requiring third-level attention.

Security measures in applications software

Kinectus includes security measures in Ultrasound applications software to support data security throughout the entire remote interaction. The level of access granted to a system running Ultrasound applications software is determined by the customer.*

Customers can block remote desktop access, locally on the ultrasound system, by setting No access mode in Remote Service Access Control. The No access mode blocks remote desktop access to all Siemens Healthineers support specialists (remote technical and applications support).

Customers can allow remote desktop access by taking the ultrasound system out of No access mode (Figure 2).

**Supported by Kinectus 2.0 and above*

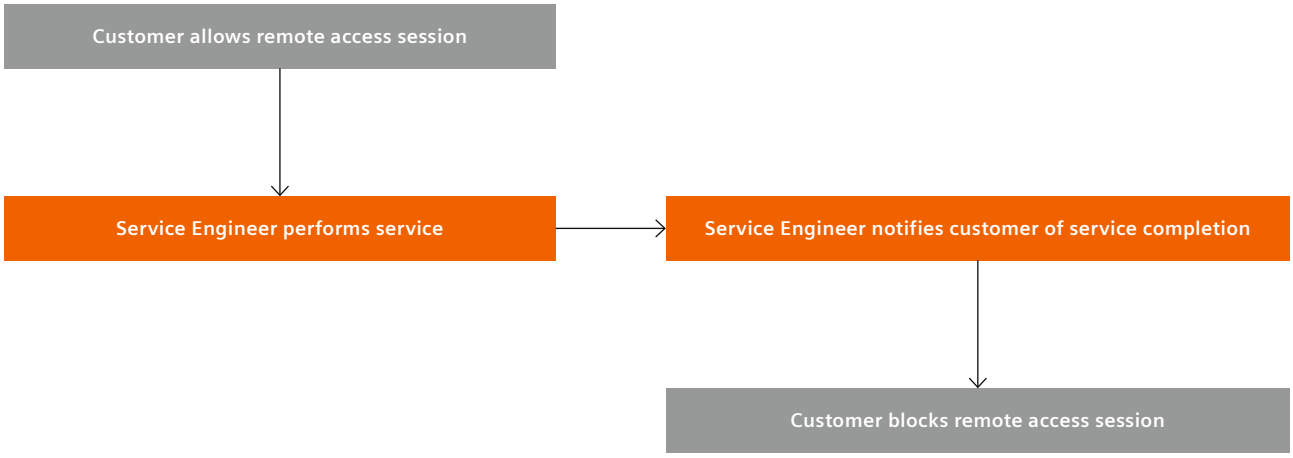

Figure 2: No access workflow example

Security measures for data in transit

Encrypt Data in Transit

To securely transport data between the customer ultrasound system and the Kinectus infrastructure, a secured, encrypted connection is employed. The connection can be routed through the customer's own firewall giving them full control over communication.

Data transfers are encrypted by design. Kinectus traffic is encrypted in transit using Transport Layer Security 1.2 (TLS) with an industry-standard Advanced Encryption Standard (AES) cipher. TLS is a set of industry-standard cryptographic protocols used for encrypting information that is exchanged over the network. If proxy access is allowed on the customer network, the HTTP CONNECT method is used as well for HTTP tunneling through the Kinectus infrastructure proxy server.

Port Requirements

Customers may configure their own firewalls to allow or block proxy access. If proxy access is allowed, the customer network requires only one open outbound TCP port (443) to a single IP address. If proxy access is not allowed (blocked), the customer network requires only one open outbound TCP port (443) to any IP address. The customer network does not require any open inbound ports. The Kinectus connection is always initiated from the ultrasound system residing on the customer network; traffic always flows outward from the ultrasound system to the Kinectus infrastructure first, over TCP port (443), before reflexive traffic flows inward from the Kinectus infrastructure to the ultrasound system (Figure 3).

