SonoDefense

Advanced cybersecurity and data privacy protection

Healthcare institutions are under growing threat of cyberattack – and the implications for data security, patient privacy, and the quality and cost of care are staggering.

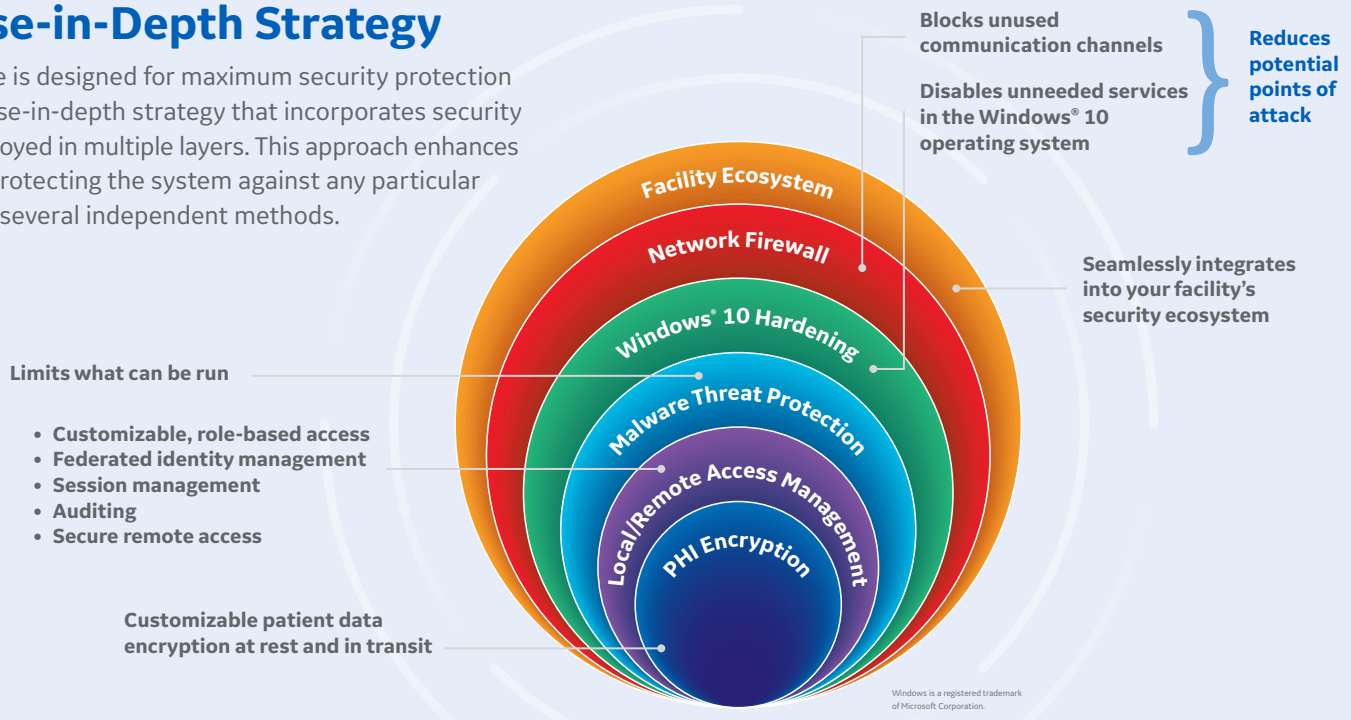
Protecting against these threats and safeguarding your patients and your institution requires more than anti-virus protection. SonoDefense is GE Healthcare's multi-layer strategic approach to cybersecurity and patient data privacy for ultrasound.

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.



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

LAYER 1

Facility Ecosystem

SonoDefense is designed to fit seamlessly into your facility's existing security ecosystem. Vulnerability scan mode allows the scanner to be integrated into a facility's vulnerability assessment infrastructure.[1]

LAYER 2

Network Firewall

A malicious cyberattack requires a point of entry. The strict firewall layer reduces the potential points of attack by disabling all unused ports and the DICOM® firewall limits DICOM connections to customer defined devices.

