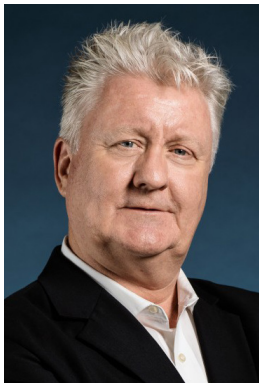
Health check

With healthcare settings now producing huge amounts of data, they are becoming an increasing target for cyberattacks, which means that network security needs to be a focus – and this presents opportunities for resellers.



Richard Staynings

CYLERA

cylera.com

> *Approximately 30% of the world's data volume [is] being generated by the healthcare industry alone.*

The recent ransomware attack that affected NHS Dumfries and Galloway, which is currently being investigated by Police Scotland and the NCSA, highlighted the threats that healthcare networks can come under.

While on this occasion, there was no direct risk to life, there were concerns that confidential data had been exfiltrated.

Richard Staynings, chief security strategist for Cylera, notes that healthcare networks are subject to all kinds of ransomware attacks. "They are chronically underfunded in terms of cyberdefences," he says. He adds that they are targets for multiple actors, from cybercriminals to aggressive states out to make an impact through sending political messages. "And so, consequently, the industry faces a challenge to protect itself."

The reason why they are such targets is simple; Richard notes that the NHS is the world's largest producer of data. "Particularly protected data that is regulated and therefore should be non-public under the law," he says. "It therefore requires massive amounts of storage for that data, which is growing in an almost exponential clip; approximately 30% of the world's data volume being generated by the healthcare industry alone. Keeping that secure while in transit and at rest is obviously a massive concern. And that requires large amounts of hardware."

Richard adds that another problem is that some of the architecture used in the NHS is old and requires updating and replacing, especially as more medical applications move to the cloud. "Patients have more access to their medical records, their GPs, pharmacies and other medical providers, and need to be able to access that via a portal or a mobile app," he says. "That is also adding to bandwidth constraints. Then we've got the original architecture of those local area networks in hospitals which are flat, whereas in many other industries, they're segmented."

Security challenge

Another problem is that the systems were never designed with security in mind, Richard adds. "This has been compounded by a move of applications to the cloud and by the rise in popularity of SSE and SASE-based networks, which are edge-based rather than call-based," he says. "We've seen some university hospitals in London that have moved to an edge-based network successfully. Others are still in the old network topology of hub and spoke-based networking. But the nature of what is connected to the network is significantly changing our design and hardware and software requirements for networking. The technology has moved to software defined networking from all the major network providers, led by Cisco, which dominates most hospital systems around the world, particularly the NHS."

Neil Langridge, marketing and alliances director at E92, adds that the huge growth of network and internet connected devices in healthcare has given rise to increased challenges in cybersecurity. "It's not just from the usual concerns around data breaches and ransomware," he says. "Healthcare is one of the leading industries in the adoption of operational technology (OT), and the connected devices outside of traditional IT. Indeed, the IoMT (Internet of Medical Things) is expected to reach a market value of $187 billion by 2027. From medical imaging devices to refrigeration to critical power supplies, the modern hospital is increasingly digital. And that

presents a huge risk, as legacy cybersecurity aren't designed for OT, and devices that aren't managed on the traditional networks."

Reseller opportunities

All this presents plenty of sales opportunities for resellers, VARs and MSPs in the healthcare sector. Neil notes that for these businesses, a key first step is understanding the full extent of the network-connected infrastructure and specific OT protocols, such as HL7, DICOM and Modbus. "Being able to present a solution that incorporates IoT and OT is essential, as well as being then able to present an offering that can integrate and connect with cloud and existing cybersecurity systems, to ensure that the IT can have a unified view of threats, activity and the ability to respond quickly," he says.

Richard adds resellers need to provide the services and software to optimise the extensive hardware purchases that a hospital may be making. "But at the same time, they have a duty of care to make sure that there's training programmes that are provided to hospital networking staff and security staff so that they can operate these things," he notes.

Alan Jones, channel marketing and Amazon manager at D-Link UK, notes that for resellers targeting the healthcare sector, it's important to understand the industry's specific requirements, challenges and budget constraints. "Highlighting the scalability, reliability and security and value of networking solutions is key to influencing healthcare organisations," he says. "Emphasising the potential for improving operational efficiencies and the ease of management can help resellers meet the needs of their healthcare clients more effectively. The NHS is very much peer-influenced, so showing examples of how other NHS Trusts or departments have benefitted from a solution could also help to unlock new opportunities."

Digital transformation

Alan adds that digital transformation is a priority for the healthcare sector, and the NHS has ambitions for most health services to have digital foundations in place by early 2025. "To realise its digital ambition, the NHS needs to be able to choose appropriate solutions from networking vendors that offer a wide choice

Neil Langridge

e92plus

e92plus.com

CONTINUED

CONTINUED

of cloud networking products tailored to the unique needs of the healthcare sector," he says.

