INDUSTRY
SOLUTION BRIEF

Power your healthcare organization with secure SD-WAN

Connect and secure everything in your network via a flexible, robust, and performant SD-WAN

Open Systems services are ISO 27001 certified.

What are some of the current challenges in the healthcare industry?

Support mobile devices and telehealth

Reach all endpoints with a flexible, robust, and performant network

Connect the Internet of Medical Things (IoMT)

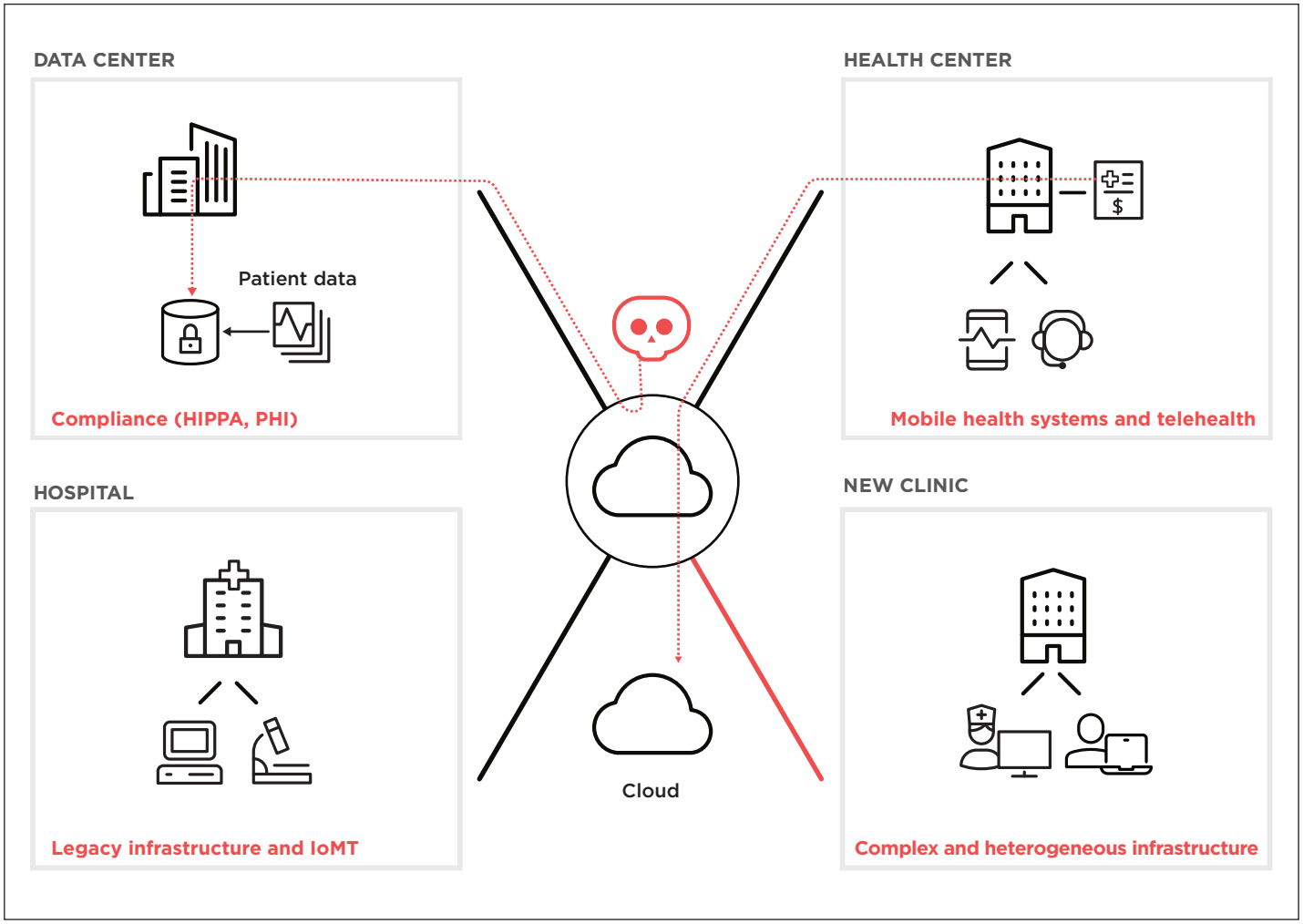
Provide connectivity to legacy devices and systems while enforcing security controls

