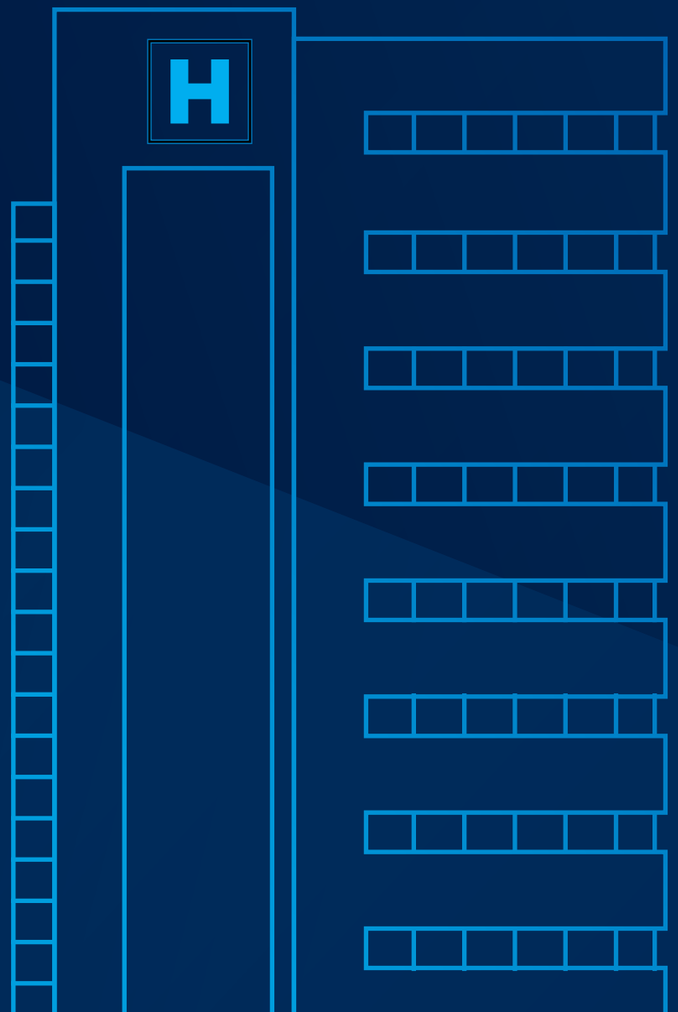
E-BOOK

Protect your patients. Protect your organization.



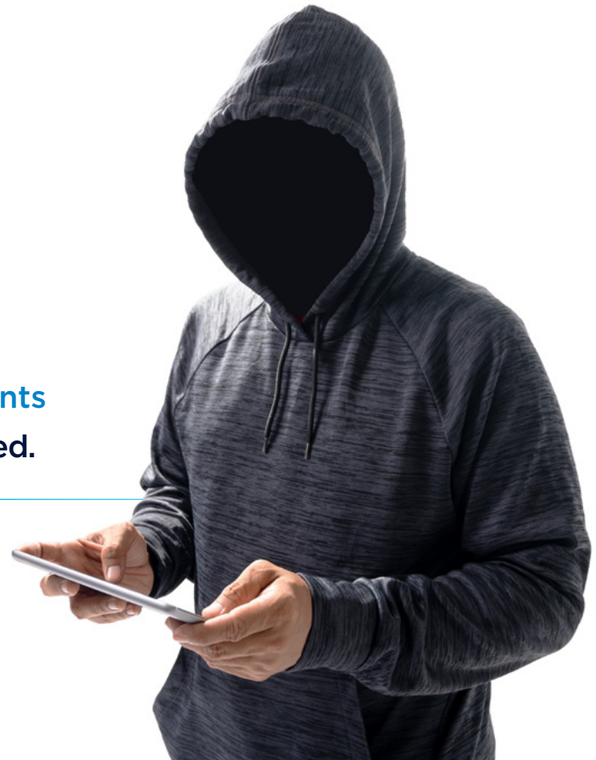
Strategies for cybersecurity in healthcare

Spectrum ENTERPRISE™

MYTH: CYBERATTACKS HAPPEN MOSTLY TO BANKS.

"There's a lot of value in patient data. You can find all kinds of confidential information that can be used in countless nefarious ways on the dark web."

