WHITE PAPER

New security threats demand new solutions

Evolving technology to protect healthcare networks, remote users and cloud architectures will uplevel your security posture

Spectrum ENTERPRISE®

The security landscape is dramatically changing for healthcare organizations (HCOs) as traditional network characteristics are transformed by a host of emerging trends and influences, ushering in new risks and threats. These developments highlight the need for HCOs to integrate comprehensive tools and technologies designed for a new and increasingly dangerous world.

133 million healthcare records were breached in 2023 — a 156% increase from 2022.[1]

Implementing telehealth and cloud-based applications, enabling electronic health records (EHR) platforms and remotely monitoring patient vital signs with wearable devices are some of the key contributors to evolving security demands. HCOs also increasingly rely on cloud-based software as a service (SaaS) applications. As a result, a range of additional tools and strategies are necessary to restrict and manage access to these resources for healthcare practitioners and patients.

The shift to cloud-based apps has facilitated the use of multiple devices to access patient data. These commonly include HCO-provided and personal technology, adding a level of complexity to security strategy. With additional data safeguards required for regulatory compliance, as well as limited IT resources to manage traditional threats like distributed denial of service (DDoS) attacks and malware, the need for greater defense in depth across your network becomes clear.

Guard against DDoS disruptions

DDoS attacks represent a growing threat for HCOs. Designed to flood connectivity to your network, application or services, these attacks aim to prevent your intended users from accessing resources.

DDoS Protection from Spectrum Enterprise® applies adaptive intelligence to evaluate your network activity and identify threats to your Dedicated Fiber Internet service.

Attack mitigation and traffic rerouting begin automatically to help stop malicious traffic before it reaches your network. The service also includes continuous, 100%, 24/7/365 U.S.-based support through a single point of contact and insight into current and historical attacks for network planning.

Adapting security strategies to evolving threats

A growing number of HCOs are turning to cloud-based architectures for the efficiency, resiliency, expediency and ubiquity they offer. But the move to the cloud is accompanied by new security concerns. Legacy network security was designed with the HCO data center as the focal point for user access. Multi-cloud architectures expand the threat surface as data and user access proliferate across multiple applications. As a result, 82% of breaches now involve data stored in the cloud.[2]

Protecting data with solutions like a cloud access security broker (CASB) has become essential to establish secure access to cloud-based applications to prevent unauthorized access and data breaches. Software-defined and cloud-based security can offer anywhere, anytime protection for data and applications. For example, firewall as a service (FWaaS) offers cloud-based protection across your staff, patients and locations and is able to scale as your needs change.

Maintaining a single security policy throughout a distributed environment for threat detection, traffic inspection and user access requires investment and IT expertise. Managed security services can provide a faster, simpler path forward, contributing to greater flexibility, less work for IT and a lower total cost of ownership. These services can include a variety of solutions to protect remote network access, such as multi-factor authentication (MFA) that helps enable zero trust network access (ZTNA). To guard against malware and data breaches, cloud-based firewalls and unified threat management (UTM) can offer protection on premises and for remote users.

Spectrum ENTERPRISE®

Comprehensive protection includes physical security

Your vulnerabilities do not end with your cloud strategy and distributed staff and patients. A security approach that equips you to deliver defense in depth should also encompass your physical locations.

Managed Network Edge helps simplify your networking with a modular, expandable and all-in-one solution. Powered by Cisco Meraki, the platform provides a range of capabilities, including WiFi, network security, remote access, SD-WAN and switching. It's cloud-controlled with an intuitive interface, so management and monitoring is easy.

You can add capabilities to the solution to monitor your physical spaces and help protect people and property:

Smart cameras: Gain valuable insights into behavior patterns while also protecting your locations. View your property using cameras that integrate with a web-based portal that offers advanced analytics, heat maps and other features for stronger security.

Environmental sensors: Intelligently monitor and automatically alert staff members of environmental events such as changes in temperature, humidity, air quality and water leaks within HCOs, data centers, cold storage environments or any place you need to protect.

As managed services, these solutions include installation, maintenance and continuous updates that result in a stronger security policy while freeing up IT for bigger priorities.