Ensure compliance with PHI, HIPAA, and more

Maintain regulatory standards for data protection and a complete audit trail of events

Unify complex infrastructure and remote sites

Enable networking and security for hospitals, clinics, and remote branches



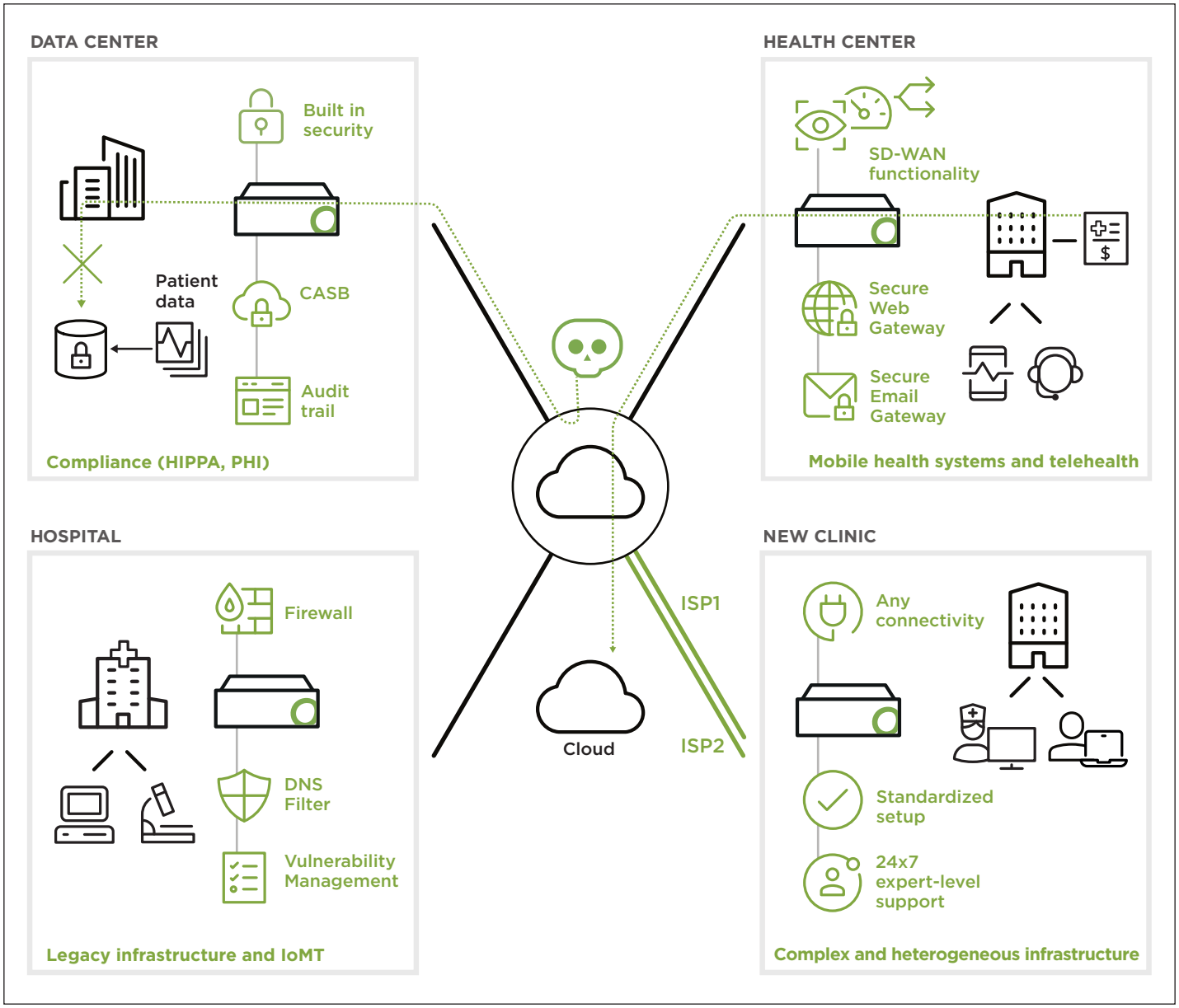
Most common pain points of healthcare institutions in their IT network and security environments