— Les Wood, Director of Product Marketing - Spectrum Enterprise



In 2022 alone, more than 52 million patients had their private healthcare records exposed.

It seems that nearly every day there is another cyberattack in the headlines. One might think that the biggest targets of cybercriminals are financial or government institutions, but there is value in patient data and the attempts to breach healthcare systems are on the rise. With every breach, hundreds of thousands of patient records could be compromised.

1,064,195

The number of healthcare records exposed in the 40 breaches reported in January 2023 alone.

Spectrum ENTERPRISE

RANSOMWARE

One of the most prevalent types of attack on healthcare organizations is ransomware

These attacks disrupt the ability to care for patients by locking healthcare systems out of their networks, keeping them from critical files and demanding payment in order to get back up and running. The FBI has warned that ransomware attacks can put patients at risk by delaying access to care and vital information, such as Electronic Health Records (EHRs).

The impacts of a significant security incident:

32%
Disruption of systems/devices impacting business operations

26%
IT operations

22%
Data breach or data leakage

21%
Disruption of systems/devices impacting clinical care

17%
Monetary loss

Cybercriminals know that healthcare systems are likely to succumb to the pressures of paying the ransom because it can cripple their patient care delivery.

While the healthcare sector pays less than other industries in ransom per instance, just under $200,000, the average healthcare breach now costs more than $10 million, according to a July 2022 report from IBM Security.

This cost includes the restoration of systems and recovery of data, but the biggest price a hospital pays may be the harm to their reputation and the breakdown of trust with their patients and the community.

"In this age of digital commerce and digital health, you must be able to access the system. If you're locked out, you can run into problems, even for small practices."

— Les Wood

Spectrum ENTERPRISE

Digital transformation can only succeed with security as its foundation.

We can build it.

Spectrum ENTERPRISE

THE GROWING ATTACK SURFACE.

STAT: The healthcare industry was the most common victim of third-party breaches at 34% in 2022. Finance and Government were second and third, both at 14%.

The digital transformation in healthcare over the past three years has been unmistakable. It has allowed physicians to provide better care and empowered patients to take a bigger role in their own health by utilizing devices like wearables and remote patient monitoring (RPM). However, this transformation has also increased the attack surface for these organizations. A move to telehealth and mobile workforces has expanded the attack surface even further. Hospitals, particularly, depend heavily on third-party technology from vendors and connected medical devices. So even if hospitals feel their networks are secure, managing access points from these third parties is critical.

Phishing attacks are often the initial points of compromise. All it takes is for staff to inadvertently click on a link in an email or open a file and the door is left wide open. Providing education to internal staff regarding procedures that keep data safe and about the potential risks of phishing email is a good first step to protect your organization. But without an intrusion detection and prevention system (IDPS), it is virtually impossible to pinpoint the vulnerability, especially since malicious actors can lie in wait on your network for months before they are detected. This brings the average breach lifecycle to 287 days, long enough to put some healthcare facilities out of business for good.

"People have an innate desire to be helpful, especially in a healthcare setting. And it's easy to trick someone into giving away credentials or clicking on a link in an email."

— Les Wood

"The more devices and more information on your network, the more the attack surface grows."

— Theresa Dudley, Manager of Vertical Programs, Healthcare - Spectrum Enterprise

Spectrum ENTERPRISE™

ANTIVIRUS IS NOT ENOUGH

Just as with health afflictions themselves, in cybersecurity there is always the feeling that "it won't happen to us." However when asked, 79% of Healthcare Executives, IT / technology leaders, clinician leaders and clinicians said that data security/cybersecurity were a top priority for their organization in the next 12 months.

"The biggest oversight for healthcare is not having a plan. Health systems need a risk management strategy in place."

— Theresa Dudley

STAT: Though the instances of cyberattacks targeting healthcare is on the rise, the majority of respondents to the 2021 HIMSS cybersecurity survey reported that 6% or less of their IT budget was allocated to cybersecurity and that level of spend has not changed over the last 4 years.

84% of respondents to the 2022 HIMSS Healthcare Cybersecurity Survey say hiring qualified cybersecurity staff is a challenge, and once they are hired, 66% noted that retention poses a significant challenge.

Cybersecurity must move at the speed of evolving threats.

