SonoDefense:

Advanced cybersecurity and data privacy protection

Healthcare institutions are under growing threat of cyberattack – and the impact is staggering. More than 176 million healthcare records were exposed or stolen between 2009 and 2017, which equates to breaches affecting over 50% of the U.S. population.[1] Data breaches in healthcare cost $380 per record on average, more than 2.5 times the global average across all industries.[2]

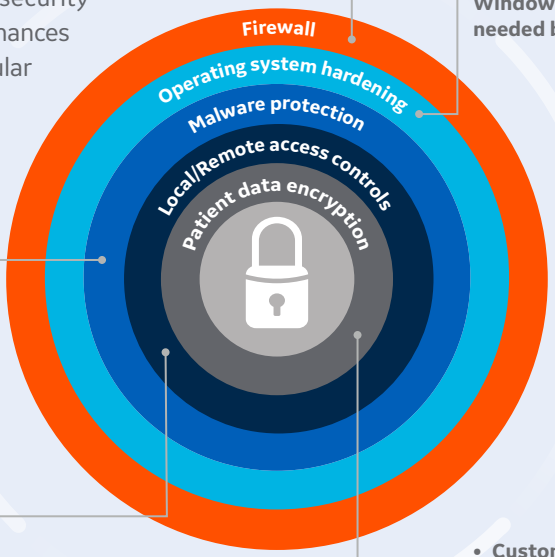
Protecting against these threats and safeguarding your patients and your institution requires more than anti-virus protection. SonoDefense is GE Healthcare's multi-layer strategic approach to cybersecurity and patient data privacy for the LOGIQ™ E10 system.

It is designed to:

- Keep the ultrasound machine safe and functional in the face of cyberthreats
- Protect patient data on the machine from unauthorized access
- Enable you to successfully implement HIPAA and security policies, while still managing productive daily workflows

Defense-in-Depth Strategy

SonoDefense is designed for maximum security protection with a defense-in-depth strategy that incorporates security controls deployed in multiple layers. This approach enhances security by protecting the system against any particular attack using several independent methods.



Blocks unused communication channels

Disables services in the Windows® 10 OS that are not needed by the LOGIQ E10

Reduces potential points of attack

Limits what can be run on the LOGIQ E10

- **Customizable, role-based access**
- **Federated Identity Management**
- **Session management**
- **Auditing**
- **Secure remote access**

- **Customizable patient data encryption**
- **Enterprise wireless encryption**
- **IPv6 Internet Protocol address standard**

The SonoDefense defense-in-depth strategy consists of FIVE LAYERS, with each layer enhancing the overall security of the system and helping to protect patient data.

LAYER 1

Firewall

A malicious cyberattack requires a point of entry. The strict firewall layer reduces the potential points of attack by disabling all unused ports.

LAYER 2

Operating system hardening

The LOGIQ E10 operating system is Windows 10 IoT, a componentized version of Windows 10 specifically made for embedded systems with an extended support model. Its applications are vast compared to the needs of the LOGIQ E10. Accordingly, we have configured the system so that all software services embedded in the operating system that are not explicitly needed to run the medical applications are removed or disabled. This "hardening" minimizes the parts of the system that are exposed to threats, helping to reduce the potential for attack. The Windows 10 IoT configuration, including security profiles, are set using guidance from standards including Defense Information Systems Agenda (DISA) Standard Technical Implementation Guides (STIGs), National Institute of Standards and Technology (NIST) Cybersecurity Framework, and Center for Internet Security (CIS) best practices.

LAYER 3

Malware protection

The Windows 10 security features provide the foundation for SonoDefense's malware protection, enforcing restrictions on applications that can be run on the LOGIQ E10 system.

- Kiosk mode for the clinical application disables the user's access to the internet and the Windows desktop, which are common malware vectors for spreading viruses through email services, web browsers, and other applications
- Media auto-run is disabled and BIOS access requires a password
- EMET and Windows Defender actively monitor for malware behavior

LAYER 4

Access Controls

SonoDefense provides cyberdefense for the real world of patient care. Its extensive customizable, role-based user access enables users to successfully implement HIPAA and security policies, while still ensuring efficient and productive daily workflows.