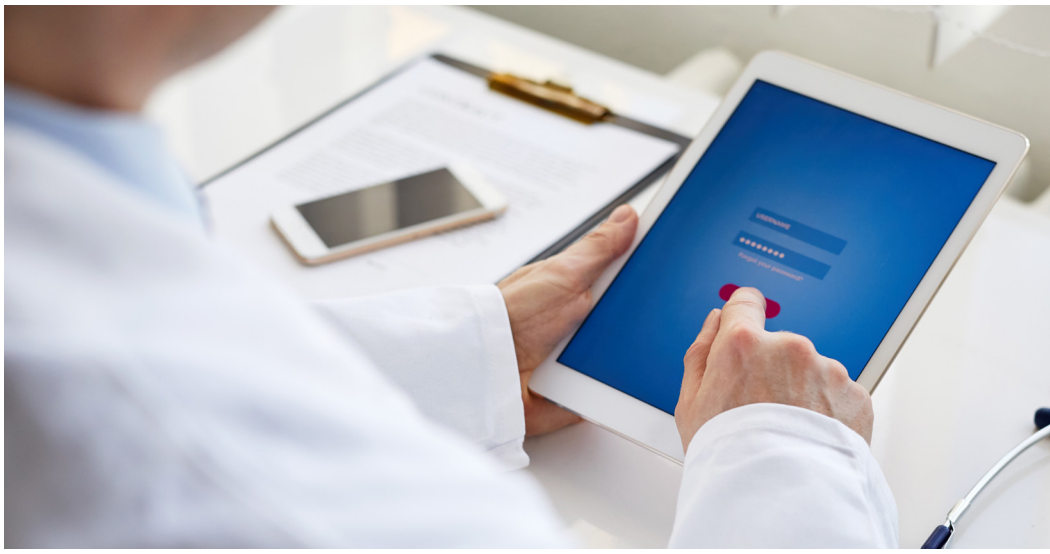
HCOs must also keep an eye on the impact escalating security demands can have on organizational spending. The average cost of a healthcare data breach in 2023 was nearly $11 million, which was the highest across all other industries (about $4.5 million).[3]

Where security investments are spent can be just as important as the size of budgets. When HCOs work with multiple systems from different vendors, potential gaps in protection can emerge. Solutions might not be designed to work together, reducing visibility and control. Using a single provider that can incorporate networking and cloud security in one platform can ensure protection remains up to date and vulnerabilities are identified before they harm your HCO.

Secure access service edge (SASE): new tools for distributed HCOs

The evolution of network models and the adoption of cloud technologies have allowed HCOs to transform how and where they provide care. But with the new benefits have come new threats and considerations across healthcare. Focusing exclusively on the network can leave HCOs vulnerable to breaches in cloud applications, malware and other threats.

As IT teams seek to securely connect people anywhere, anytime, with streamlined access from any device, they must also address a vastly larger and more complex attack surface. Doing so requires a new approach powered by new solutions built for distributed staff, patients, locations and applications. SASE offers a powerful framework to enable easy access to resources inside and outside the network while meeting performance demands and blocking sophisticated security threats.



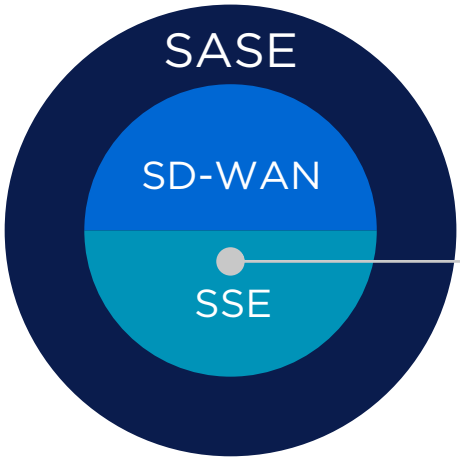
Spectrum ENTERPRISE®

What is SASE?

SASE brings together two key components:

1. SD-WAN for unified access and network controls.
2. Secure service edge (SSE), a set of cloud-based cybersecurity solutions centered on the identity of users, devices and operations.

The global SASE market is projected to grow from $1.9 billion in 2023 to $5.9 billion by 2028.[4]



SSE is a collection of cloud-based security functions that manage access to websites and applications from anywhere users are located.

- CASB
- Secure web gateway (SWG)
- ZTNA
- FWaaS
- UTM
- MFA

SASE is a combination of technologies, rather than a single off-the-shelf solution.

Become familiar with the networking and security concepts that make this framework so powerful:

SASE explained: A glossary for evolving network security

SASE converges networking and security — typically as a cloud-delivered managed service — to safeguard internal networks, users, devices and endpoints connecting via the internet. Adopting managed SASE solutions can help your IT team effectively and efficiently secure a multi-cloud environment and constantly changing network endpoints.

