Ultrasound Cybersecurity

GE HealthCare

Cyberattacks are the largest threat to hospitals, according to a recent report from The U.S. Department of Health and Human Services.[i]

And the problem isn’t limited just to expenses, inconveniences, and loss of productivity. In healthcare, cyber vulnerabilities can impact care.

"These attacks are not only affecting patient care and safety, they are also creating fear and confusion while eroding the public's trust and faith in our hospital systems throughout the U.S., potentially leading to public health challenges."

—The U.S. Department of Health and Human Services.[i]

A June 2023 report referred to healthcare as “a sector under siege,” noting that the

Clinical settings are “highly targeted by ransomware gangs, which results in both the loss of use of their systems—potentially with life-threatening consequences—as well as data breaches.”[ii]

Cyberattacks on hospitals are growing threats to patient safety, experts say

ABC News | May 10, 2023

Global Healthcare Cyberattacks **increased by 75%** in 2022

The HIPPA Journal

Hacking healthcare: With **385M patient records exposed,** cybersecurity experts sound alarm on breach surge

Healthcare Dive | March 9, 2023

Globally, cyberattacks on healthcare institutions increased 22% from Q1 2022 to Q2 2023, averaging 1,684 attacks per week.

This makes it the third most targeted industry in 2023 — ahead of finance, insurance and communications.[iii]

Cyber breaches in healthcare can impact connected tools essential to care. Patient records, imaging studies, communications links with other providers, payers, labs and more are often compromised.

People, products and systems: Addressing vulnerabilities

Cyber protection is a hospital-wide responsibility, and everybody has a role to play in ensuring security.

Potential vulnerabilities exist with any connected device in the hospital or clinic setting and with individuals accessing information through the hospital systems.

A 2020 report indicates that basic human error, like unauthorized access, poor management of accounts or weak password protection, accounted for 31 percent of healthcare industry breaches in 2019.[iv]


Given the breadth of potential vulnerabilities in global health systems, any cybersecurity plan must be multifaceted and protect the institution, its people and devices in several layers.

PROTECTING ULTRASOUND DEVICES:

SonoDefense

Effective cyber defense is critical in helping to ensure the security of connected imaging devices and healthcare networks as well as important related patient privacy and health information.

Ultrasound devices, which are often portable and frequently move around the facility, have some unique vulnerabilities.

For these devices specifically, SonoDefense is GE HealthCare's strategic, multilayer approach to cybersecurity and patient data privacy. It is designed to:

Keep the ultrasound machine safe and functional in the face of cyber threats.

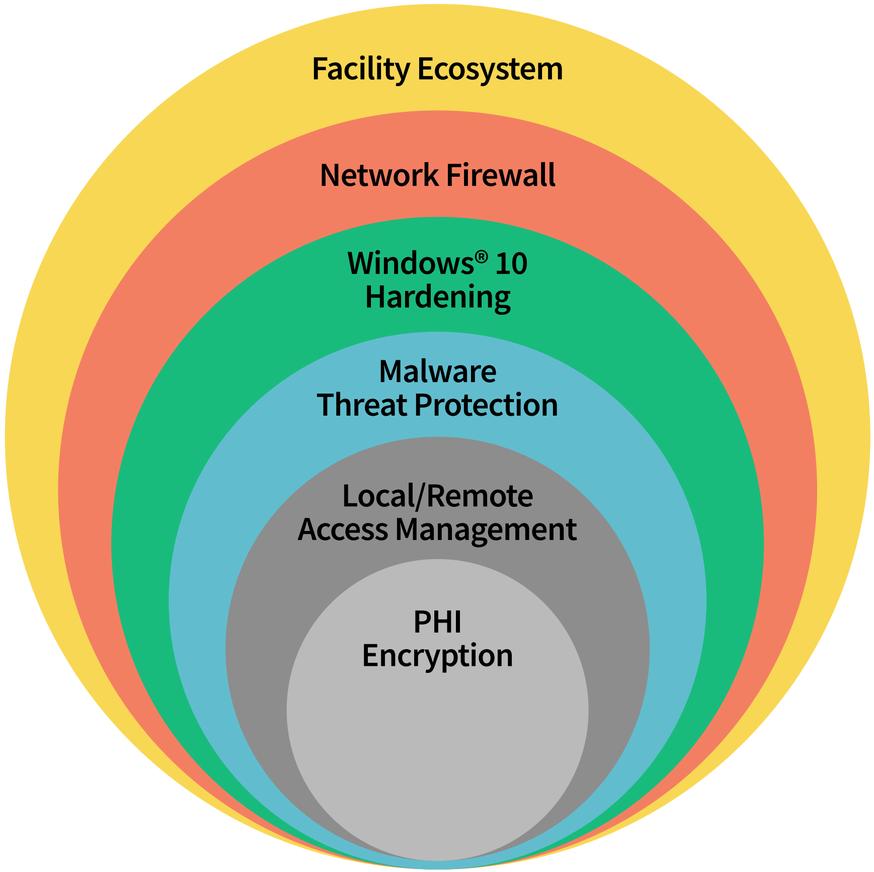
Protect patient data on the machine from unauthorized access.

