# Advanced protection from cybersecurity threats

CARESCAPE Network and CARESCAPE Gateway - Cybersecurity Fundamentals

**INTRODUCTION**

GE Healthcare's CARESCAPE™ Network and CARESCAPE Gateway offer an unparalleled ability to capture patient data in real-time and deliver integrated data across the enterprise to support informed decision-making by healthcare providers. The CARESCAPE Network is an Ethernet-based network connecting GE patient monitors to clinical and hospital networks and servers and carefully balances the delivery of robust patient care with the ever-growing need to protect the privacy and security of personal health information. This white paper addresses the system and patient data security aspects of the network components and the gateway connecting them.

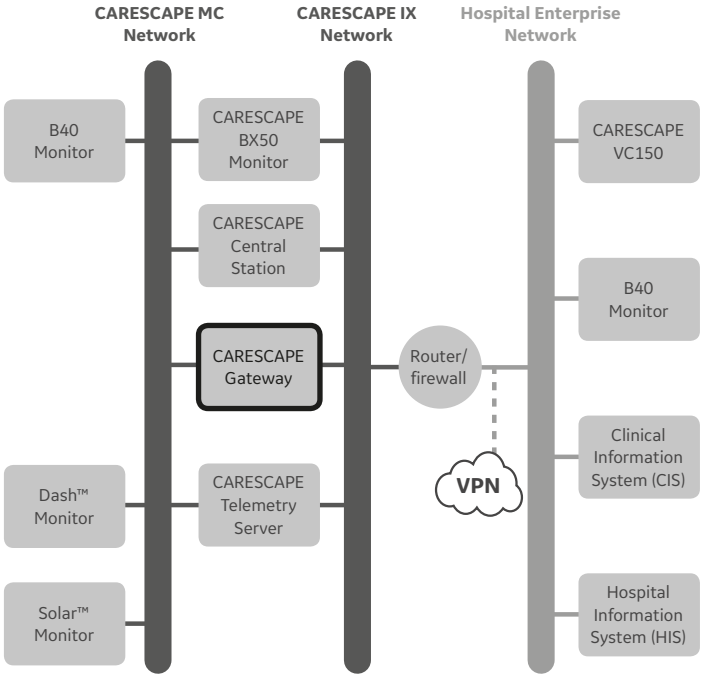
**ARCHITECTURE**

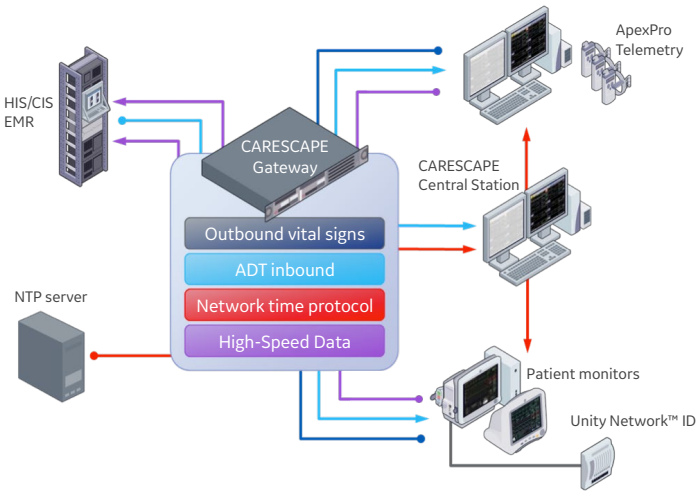
The CARESCAPE Network architecture is composed of the mission-critical (MC) network, the information exchange (IX) network, and the CARESCAPE Gateway.

The CARESCAPE MC Network is used to connect patient monitors, central stations, and the CARESCAPE Gateway. The CARESCAPE MC Network carries real-time patient monitoring data such as parameters, waveforms, control channels, trends, alarm histories, and the like, along with device discovery and alarms.

