Skeye

gehealthcare.com

Beginning at the end

Today, the world of modern healthcare is universally connected. And those connections—particularly data connections—have helped improve the quality of our care. They keep us closer by putting critical information at our fingertips. But they also carry inherent risks. With more data connections, and more medical devices to maintain and manage, healthcare organizations often lack the time and expertise to protect equipment against critical cybersecurity risks.

To that end—it's also where the future of security begins.

GE Healthcare's Skeye is a cybersecurity solution for networked medical devices, backed by proactive monitoring—across networked medical device end points—regardless of manufacturer.

Larger clinical networks. New risks.

Patient care depends on the interconnectivity and the availability of hundreds of different devices, all of which must be carefully cataloged and monitored to assure their integrity and resilience in the face of cybersecurity threats. And with more and more devices connected to even bigger networks—with varying degrees of protection—managing risk at every endpoint has become more important than ever before.

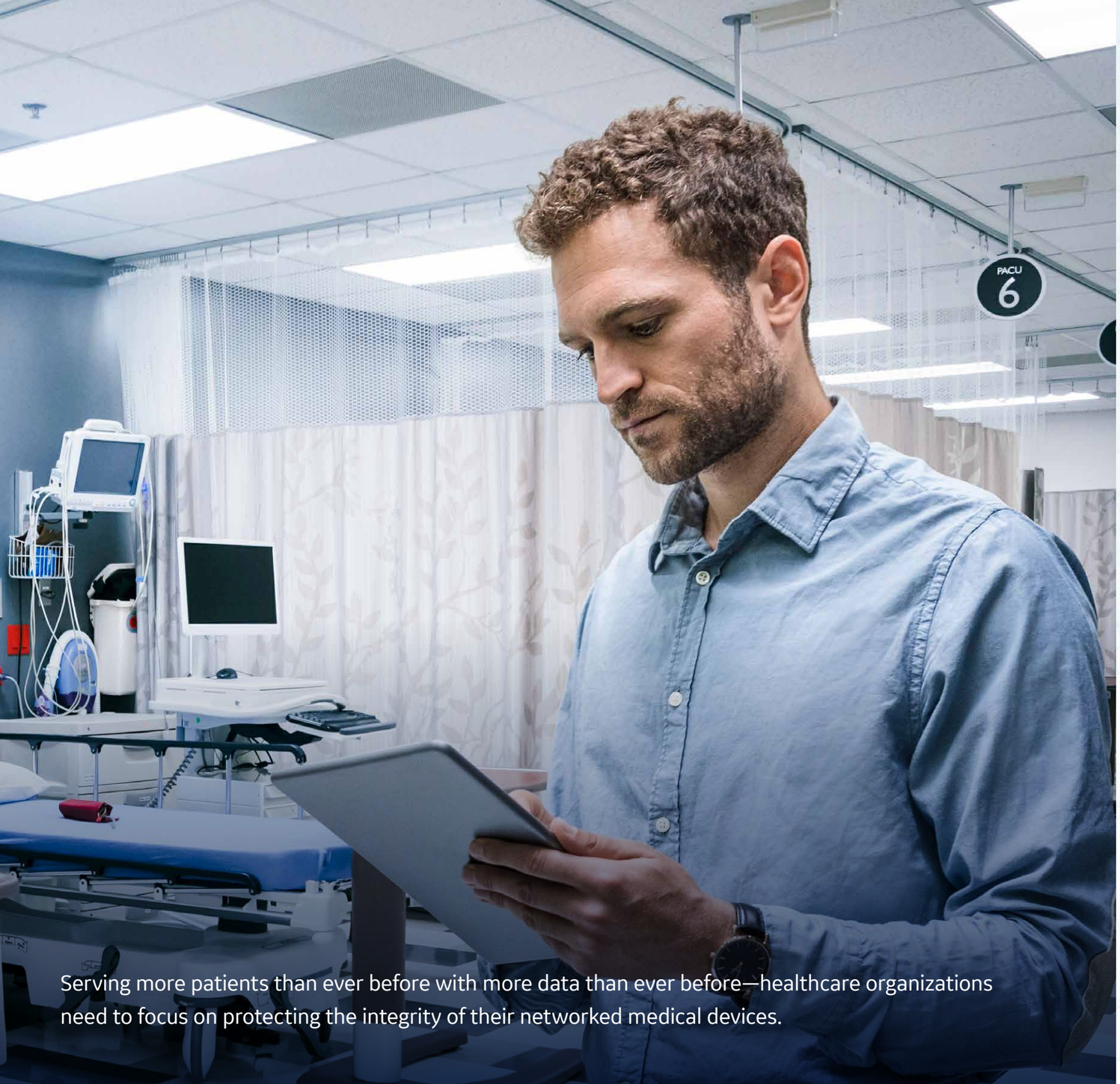
The numbers speak for themselves.

82% of hospital tech experts reported a "significant security incident" in 2018[1]

In 2018, healthcare breach resolution costs were higher than the financial industry at approximately $408 per record[3]

The average cost of a data breach in 2018 was $3.86M[2]

The total cost of healthcare breaches in 2018 was $4.7B[4]



Serving more patients than ever before with more data than ever before—healthcare organizations need to focus on protecting the integrity of their networked medical devices.

Robust

GE Healthcare's managed cybersecurity services for networked medical devices are designed to help assess, understand, protect, facilitate remediation, and support cybersecurity efforts.

Dedicated

GE Healthcare's dedication to cybersecurity is backed by a proactive security operations center (SOC) responsible for monitoring an organization's networked medical device inventory—as well as detecting, analyzing, and responding to security vulnerabilities in real-time.