Enable you to successfully implement HIPAA and security policies, without sacrificing productive daily workflows.

SonoDefense is engineered for maximum protection, complete with multilayered security controls.

SonoDefense six-layer protection at a glance

The six layers of SonoDefense address different vulnerabilities.



Layer 1: SonoDefense fits seamlessly into your **facility's existing security ecosystem**.

Layer 2: A strong **network firewall** limits points-of-entry for bad actors.

Layer 3: **Windows® 10 IoT** security profiles are configured to top industry standards. Hardening minimizes the points of attack by limiting Windows services to only those that are explicitly needed to deliver a world-class ultrasound experience.

Layer 4: Provides **malware threat protection** by enforcing restrictions on applications that can be run on the ultrasound system, such as blocking known malicious software and using trusted application enforcement policies.

Layer 5: The real world of patient care requires that team members access certain information to facilitate efficient and productive workflows. **Local/remote access management** allows for extensive, customizable role-based user access as well as password policies, single sign-on enterprise support, audit reports and more.

Layer 6: **PHI encryption** is designed to protect data privacy by customizable encryption of patient data at rest and in transit to assist your organization in complying with HIPAA/HITECH regulations.

Security that evolves as threats evolve

Cyber threats are ever-evolving, and devices require security that can anticipate and respond.

GE HealthCare’s family of ultrasound products are equipped with eDelivery in some markets. This ensures that as soon as safety patches become available, they can be remotely downloaded.

Your system stays up to date, making it more reliable and secure.

The future of cybersecurity

With cyberattacks expected to grow and bad actors continually finding new ways to breach systems, the need for heightened security isn’t going away.

When the stakes are high, it’s critical that organizations take every opportunity to close the door on would-be hackers.

GE HealthCare’s ultrasound products protected by SonoDefense are one key step to help protect both patients and health systems.

SonoDefense is part of the GE HealthCare ultrasound product suite, including Voluson™ women’s health ultrasound; Venue™ family* point of care ultrasound systems; Vivid™ cardiovascular ultrasound; LOGIQ™ general imaging ultrasound; Invenia™ ABUS ultrasound; and select Versana primary care ultrasound products. Review product-level information for additional information.

*Venue family, as referenced herein, consists of Venue, Venue Go™ and Venue Fit™.

Endnotes

i. Hospital Cyber Resiliency Initiative Landscape Analysis, 2023, U.S. Department of Health and Human Services.

ii. Verizon Business 2023 Data Breach Investigations Report (2023 DBIR).

iii. https://blog.checkpoint.com/research/global-cyberattacks-continue-to-rise/

iv. Verizon Business 2020 Data Breach Investigations Report (2020 DBIR).

GE HealthCare

10/23 JB25844XX