Often, there is the perception that your IT provider is adequately handling the protection of your organization or that a firewall or antivirus is enough. In truth, to be effective cybersecurity must move at the speed of the evolving threats, and for that you need the right personnel.

Partnering with a company that provides a fully managed solution is vital.

The staffing shortages which continue to plague healthcare are not just impacting nurses and doctors. Many hospital systems simply do not have the right people in place to monitor their networks and respond to threats. That is why partnering with a company that provides a fully managed solution is vital.

STAT: The biggest gaps to achieving robust healthcare cybersecurity are:

61%	Lack of people
50%	Lack of budget
45%	Lack of data inventory
38%	Lack of data classification
38%	Lack of certain specialized skills for cybersecurity staff

Spectrum ENTERPRISE

DEFENSE IN DEPTH

No organization can be truly protected by a single layer of security. Defense in Depth is a layered approach to cybersecurity that will significantly improve your security profile, regardless of user, device or application location.

The firewall is your first line of defense, but full protection means employing a comprehensive cybersecurity solution with a full range of features to address the evolving threat landscape. To protect against attacks targeting data, devices, applications, users or locations, you need network security with firewalls, antivirus and anti-malware, VPNs, network access control, intrusion detection, monitoring, web security gateways, data encryption multi-factor authentication and beyond. You also need a partner who can integrate these features seamlessly and manage them, along with your licenses, now and into the future.

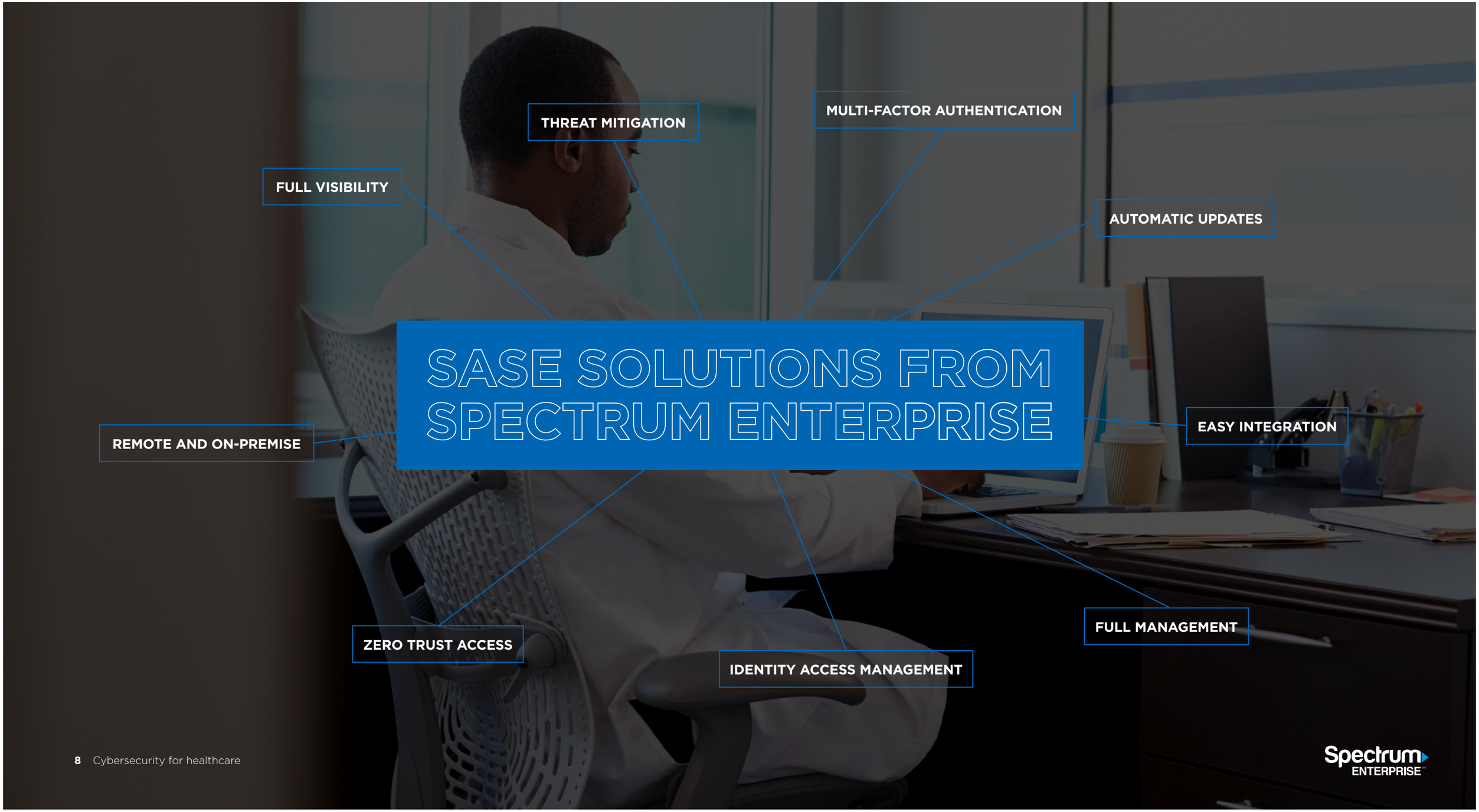
"Healthcare systems often operate networks comprised of multiple legacy solutions that don't interoperate effectively. Trying to integrate these elements while keeping everything up to date can be exhausting."