The CARESCAPE IX Network carries non-real-time monitoring data, for example, processed full-disclosure data between devices and for printing files, and device servicing data, such as remote access for configuration, desktop viewing, and GE Healthcare's remote servicing. The CARESCAPE IX Network is also used for connecting to the hospital networks and enterprise clinical data systems via a router/firewall.

The CARESCAPE Gateway provides a mechanism for exchanging information between systems on the hospital's enterprise network and devices on the MC network via the IX network. It forms a secure data bridge so data residing on either network can be shared across the two networks.






The CARESCAPE Gateway provides the following functions:

- **Outbound vital sign data** in an HL7® format from patient monitoring devices to hospital information systems
- **Inbound ADT information** from the hospital information system to patient monitoring devices on the MC network to minimize incorrect data entry
- **An network time protocol (NTP) time source** to the CARESCAPE Network's Time Master to synchronize the clocks on CARESCAPE Network
- **Near real-time streaming data** in an XML format for vital sign data and waveforms from patient monitoring systems

## NETWORK SECURITY

The MC and the IX networks are designed to provide a balance between functionality and security. The networks have different security features and postures that match their clinical role.

### MC Security

The CARESCAPE MC Network is an isolated, non-routable network engineered to provide unparalleled performance between patient monitors, central workstations, clinical information centers, and interconnectivity components; the MC network has no direct access to hospital or public networks. This isolation assures a high degree of security for the real-time data transported on this network. GE requires that all GE monitoring connections, for example, cabling and VLANs, be devoted to the monitoring system due to the life-critical and mission-critical nature of the patient monitoring system.

### IX Security

The CARESCAPE IX Network is a routable network that acts as a conduit for non-real-time information to components attached to the network and to systems in the hospital enterprise network. The IX network is separated from the MC network by the CARESCAPE Gateway which can securely transfer data from one network to the other. The IX network is also separated from the hospital enterprise network by a Layer 3 IX network router/firewall that employs a number of features to ensure security:

- Extended access control lists are used to ensure that only authorized systems have access to data from the IX network.
- The router/firewall can only be managed from the IX network; it cannot be managed from the hospital enterprise network.
- The router/firewall supports a VPN tunnel for remote service access.

The secure data link provided by the IX network router/firewall must be installed and properly configured between the IX network and the hospital enterprise network to ensure data security.

## GATEWAY SECURITY

The CARESCAPE Gateway is an application that comes pre-installed on hardware supplied by GE Healthcare. The CARESCAPE Gateway is intended to electronically transfer data to and from medical devices, however, it is not intended to control any monitoring functions of the monitoring devices to which it connects, nor is it intended to be used in the monitoring of the patients connected to the devices. The typical "user" is an information system or application that resides outside of the monitoring network that needs this data (e.g., a CIS system). The CARESCAPE Gateway has no clinical user interface; the only user interface is web-based and is intended only for administrators of the device. The CARESCAPE Gateway itself operates unattended and is not located near the patient or caregiver.

### Cyberthreat Protection

The threat from malicious software continues to grow through computer viruses, worms, Trojan horses, denial-of-service attacks, and other malware. The CARESCAPE Gateway is engineered and hardened to be resilient against malware. As with any threat protection system, a layered approach is usually the most effective, and is the approach employed with the CARESCAPE Gateway system. Hardening in combination with a secure network help ensures maximum protection and up-time.

Intelligent whitelisting protection against advanced persistent threats (APTs) is at the heart of the system's defense. Whitelisting is an advanced form of traditional, signature-based, anti-threat system scanning technology. With whitelisting, only authorized applications are allowed to execute. By default, any attempt to execute, modify files on disk or change system memory by unknown software is denied. In addition, whitelisting continually verifies the integrity of approved applications and libraries to ensure they haven't been tampered with. If the integrity checks fail, they will not be allowed to execute. Therefore, even if an application or platform vulnerability is exploited, the threat cannot execute or create damage.