As a healthcare enterprise, your network is critical to quality of care

Healthcare organizations rely on their extensive networks to deliver patient and administrative data efficiently across clouds and to every endpoint, many of which are now tablets and other mobile devices. Equally important, the enterprise network must both protect patient data according to governing regulations and provide security for a complex IT infrastructure that typically includes a significant number of legacy machines. Finally, that same network must also enable business innovation and acceleration. To do all these things reliably requires a best-of-breed networking and security solution – it requires the Open Systems Secure SD-WAN.

Your SD-WAN is a key resource

A unified, secure network like the Open Systems Secure SD-WAN is critical to enabling healthcare organizations to ensure compliance and complete audit trails, integrate and secure both complex, often legacy infrastructures and remote locations, and drive mobility and telehealth services – all while providing end users across the organization with the fast connectivity and strong security they need to drive innovation and business value.



How Open Systems can support the healthcare industry in patient data protection, IoMT and simplification of complex infrastructure.

Let's address healthcare industry challenges one by one

Meet the agility demands of mobile devices and telehealth

Modern healthcare IT environments must contend with ever-rising demand for mobile device connectivity and telehealth services. Mobile access also presents new security and bandwidth challenges as patient data, billing information, bookings, and video conferencing all traverse the same environment. Powering healthcare IT services requires a flexible, resilient, and high-performance network that stretches to every endpoint and offers intelligent, granular controls.

Open Systems enables customers to implement use case-based firewalls to control access, and Bandwidth Control and Path Selection features to manage connectivity and performance, among many disparate services. For billing systems, Open Systems provides secure mechanisms for connecting to cloud partners, while our Secure Email Gateway protects users from spoofing, phishing, or malware attacks and potential subsequent damage to the brand.

Challenge

Open Systems solution

1

You need to assure secure access, for example, to patient data or surgery room bookings from mobile devices such as tablets or mobile phones.

1

Leverage our **Next-Gen Firewall** to filter access based on use case – limiting user access according to necessity and ensuring secure connectivity for mission-critical services. Track traffic flows and eliminate unused access paths based on firewall rule profiling.

2

You'd like to enable telehealth operations by delivering reliable and smooth video conferencing.

2

Open Systems Secure SD-WAN features like **Bandwidth Control** and **Path Selection** provide automated, application-aware network management, per location and per connection, to ensure your telehealth center has all the throughput it needs.

3

Your billing systems require seamless access and secure connectivity to partners in the cloud.

3

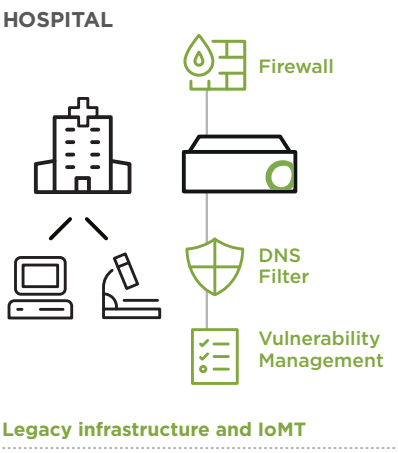
Open Systems offers IPsec VPN tunneling to securely and reliably connect billing systems to your cloud partners via **Partner Connect** – or you can provide a secure web connection via our **Secure Web Gateway** and **Cloud Access Security Broker.**

4

You need to secure the organization's email communications – which are still an extremely common method of patient communication.