- ***User roles*** – Custom creation of user roles and the ability to assign rights to those roles
- ***User management*** – Individual users are created and assigned customizable roles, dictating their allowable access to and manipulation of patient data and system configuration
- ***Password policies*** – Configurable across all attributes including length, content, reuse and expiration
- ***Federated identity management*** – Lightweight Directory Access Protocol (LDAP), or single sign-on, can be used to manage users consistently across your enterprise
- ***Session management*** – System access can be restricted after a configurable period of inactivity
- ***Audit report*** – Patient data and system access are recorded in a log to facilitate an incident investigation
- ***Remote service access*** – Remote service is only allowed if authorized by local user on device
- ***Local service access*** – Managed via role-based Secure Service Access (SSA)

LAYER 5

Encryption

The encryption layer of SonoDefense security software is designed to protect data privacy and assist your organization in complying HIPAA/HITECH regulations. Safeguards include:

- All patient data on the system's patient archive drive can be encrypted to provide protection in the event of a stolen device or hard drive
- Support for IPv6 includes IP Security (IPsec) for encrypted networking communication and node authentication
- Wireless network communication can also be encrypted including enterprise level protocols
- All remote service access is encrypted using FIPS compliant algorithms

Security-related features

All features are standard

Firewall policy blocks all unnecessary ports	
OS – Windows 10 IoT	
OS hardening	• Configuration settings use guidance from DISA STIGs, NIST Cybersecurity Framework, and CIS best practices • Disabled unnecessary services and protocols
Media export security	• Provides the ability to disable export of patient data to removable media. Configurable at system level or individual user level
Malware protection	• Disable auto-run for removable media • Kiosk mode • EMET and Windows Defender

Access and Access Level *(Requires administrator right)*	
Ability to create user groups	
Ability to assign patient data access rights to each group	• Create • Update/Access • Delete • Export (removable media)
Ability to assign other rights	• Administrator • Configuration adjustments - Basic - Imaging - Advanced • Audit and system logs - Capture - Capture with PHI • Active Service Desktop
Create users and assign to groups	
Configurable emergency user rights	
Choose login ID list (enabled or disabled)	
Passwords	• Usage (enabled or disabled) • Policies – provides the ability to specify password policies for local accounts - Password cannot contain user name (on/off) - Password history (0-25) - Minimum password length (1-20 characters) - Minimum password age (0-168 hours)
Passwords, *continued*	- Maximum password age (30-365 days) - Password complexity • Minimum number of character sets (0-4) • Minimum number of upper case characters (0-3) • Minimum number of lower case characters (0-3) • Minimum number of digits (0-3) • Minimum number of symbols (0-3) - Account lockout policies • Failed logins before account blocked (off, 1-10) • Account block time (0-60 minutes)
Session Management	• Lock Screen timeout – automatically locks screen and requires password reentry after specified period of inactivity (disabled, 1-60 minutes) • Auto logoff timeout – automatically logs off a user after the specified period of inactivity (disabled, 1-60 minutes)

Local user management policy *(Requires administrator right to configure)*
User management restricted to administrator rights
Local user management
User display ID can be unique from login ID
Ability to temporarily disable a user
Ability to force a password reset
Support for multiple unique user accounts
Support for multiple unique administrator account
Can combine with remote users

Remote user management policy *(Requires administrator right to configure)*
Supports active directory authentication utilizing LDAP
Support for individual accounts and AD groups for users and administrators
May utilize LDAP or secure LDAP
Customer may configure the system to perform authenticated binding
Can combine with local users
Customizable mapping to local groups for rights management

Security-related features, *continued*

All features are standard

Remote Service Access
FIPS 140-2 compliant encryption
Remote control is only allowed if authorized by local user on device
No open ports required

Additional Features	
Local service access	• Secure Service Access (SSA)
Hard drive encryption	• AES-256 • USB key or manual password entry
Audit and system log creation with or without PHI	
Wireless security protocols	• WPA2-Personal • WPA2-Enterprise • 802.1x • Intel-CCKM-Enterprise • Enforced FIPS 140-2 compliance capability
Internet Protocol address standard	• IPv4 • IPv6

References:

1. "Healthcare Data Breach Statistics." HIPAA Journal, Mar 22, 2018.
2. "Healthcare Data Breach Costs Highest for 7th Straight Year." Health IT Security, June 20, 2017.

Imagination at work

April 2018 JB57429XX