LAYER 3

Windows 10 Hardening

Windows 10 IoT is a version of Windows 10 specifically made for embedded systems with an extended support model. Its applications are vast compared to the needs of the SonoDefense-enabled scanner. 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, is 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 4

Malware Threat Protection

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

- Known malicious software and potentially unwanted applications (PUAs) are explicitly blocked
- Whitelisting only permits trusted applications that meet secure implementation guidelines to run on the ultrasound system
- Kiosk mode 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
- Security tools actively monitor for malware behavior

LAYER 5

Local/Remote Access Management

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 assignment rights for roles puts the institution in control
- ***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*** – Policies include length and content
- ***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 period of inactivity
- ***Audit report*** – An extensive list of events, including patient data and system access, are recorded in an audit log to facilitate an incident investigation
- ***Centralized logging support***[4] – Supports industry standard syslog protocol with optional encryption for transmitting system and audit logs to customer controlled log server
- ***Remote service access*** – Remote service is only allowed if authorized by local user on device
- ***Local service access*** – Protected by a two-factor authentication scheme

LAYER 6

PHI Encryption

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

- Data on the system's customer data volumes can be encrypted to provide protection in the event of a stolen device or hard drive
- Patient data can be deleted from the hard drive in a way that is cryptographically unreadable and unrecoverable
- Support for IPv6 includes IP Security (IPsec) for encrypted networking communication and node authentication
- DICOM Transport Layer Security (TLS) encrypts both wired and wireless DICOM communications[2]
- Wireless network communication can be encrypted with industry standard protocols[2]
- All remote service access is encrypted using FIPS compliant algorithms

Security-related features for LOGIQ™ ultrasound scanners[5]

All features are standard unless otherwise noted

Firewall policy blocks all unnecessary ports and limits DICOM communications to only defined devices	
OS – Windows 10 IoT	
OS hardening	• Configuration settings use guidance from DISA STIGs, NIST Cybersecurity Framework, and CIS best practices • Disabled unnecessary services, protocols and telemetry • Secure boot
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	• Explicit blocking of known malicious software and PUAs • Whitelisting • Device Guard • Disable auto-run for removable media • Kiosk mode • Windows Defender

Access and access level *(Requires administrator right to configure)*	
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[4]	
Choose login ID list (enabled or disabled)	
Passwords	• Usage (enabled or disabled) • Policies – provides the ability to specify password policies for application user accounts – Password cannot contain user name (on/off) – Password history (0-25)
Passwords, *continued*	– Minimum password length (1-20 characters) – Minimum password age (0-168 hours) – 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) • Customizable pre-login notice for users
Security baseline[4]	• Allows an administrator to conveniently select from several factory configured security policy options as a starting point

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 accounts
Can combine with remote users

Security-related features, *continued*

All features are standard unless otherwise noted

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

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

Additional features	
Local service access	• Secure Service Access (SSA)
Windows local user accounts	• Passwords for all accounts may be changed
Hard drive encryption[6]	• AES-256 • Automatic unlock tied to system hardware,[4] USB key, or manual password entry
Syslog client for distributed log file processing[4]	
Wireless security protocols[2]	• WPA2-Personal • WPA2-Enterprise • 802.1x • Enforced FIPS 140-2 compliance capability
Internet protocol address standard	• IPv4 • IPv6
Secure delete to render deleted patient data unreadable and unrecoverable	
DICOM TLS	
Vulnerability scan mode[1]	• Nessus®
Software security updates[4,5]	• Customer can download and install digitally signed software security updates on the system

Auditing	
Audit and system log creation with or without PHI[4]	
Sample audit events	• System startup and shutdown • User login and logout • Transfer of DICOM instances • Data Import/Export • Display, modification, and deletion of images and patient information • User management events • Network, security and system configuration changes

References:

1. Vulnerability scan mode is an optional system feature and is available on LOGIQ E10 and E10s only.
2. Wireless connectivity is an optional system feature.
3. Unless otherwise noted, the SonoDefense feature set described in this document applies to: LOGIQ E10/E10s R2 software, LOGIQ S8 R4.2.5x software and LOGIQ P9/P7 R3.0.8.
4. Not available on LOGIQ S8.
5. Not available on LOGIQ P9/P7.
6. Only available on the patient data drive on LOGIQ S8.

March 2020 JB66757XX(1)