Cloud-based security solutions

Integrating portfolio solutions like Secure Access with Cisco Duo and Cloud Security with Cisco+ Secure Connect make it easier to deliver defense in depth while creating a unified security policy for your HCO. IT administrators also benefit from improved insight into their networks from a single portal, providing control across the entire HCO.

- **Protect access to your network and sensitive information** with Secure Access with Cisco Duo. Help ensure your staff has secure access to internal applications-and protected health information regardless of location or device. Gain visibility into who and what devices are using your network at any time.
- **Defend your network users and data**, both in the cloud or on your network, with Cloud Security with Cisco+ Secure Connect. Provide a consistent and universal security experience regardless of user location with cloud-based firewalls, secure web gateways, ZTNA and more.

The SD-WAN and cloud-based security solutions enable you to extend your security policies beyond the HCO firewall for greater visibility and control of cloud applications and data. These tools make VPNs more secure and can help document compliance with regulatory requirements, such as HIPAA, for patient data protection.

Spectrum ENTERPRISE®

2023 top five highest average costs of a data breach by industry[5]

$10.9M
Healthcare organizations

$5.9M
Financial

$4.8M
Pharmaceuticals

$4.8M
Energy

$4.7M
Industrial

The SASE framework can provide solutions that complement each other's functionality to protect the entire network infrastructure:

Solution	Functionality
CASB	Optimize user productivity by providing secure, fast access to cloud-based applications and resources — without backhauling remote traffic to the data center. CASB allows organizations to manage and enforce data security policies and practices regardless of the user location, device or cloud application.
SWG	Monitor and filter internet traffic for external threats and prevent user access to potentially harmful websites and applications. An on-premises or cloud-delivered SWG also helps enforce HCO and regulatory policy compliance.
ZTNA	Grant access to cloud resources and data centers with continuous verification of information such as user ID, device identity and location. This capability represents a step up from previous security practices that assume a user is trustworthy.
FWaaS	Help protect the entire HCO with UTM firewall controls and advanced security for all users and locations delivered as a cloud service that scales to handle SSL inspection, growing bandwidth demands and cloud application traffic.
MFA	Enforce access restrictions for data or applications based on user, device and location. Confirm user identities and prevent attackers from accessing additional sensitive data if a single login is compromised. Passwordless authentication allows employees to use single sign-on (SSO) applications, mobile device PINs or biometric data to provide frictionless logins. Creating a centralized authentication system makes it easier to manage and secure online accounts.
Content filtering	Control content access through your firewalls, bolster security and enforce HCO policies. Specify character strings that, if matched, identify content your organization has designated illegal or inappropriate and should be blocked. Additionally, this capability screens websites for malware and other threats before permitting access.
Domain name system (DNS)-layer security	Block traffic to malicious systems and stop threats before they are accessed by customers or employees. Also, prevent callbacks to attackers if infected machines connect to your network.

Spectrum ENTERPRISE®

Strengthening protection through partnership

As the threat landscape evolves and grows more sophisticated, HCOs require new strategies to keep people, data and systems safe. Build an effective security response around a SASE framework coupled with DDoS protection, UTM and networking solutions that help automate protection and governance.

You can establish defense in depth while also simplifying your IT operations. Managed services from Spectrum Enterprise® provide the design expertise, hardware and ongoing maintenance for security solutions that match your unique needs. All-in-one networking platforms like Managed Network Edge allow you to scale and adapt as security requirements change. The solution is also backed by 100%, 24/7/365 U.S.-based support.

Give your employees and other stakeholders secure, reliable access to the data and applications they need with less day-to-day management of your technology.

Learn more

1. "Security Breaches in Healthcare in 2023," The HIPAA Journal, Jan. 31, 2024.
2. "Cost of a Data Breach 2023," Ponemon Institute and IBM Security, 2023.
3. Ibid.
4. "SASE Market by Offering (Network as a Service, Security as a Service), Organization Size (SMEs, Large Enterprises), Vertical (Government, BFSI, Retail and eCommerce, IT and ITeS, and Region (North America, Europe, APAC, RoW) – Global Forecast to 2028," Markets and Markets, April 2023.
5. Saumick Basu, "68 Cloud Security Statistics to Be Aware of in 2024," Astra, December 22, 2023.

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.

©2024 Charter Communications. All rights reserved. Spectrum Enterprise is a registered trademark of Charter Communications. All other logos, marks, designs, and otherwise are the trademarks and intellectual property of their respective third-party owners. Not all products, pricing and services are available in all areas. Pricing and actual speeds may vary. Restrictions may apply. Subject to change without notice.

Spectrum ENTERPRISE®