— Andrew Craver, Vice President of Segment Marketing - Spectrum Enterprise

" You need to find a way to simplify the experience, for the network to be up, for it to be secure."

— Theresa Dudley

Spectrum ENTERPRISE™


THREAT MITIGATION
MULTI-FACTOR AUTHENTICATION
FULL VISIBILITY
AUTOMATIC UPDATES
SASE SOLUTIONS FROM SPECTRUM ENTERPRISE
REMOTE AND ON-PREMISE
EASY INTEGRATION
ZERO TRUST ACCESS
IDENTITY ACCESS MANAGEMENT
FULL MANAGEMENT

SECURITY SOLUTIONS FROM SPECTRUM ENTERPRISE

We simplify security to enable safe, effective interaction between users, systems and content. With trusted leading-edge technology and expert support, we enable healthcare IT teams to be more effective, more informed and more responsive no matter whether they are a single- or multi-site organization.

Managed and fully supported for your biggest challenge

From solution design to implementation and on-going support, we bring expertise to help you tackle the toughest threats, streamline operations, reduce administration and scale while preserving your ability to granularly control the platform.

We're here to meet your evolving needs.

As a single provider we bring services together to create an experience that's reliable, scalable and efficient.

24/7

Integrated solutions for fewer disruptions

Simplify the security experience and reduce the technology and vendors needed to protect your network with a solution that is designed to easily integrate into your environment.

Spectrum ENTERPRISE

CLOUD SECURITY WITH CISCO SECURE CONNECT

As cloud services become more sophisticated, so too do the security needs associated with it. Cloud Security with Cisco+ Secure Connect allows users to securely and directly access cloud SaaS applications and the internet without reliance on a traditional centralized or premises-based security solution.

SECURE ACCESS WITH CISCO DUO

"We have trained technical resources available 24/7/365. With staff shortages in healthcare, sometimes smaller providers may not have the IT resources they need, everywhere they need them."

— Les Wood

As more organizations perform work outside their network perimeters, IT and security teams are finding it increasingly difficult to trust or identify users. Secure Access with Cisco Duo empowers remote workers by allowing IT staff to establish secure access policies by user and device, regardless of location.

Spectrum ENTERPRISE

IMPROVE THE CYBERHEALTH OF YOUR ORGANIZATION

With the impacts of cybercrime growing every year, we understand the urgency of staying ahead of the risks. That's why we have security experts and partnerships with leading providers, to deliver fully managed solutions designed to improve your cybersecurity posture, and the patient experience.

If you are interested in a tailored cybersecurity platform that meets the needs of your organization, today and into the future, contact our cybersecurity team at 1-866-459-0059 or visit enterprise.spectrum.com/security

---

About Spectrum Enterprise

Spectrum Enterprise, a part of Charter Communications, Inc., is a national provider of scalable, fiber technology solutions serving many of America's largest businesses and communications service providers. The broad Spectrum Enterprise portfolio includes networking and managed services solutions: Internet access, Ethernet access and networks, Voice and TV solutions. The Spectrum Enterprise team of experts works closely with clients to achieve greater business success by providing solutions designed to meet their evolving needs. For more information, visit enterprise.spectrum.com.

SE-HC-EB007

Spectrum ENTERPRISE™