Intelligent whitelisting:

- Eliminates the need to download and update threat definitions or signatures
- Protects against zero-day and advanced persistent threats
- Allows for software updates and patches only via signed software
- Allows for deterministic application execution, with low overhead

While intelligent whitelisting is an extremely powerful and robust technology, the CARESCAPE Gateway employs many other security solutions, mechanisms, and design philosophies to ensure total protection:

- A host firewall is enabled for network connections.
- Only necessary application ingress and egress ports are open to the enterprise network minimizing the attack surface. The full list of open ports is available in the product manual.
- Personal health information (PHI) is erased, without the possibility of reidentification, each day from the log files. During the day, some PHI is in the active log file for serviceability and troubleshooting, however, any exportation of log files, even logs for the current day, are immediately deidentified.
- All software updates must have signed software package files before they can be installed.
- Product configuration is managed via encrypted http (https) only. The out-of-box configuration uses a self-signed certificate to ensure security by default, however, GE recommends that the customer installs and manages their own certificate.
- There is minimal transfer of PHI on the enterprise network. All physiological, device and event data is only identified by a UUID (Universally Unique Identifier), without embedding any PHI in the data. UUID-to-patient association is performed with minimal transactions.
- Root access, sudo and ssh are disabled.
- Software integrity checking is continuously performed as a background task.
- Following the security best practice of "Least Privilege", software processes run with minimal permissions, primarily in user-space.
- A Linux® CentOS 6 base, with minimal packages included in the distribution. Only necessary services are enabled and running. Common threat vectors such as email clients and media players are not installed on the device.
- All user activity is maintained in an audit log.

**Secure Software Development**

The CARESCAPE Gateway software was developed in accordance with GE Healthcare's Design Engineering for Privacy and Security (DEPS) process. The DEPS process ensures that security is designed into the product at all phases of the product lifecycle. Upon initiation of development, a privacy impact assessment was performed to identify any private information that would require special consideration. A security risk assessment was completed to identify risks and describe mitigations for those risks. Threat modeling was performed to further identify potential risks to the system and highlight areas that would require increased attention. A failure mode effects analysis was employed to discover possible risks resulting from failures. During development, secure coding practices were utilized to prevent the introduction of common vulnerabilities. Tools such as static and dynamic code analysis were used throughout the software development lifecycle to continuously assess the code for vulnerabilities. This process resulted in a product that has been designed and developed with security as a guiding principle.

## PRIVACY PROTECTION

The CARESCAPE Gateway does not allow PHI to be exported to removable media, such as USB media.

Point-of-care devices on the CARESCAPE Network, such as patient monitors, are typically in a "discharged" state when not in use. No confidential or restricted data is in memory and all data from the previous case has been erased from the device (name, patient ID, height, weight, etc.).

Patient data (patient identification, parameter values, trends, etc.) on the monitor and in transmissions on the MC network is not encrypted, but the transmission protocol is proprietary and includes CRC for error detection.

HL7 is used to transmit patient data from the IX network to clinical information systems or hospital information systems on the hospital enterprise network via the CARESCAPE Gateway. These data streams are not encrypted but the destinations are controlled by the IX network router to specific, authorized systems.

## SUMMARY

The security features of the CARESCAPE Network and the CARESCAPE Gateway provide a high level of protection and privacy for patient data while still permitting ease of use and outstanding patient care and safety. Leveraging best-in-class security solutions and design techniques are critical as new devices are integrated onto the hospital enterprise network and with the advanced security features of the CARESCAPE Network and CARESCAPE Gateway, GE Healthcare is striving to ensure our solutions meet and exceed the high bar set by healthcare institutions. In addition, it is our goal to minimize the time and effort (and worry) of installation by choosing technologies and solutions that are as close to "set and forget" as possible. While the security technology landscape is continually evolving, our products are evolving with it.

## Imagination at work



JB52716XX 10/17