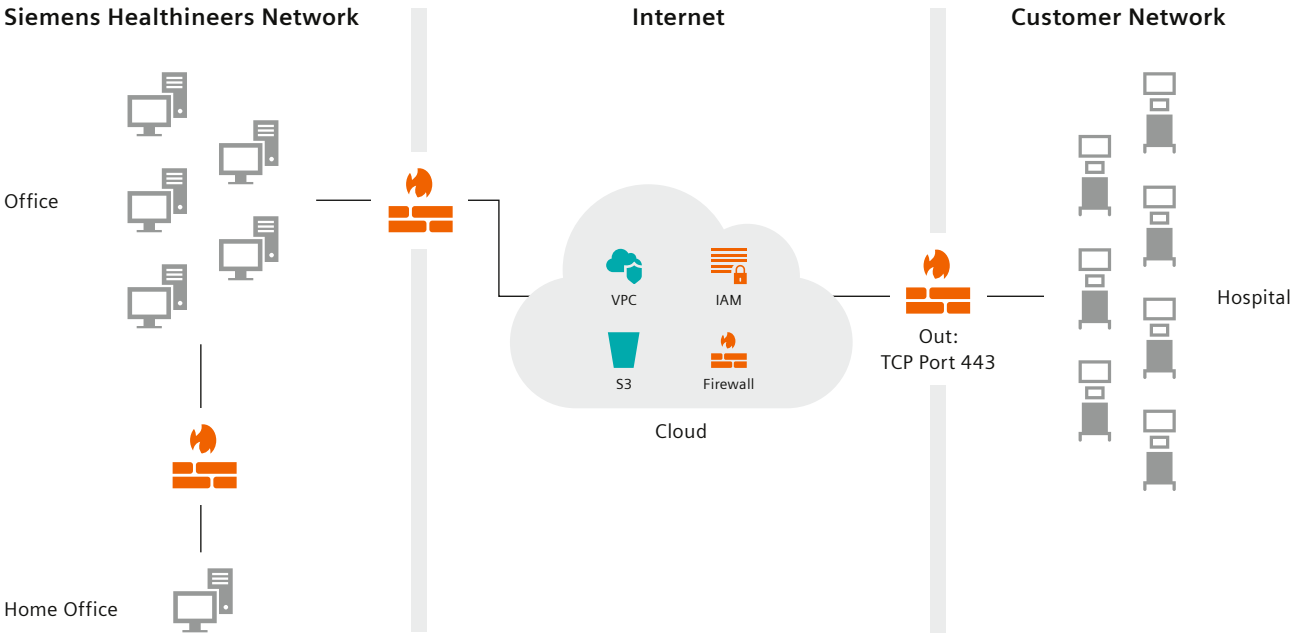

Figure 3: Security measures diagram

Security measures in infrastructure

The Kinectus infrastructure includes security measures to protect against malicious attacks. The AWS Well-Architected Framework is used to help build the secure Kinectus infrastructure.

The infrastructure includes several security measures to protect against unauthorized access and data breaches. These measures include:

Authentication and Authorization

User connections to the infrastructure are secured and authenticated using Microsoft Entra ID (Azure Active Directory) and AWS Identity and Access Management (IAM), and access to resources is restricted based on the principle of least privilege. Access to Kinectus is restricted to trained and authorized personnel only. Remote access is restricted to employees of Siemens Healthineers with appropriate authentication credentials. In Kinectus, there are service and applications user accounts required to manage the functions of the product. Users must have a valid user account to access the system using Single Sign-On (SSO) and Multifactor Authentication (MFA). Every user has a unique account. User access rights are controlled through a role-based access control (RBAC) system. User access is automatically disabled upon change of employment status. Key remote interactions between the Siemens Healthineers Ultrasound Support specialist and the customer's connected ultrasound system are recorded and available for audit. Remote user, ultrasound system serial number and date time information is recorded for activities, including, but not limited to remote session start/stop, ultrasound system log collection and software distribution.