Inclusive

By design, GE Healthcare's cybersecurity approach helps ensure that networked medical devices within an organization receive the same high level of protection.

Experienced

A leading provider of medical technologies, digital infrastructure, and data analytics solutions, GE Healthcare is a beacon in the medical device protection and cybersecurity space. And as a multi-vendor service provider, customers can also depend on this same expertise to help protect their inventory of networked medical devices—regardless of manufacturer.

360 degrees of defense

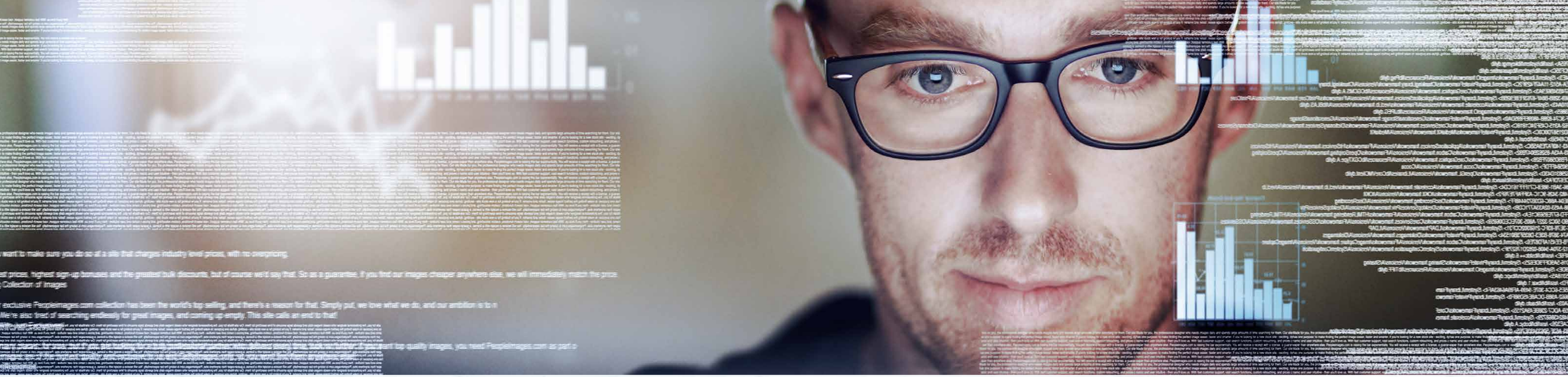
At GE Healthcare, we believe that cybersecurity for your networked medical devices is uniquely complex. That's why we take a proactive approach to combat it—with protection on every level, in every direction. The Skeye solution aligns with the best practices and guidelines of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework, which is a prioritized, flexible, and cost-effective approach to help promote the protection and resilience of critical infrastructure.[5]

Security operations center

Proactive protection. Total peace of mind.

At GE Healthcare, our security operations center (SOC) is the heart of our cybersecurity environment. Our SOC uses sophisticated technologies and artificial intelligence for automated, end-to-end security protection.

- Professionals with cybersecurity and medical device expertise
- Helps detect, analyze, and respond to cybersecurity threats in real-time
- Incorporates artificial intelligence tools for greater insights and faster response times



Protection from every direction

Clinical security assessment

We assess the maturity of your medical device security program by helping to identify risks and vulnerabilities with your clinical systems. And then, we provide in-depth analysis and recommendations on procedures, all while prioritizing risks for an actionable remediation plan.

Device discovery

Using the power of artificial intelligence, we are able to automate networked medical device inventory and learn unique device security risk profiles. This gives healthcare providers automated, real-time management for medical devices from the moment a device is onboarded to the very second it's decommissioned.

Vulnerability management[6]

We help customers detect and analyze vulnerabilities, utilizing passive network analysis rather than traditional (more intrusive) IT methods, and translate remediation recommendations into actionable service requests.

Remediation recommendations

Our cybersecurity team investigates vulnerabilities, helps you create and recommend policies, and provides recommendations that can help protect your assets across diverse groups of medical devices—so you don't have to decommission them.

Remediation execution[6]

Our security operations center staff and on-site field engineers integrate process and technology across functions that gives you better visibility into what's going on: from corrective maintenance work activities to remediation progress and time to completion.

Security event support

We support your in-house security teams by helping provide information and observed behavior of malware, available analytics on that malware, observed threat indicators, and available remediation actions.

Bottom line

In healthcare, the bottom line comes down to your patients. Skeye's AI enabled offering, backed by GE Healthcare's field engineers and dedicated SOC, does more than help protect you against costly cybersecurity threats. It also helps protect your organization's security, profitability, and reputation for delivering care and protection where it matters most—your patients.

Continuous medical device operation and availability

Preserved reputation for delivering high-quality care

Increased patient privacy, security, and data safety

Reduced likelihood of cybersecurity losses

Improved staff and patient confidence

Footnotes

1 https://www.chicagotribune.com/business/ct-biz-hospital-data-breaches-20190307-story.html

2 https://www.healthcare-informatics.com/news-item/cybersecurity/healthcare-data-breach-costs-remaining highest-408-record/

3 https://www.hipaajournal.com/healthcare-data-breach-costs-highest-of-any-industry-at-408-per-record/

4 https://www.healthcaredive.com/news/nearly-300-breaches-last-year-exposed-115m-patient-records-bitglas-says/549296/

5 https://www.nist.gov/cyberframework

6 Applies only to medical devices under GE Healthcare service contract

Imagination at work

JB69507US