

Protect your healthcare organization from cyberthreats with less day-to-day management

Connect confidently with an integrated security experience from Spectrum Business®



2,210

The number of weekly cyberattacks experienced by the average healthcare organization.³

Only 14%

of healthcare IT leaders say that their organizations' IT security teams are fully staffed.⁷

\$3.1B

The total cost to one U.S. healthcare organization of a major 2024 cyberattack.⁸

\$5.7M

The average ransom demand during cyberattacks on healthcare organizations in 2024.¹⁰

For cybercriminals, finding vulnerabilities in network infrastructure is second nature.

The large volumes of sensitive personally identifiable information (PII) that healthcare organizations (HCOs) collect and store has made the healthcare industry an attractive target for cybercrime. With widespread internet access, mobile and Internet of Things (IoT) devices and AI-assisted technology, hackers have many ways to gain entry into critical systems. In 2024, 82% of healthcare organizations reported significant security incidents,¹ and 59% were hit by ransomware attacks.²

To protect their networks, critical data and patients' well-being, many healthcare organizations are working to stay ahead of new risks by investing in cybersecurity solutions. From 2024 to 2025, 76% of healthcare organizations maintained or increased their cybersecurity budget.⁴ Even so, IT leaders are finding it difficult to manage the volume and complexity of security alerts. Healthcare was second only to financial services in the number of times the industry was compromised in 2024, marking the first year since 2017 that it did not occupy the top spot.⁵ Healthcare and medical organizations also accounted for 10% of all publicly reported ransomware victims in 2024, making the industry the second most targeted sector behind manufacturing.⁶

At Spectrum Business, we can help you face the current threat landscape confidently by providing much more than just traditional cybersecurity measures for your practice. By combining your leadership and our expertise, we will utilize the strength of our network to deliver deeply coordinated protection with advanced solutions built to reduce administrative effort and an approach to security that extends from our network core all the way to your clinical environment.

The power of an integrated security experience

When exploring new ways to help your practice stay ahead of cyberthreats, it's important to keep in mind that it takes more than just the right solutions to deliver complete protection. To connect with confidence, you want security measures that are integrated with your internet and network connectivity.

A network built for protection

Security in today's healthcare environment starts with having a solid foundation. Spectrum Business is a trusted provider with the right expertise to help you guard against cyberthreats and stay ahead of emerging technology trends that can increase your risk. Rely on us to provide 24/7/365 monitoring that detects threats and automatically responds to network intrusions and cyberattacks.

Expertise that ensures performance

In 2024, 69% of healthcare organizations hit by a cyberattack experienced disruptions in patient care as a result.⁹ The legacy technology and infrastructure controls of the healthcare sector can make it more difficult to safeguard devices, limit lateral movement and stop attacks from spreading. This can make it difficult for security professionals to respond in a timely fashion. To increase efficiency, IT leaders need to know which solutions and processes are most effective. We assist by partnering with major security leaders to review, verify and apply measures proven to keep your internet service and network secure.

11.7 TB

The average network-layer DDoS attack volume in 2024, compared to 5.3 TB in 2023.¹¹

\$9.77M

The average cost of a data breach in the healthcare industry as of 2024 — the most expensive of any industry.¹²

A unified security approach integrated with your internet and network connectivity can help you eliminate vulnerabilities and expedite issue resolution.

Solutions customized for the demands of your practice

Every healthcare organization has different needs. That's why we start our process by evaluating your current infrastructure and applications to design the network topology most appropriate for your practice. Built-in redundancy delivers layers of protection that help keep your traffic safe and prevent attacks from impacting your clinical and patient experiences.

Multilevel security — from packet level to network traffic

Often, healthcare entities need more than just traditional local area network (LAN)-side protection for peace of mind. Cybercriminals can use volumetric distributed denial of service (DDoS) attacks combined with application-layer attacks to overwhelm specific targets and cause complete infrastructure collapse. We can help you avoid these costly disruptions with our DDoS Protection service, powered by Radware and designed to detect and mitigate such attacks and help keep your network up and running.

The flexibility to fine-tune your threat protection

As security demands change, you need the ability to adjust your strategies quickly and seamlessly. At Spectrum Business, we have your security needs covered by providing a range of additional solutions, including perimeter-based protection, firewalls with built-in VPN access, next-generation firewalls with advanced security services and support for integration with client authentication sources. Along with other safeguards such as unified threat management (UTM), these solutions are designed to be flexible and provide multiple security functions from one centralized interface. And with all these services fully managed by our IT experts, you don't have to worry about whether you have the latest updates installed, as our network engineers and support teams handle them for you. Meanwhile, our managed security service portal allows you to monitor your organization's network activity, unlocking insights via logs and event tracking.