4

Open Systems offers powerful threat protection via the email filtering functions of our **Secure Email Gateway.** Protect your end users' communications from spoofing, phishing, or malware attacks – and by extension protect the reputation of your brand – by leveraging visibility, enforcement, and deep analysis of your email traffic.



Connect and secure all your legacy equipment

Healthcare infrastructure can be difficult to secure. Legacy devices, such as X-ray, MRI machines or microscopes, may not support web proxies – rendering them vulnerable – and their control software may also be at risk due to age. These assets need to be handled specially in the midst of an already complex networking and security picture, and, if a vulnerable device is compromised, the network must have controls to prevent the internal spread of infections.

Open Systems solutions address these challenges with a variety of best-of-breed technologies – like a global, zone-based firewall, a DNS Filter, a Secure Web Gateway, and Network Security Monitoring – that means you can stay focused on your strategic objectives.

Challenge

Open Systems solution

1

For added network security, you'd like to isolate business-critical but legacy machines – like X-ray and MRI machines or microscopes – from other user activity and patient data.

1

Open Systems SD-WAN features a global, **zone-based WAN firewall** that enables internal network segmentation – effectively adding firewalls within your firewall – to protect your critical assets.

2

You'd also like to add additional protection for non-proxy-aware devices.

2

Open Systems covers all your IT: our **DNS Filter** performs threat protection for non-proxy-aware devices, while our **Secure Web Gateway** does the same for proxy-aware devices.

3

For your machines running older software, you must adopt solutions to protect known vulnerabilities.

3

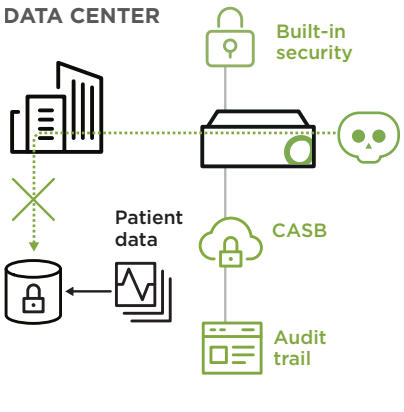
The Open Systems **Vulnerability Management** solution allows you to add further protection and monitor the status of that protection in real time. See your security posture from the hacker's point of view – get visibility into threats across your on-premises, cloud, and mobile IT assets, and enjoy proactive alerts and remediation.

4

As much as possible, you'd like to ensure that no legacy (and therefore vulnerable) medical device is compromised or, in the case of an infection, that malware does not spread internally.

4

Open Systems takes a holistic approach to threat detection and response. Because legacy devices may not accept an **Endpoint Detection and Response** installation, we provide advanced **Network Security Monitoring** to detect compromised systems quickly and enable efficient analysis and response – including our Global Threat Isolation feature, which can isolate a machine on the perimeter in the event of a compromise.



Ensure compliance with multiple regulatory obligations

Today's healthcare enterprise is responsible for ensuring the protection of patient data under HIPAA, GDPR, and PHI. Given how much sensitive data organizations typically handle, data security is a large and demanding task. You need strong security protections at every level, and comprehensive solutions for threat detection and response. Moreover, you need to be able to demonstrate the security features and compliance of your network to multiple regulatory bodies.

The consistent architecture and advanced automation of the Open Systems Secure SD-WAN, combined with the 24x7 expert-level support that Open Systems provides, enables enterprises to easily meet IT regulatory requirements. Our SD-WAN protects you against external threats with built-in, best-of-breed security features, and delivers powerful threat detection and response via additional options. From a regulatory perspective, the deep visibility and end-to-end audit trail built into our SD-WAN ensure you meet compliance requirements. Here are a few examples of how Open Systems drives compliance.

Challenge

Open Systems solution

1

You need to adhere to HIPAA (Health Insurance Portability and Accountability Act) and General Data Protection Regulation (GDPR) standards.