Encrypt Data at Rest

Kinectus utilizes Amazon S3, an object storage service offering industry-leading scalability, data availability, security and performance. All Kinectus object uploads to Amazon S3 are automatically encrypted using 256-bit Advanced Encryption Standard (AES-256).

Ultrasound system log collection is triggered through two different mechanisms: User-initiated transfers and infrastructure-initiated transfers. Ultrasound system device logs can be uploaded to a secured, encrypted Amazon S3 bucket in the Kinectus infrastructure (Figure 3).

All uploaded ultrasound system device logs are exclusively stored in a European Union (EU) cloud region within the Kinectus infrastructure.

Firewall Protection

The infrastructure is protected by a firewall that helps restrict access. The firewall also monitors network traffic and blocks suspicious activity (Figure 3).

Vulnerability Management

The infrastructure components are regularly scanned for security and vulnerability issues. Any identified security or vulnerability issue is promptly addressed and remediated.

Physical and Environmental Controls

AWS protects the infrastructure that runs all services offered in the AWS cloud. This infrastructure is composed of the hardware, software, networking and facilities that run AWS cloud services.

Protection against malicious attacks

In addition to the security measures described above, Kinectus also includes protection against various types of malicious attacks, including:

Denial of Service (DoS) Protection

The infrastructure includes DoS protection mechanisms to prevent or mitigate the effects of DoS attacks.

Intrusion Prevention

Intrusion Prevention measures are implemented in the infrastructure to prevent unauthorized access and ensure that only authorized personnel can access the system.

Conclusion

Kinectus provides secure remote access for ultrasound systems, ensuring that sensitive data is protected throughout the entire service delivery process.

The security measures implemented in the solution include access controls, encryption, network controls and protection against malicious attacks. These measures work together to provide a secure and reliable remote connectivity solution for Siemens Healthineers customers. Multiple layers of security controls are placed on the ultrasound system as well. For more information about these controls, please refer to the product-specific security white paper and/or Manufacturer Disclosure Statement for Medical Device Security (MDS2).

Please note:

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 Healthineers sales organization worldwide. Some/all of the features and products described herein may not be available in the United States.

The information in 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.

Any technical data contained in this document may vary within defined tolerances.

Amazon, Amazon Web Services, AWS and all related marks are trademarks of Amazon.com, Inc. or its affiliates.

Microsoft is a registered trademark of the Microsoft Corporation in the United States and other countries.

At Siemens Healthineers, we pioneer breakthroughs in healthcare. For everyone. Everywhere. Sustainably. As a leader in medical technology, we want to advance a world in which breakthroughs in healthcare create new possibilities with a minimal impact on our planet. By consistently bringing innovations to the market, we enable healthcare professionals to innovate personalized care, achieve operational excellence, and transform the system of care.

Our portfolio, spanning in vitro and in vivo diagnostics to image-guided therapy and cancer care, is crucial for clinical decision-making and treatment pathways. With the unique combination of our strengths in patient twinning[1], precision therapy, as well as digital, data, and artificial intelligence (AI), we are well positioned to take on the greatest challenges in healthcare. We will continue to build on these strengths to help overcome the world's most threatening diseases, enable efficient operations, and expand access to care.

We are a team of more than 71,000 Healthineers in over 70 countries passionately pushing the boundaries of what is possible in healthcare to help improve the lives of people around the world.

[1] *Personalization of diagnosis, therapy selection and monitoring, after care and managing health.*

Siemens Healthineers Headquarters
Siemens Healthineers AG
Siemensstr. 3
91301 Forchheim, Germany
Phone: +49 9191 18-0
siemens-healthineers.com

Manufacturer
Siemens Medical Solutions USA, Inc.
Ultrasound
22010 S.E. 51st Street
Issaquah, WA 98029, USA
Phone: 1-888-826-9702
siemens-healthineers.com/ultrasound

Published by Siemens Medical Solutions USA, Inc. · QR700005178 · 14590 0224 online · © Siemens Medical Solutions USA, Inc., 2024