A unified security approach integrated with your internet and network connectivity can help you eliminate vulnerabilities and expedite issue resolution. With today's expanded attack surface, it's essential to have a partner that can remove the complexities of protecting your practice's staff, clinicians, patients and data. That's why we provide solutions capable of addressing your unique security threats while giving you confidence in your infrastructure.

Sophisticated solutions to optimize your IT security

The increase in cloud services, mobile connectivity and IoT devices is a major reason why protecting healthcare organizations has become so challenging. While the intelligence built into our network core can help by capturing and removing many large-scale cyberattacks, you can still be open to vulnerabilities based on your specific infrastructure. We can identify the strategies and solutions that would be most effective in protecting your organization's attack surface and help you understand the role they play in keeping your network safe.



DDoS Protection

Protect the availability of your HCO's assets by employing a scalable, subscription-based DDoS solution that uses proprietary machine learning and advanced analytics to identify anomalies in traffic flows and respond to and mitigate attacks away from your network.

**Secure Access with Cisco Duo**

Help protect your HCO from unauthorized access to sensitive systems, regulatory violations and data loss that can disrupt operations. Capabilities that include multi-factor authentication (MFA) and identity management allow IT to set access policies by user and device, regardless of location.

**Cloud Security with Cisco+ Secure Connect**

Allow remote users to access cloud SaaS applications and the internet securely and directly without reliance on a traditional centralized or premises-based security solution. This cloud-based security service includes secure web gateways, cloud access security broker, identity management, zero trust network access and more.

**Enterprise Network Edge**

Improve the network experience for your clinical teams with an enterprise-grade managed solution that brings together connectivity, equipment and network management to support both hybrid networks and workforces. Powered by Fortinet, the solution simplifies IT operations by providing networking with security features and optional integrated WiFi and switching in a multi-cloud-ready platform.

**Managed Network Edge**

Simplify the deployment and management of your network with this modular, all-in-one solution. Delivered over the Cisco Meraki platform, Managed Network Edge offers security features, routing, an SD-WAN, WiFi and switching. Available smart cameras, powered by advanced AI and machine learning, provide actionable insights into your physical and digital spaces. Intelligent sensors automatically detect and alert staff to environmental events. Achieve flexibility and scalability with connectivity, equipment and network management from a single partner.

**Ethernet Services**

Meet growing data needs by connecting locations with a fast, reliable WAN solution backed by a 100% uptime service-level agreement (SLA) guarantee and built on a dedicated fiber infrastructure. Bandwidth up to 100 Gbps is available.

**Cloud Connect**

Extend your network with fast, secure and dependable private connections to cloud service providers with a service backed by a 100% uptime SLA guarantee.

**Managed WiFi**

Meet clinical and patient demands for reliable connections to the internet with ubiquitous coverage across your healthcare campus.

Consult with experts and explore professional integration services to determine the optimal configuration for your needs with solutions backed by 100% U.S.-based support, available 24/7/365.

Count on us to help you keep patient data safe

Protecting your hospital or clinic from cybersecurity threats has never been more important. Changes in technology are creating new network vulnerabilities and exploits, while opportunistic hackers are intensifying their efforts to take advantage of challenging situations. To stay ahead of risks and move your practice forward confidently, you need to consider all aspects of your security strategy.

Receive the level of protection you need with a single digital security experience that starts at our network core and extends all the way to the solutions you use to keep your HCO safe. With our network design expertise, we can help you set up the infrastructure to connect securely and provide the fine-tuned security solutions you need to protect your network traffic and data.

Learn more

1. ["2024 HIMSS Healthcare Cybersecurity Survey."](#) HIMSS, 2025.
2. ["2024 Ponemon Healthcare Cybersecurity Report."](#) Proofpoint, 2024.
3. ["The State of Cyber Security 2025."](#) Check Point Research, 2025.
4. ["2024 HIMSS Healthcare Cybersecurity Survey."](#)
5. ["Identity Theft Resource Center 2024 Data Breach Report."](#) Identity Theft Resource Center, January 28, 2025.
6. ["The State of Cyber Security 2025."](#)
7. Jordan Scott, ["New CDW Research Report: Shortages Impact Healthcare Cybersecurity Strategies."](#) HealthTech, June 10, 2024.
8. Rebecca Pifer, ["UnitedHealth Reaches Record Revenue in 2024, Though Profit Falls."](#) Healthcare Dive, January 16, 2025.
9. ["2024 Ponemon Healthcare Cybersecurity Report."](#)
10. Rebecca Moody, ["Ransomware Roundup: 2024 End-of-Year Report."](#) Comparitech, January 9, 2025.
11. ["2025 Global Threat Analysis Report."](#) Radware, 2025.
12. ["Cost of a Data Breach Report 2024."](#) Ponemon Institute and IBM Security, July 2024.