1

The Open Systems Secure SD-WAN features **built-in security** at every level. Our Next-Gen Firewall with internal zoning enables a multi-tiered organizational security policy. Similarly, our Secure Web Gateway and DNS Filter provide protection from malicious content on the public internet, while our Network Security Monitoring, Endpoint Detection and Response, and Vulnerability Management handle network threat detection and response.

2

If – despite all protection mechanisms – an attack occurs, you need a fast, comprehensive, and professional response.

2

The Open Systems OS-CERT team is a highly-skilled group that provides fast **Incident Response.** They are closely connected to a global network of security professionals who work together to mitigate threats.

3

Regulatory requirements require you to define and enforce global application usage and data policies for Protected Health Information (PHI).

3

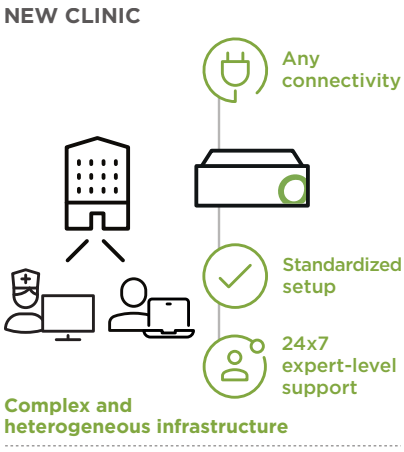
With Open Systems' **Cloud Access Security Broker (CASB),** organizations can monitor cloud application usage and then define access and usage parameters for different users and access methods in order to enforce security policies on cloud applications and make sure patient data remains confidential.

4

As part of your compliance obligations, you must provide permanent visibility and audit reporting of all actions.

4

Open Systems Secure SD-WAN makes the complete enterprise **audit trail** easily accessible on the Customer Portal. Leverage **full visibility** to see details on who requested any particular system change and when.



Unify your heterogeneous infrastructure

Connecting and securing healthcare networks, from the hospital to the clinic to the branch office, is complex. IT leaders want high availability across the environment and simple management that includes fast standardized setups, extensive automation, and deep visibility. It's a task that's only possible with a best-of-breed SD-WAN.

The Open Systems Secure SD-WAN is transport-agnostic, which – together with a standardized SD-WAN solution – enables us to establish site connectivity quickly. Fully automated hardware and line failovers protect uptime at every location, while complete visibility across global and local configurations instills confidence. Our expert-level support (NOC) engineers respond to – and coordinate all actions – in the event of a security incident.

Challenge

Open Systems solution

1

You need to deliver a robust WAN architecture that's also elegantly simple.

1

Our unified Secure SD-WAN combines **high availability** (including power and line), high performance, and flexible redundancy in the form of fully automated hardware and line failovers and seamless hardware replacement when needed.

2

You need a solution that can handle the heterogeneous nature of healthcare infrastructure.

2

Open Systems Secure SD-WAN delivers a **standardized general setup** on all sites: once an architecture is designed and agreed on, it is enforced everywhere. Local IT administrators will be reassured by full visibility over global and local configurations – from a single pane of glass.

3

You have new, remote locations that you need to connect quickly and easily.

3

Since our Secure SD-WAN runs on **any transport layer,** Open Systems can deliver connectivity as fast as possible to new sites, regardless of location.

4

If a site goes down, you must ensure an immediate, coordinated response.

4

Open Systems delivers **automated, proactive monitoring** of connectivity and services that identifies most issues before they become problems. Our **expert-level support** (NOC) is ready 24x7 to handle most responses. We fully coordinate analysis and remediation actions, and we escalate to the customer as needed.

Open Systems is a leading global provider of a secure SD-WAN that enables enterprises to grow without compromise. With assured security, AI-assisted automation and expert management that free valuable IT resources, Open Systems delivers the visibility, flexibility and control you really want with the performance, simplicity and security you absolutely need in your network.