"It's important that the NHS can scale its operations efficiently. This is crucial for healthcare providers as they face increasing patient numbers and the need to expand onsite and offsite services. Therefore, the NHS must choose networking solutions designed to support this scalability, enabling it and supporting healthcare organisations to manage and store vast amounts of data securely and efficiently. By facilitating easy access to patient records, diagnostic images and other critical information, the latest networking technology helps streamline patient care processes and can improve overall operational performance.

"Networking solutions need to be able to address these issues head-on with reliable connectivity, advanced encryption and secure access controls. Only network solutions providers committed to security and reliability can help ensure that healthcare organisations are able to protect sensitive patient data against cyber threats and comply with regulatory standards, all while maintaining continuous day-to-day IT operations.

Trevor Dearing, director of critical infrastructure at Illumio, says that it can be a challenge for healthcare organisations to scale the complexity of network hardware and cybersecurity solutions because they can contradict each other. "Hardware, networking, data processing and database infrastructure allows healthcare organisations to scale performance, whereas security solutions need to scale and adapt to changes in the healthcare environment in a way hardware cannot.

"A significant proportion of healthcare organisations still operate with physical processes, for example patient records on paper, and are only now starting to move to more efficient systems, such as electronic patient records. It's important that during this digital transformation phase, healthcare organisations also transform security, and, more critically, at the same rate. Similar to cloud environments, security needs to be scalable, this requires solutions which are more dynamic than traditional security technologies."

Trevor adds that healthcare technology is changing to provide more integrated care and remote services, so security needs to reflect this. "Healthcare organisations need a robust system that ensures operational uptime but is also flexible enough to provide real-time access to systems and data as the healthcare

Alan Jones

D-Link

dlink.com

> *"Similar to cloud environments, security needs to be scalable, this requires solutions which are more dynamic than traditional security technologies."*

Trevor Dearing

illumio

illumio.com

organisation's requirements and networks change," he says. "Security needs to be independent from the network infrastructure to ensure when the hospital's infrastructure changes, cyber resilience is maintained.

"Healthcare organisations usually have very limited budgets and resources, so they are looking for solutions to address multiple issues. Therefore, resellers will need to provide different solutions in just one offer. As a result, resellers should look towards solutions that provide a zero trust approach. Through Zero Trust Segmentation, organisations can provide the scalability and flexibility needed during digital transformation, but also segment and contain attacks at the point of entry to protect critical assets or sensitive data."

Richard adds that increasingly devices will need to be locked down to individual ports, protocols and destination IP addresses that are specifically authorised. "We know if it needs to communicate with this machine or that system," he says. "We can even lock it down further so that it only can be communicated with via certain active directory user identities; such as those who are permitted to administer an X-ray system or a CT scan or whatever the device happens to be.

"We can get down towards more zero trust principles. Healthcare is beginning to embrace zero trust principles, not just at the user level, but we're moving more towards mandatory access controls, like the sort of thing you would see in the military, where you have access to certain systems and certain data based upon your role within the hospital hierarchy."

IoT headaches

IoT, or IoMT devices, which, as mentioned, are increasingly being used in healthcare settings, are also providing security headaches that

need to be addressed. “We’re also seeing how the integration of IoT devices, the adoption of telemedicine and the use of mobile health applications are reshaping the demands for secure networking in healthcare,” says Alan. “With these additional requirements in mind, it is imperative that the networking solutions the NHS choose are equipped with advanced security features to meet these new challenges. By providing a secure and manageable networking infrastructure, healthcare providers can embrace digital innovation confidently, ensuring the safety and privacy of patient data.”

Richard adds that vendors are responsible for managing the security risks of those IoT devices, and they often struggle because they don’t know what’s on the network. “We’ve got to get to a better understanding, better visibility of assets that connect to the network, what those assets are, what risks they pose to the integrity of the network and to patients who may be connected to them or being treated, managed or monitored by them and find a way to minimise those risks, either by sending out teams to patch those devices, where patches exist or by looking at compensating security controls,” he says.

“I think most hospitals struggle with that right now. They don’t have a modern network that support these technologies, certainly edge-based networking.”

Aaron Walton, threat intel analyst at Expel, says that healthcare organisations will continue to be pushed into finding more solutions to secure their networks. “However, these solutions need to be affordable and accessible,” he says.

“In this year and beyond, healthcare will move more toward solutions that can protect their networks – even when that network is connected to another, potentially compromised network – and solutions that can aid in meeting and demonstrating regulatory compliance requirements.

“More than ever, organisations recognise the considerable threats against their industry, while at the same time knowing they’re strapped for cash. Within all of this, organisations will need to ensure they can meet all these goals, and solutions will need to rise to the occasion.”

Work to be done

Indeed, there is plenty of work that needs to be done and that resellers working with healthcare organisations can do to guide healthcare organisations towards what they need and make sure they are as secure as possible.

“Unfortunately, a lot of hospital IT staff are constantly troubleshooting problems and they don’t really get a chance to sit down and work in project-based teams to evaluate, upgrade and optimise the kit they’ve got, they’re just trying to scrape it all together with Sellotape,” says Richard. “Unfortunately, that’s a result of chronic underinvestment. A lot of old kit has now gone, but we still don’t have the levels of optimisation of existing tools and technologies that hospitals have purchased and procured because they don’t have the expertise to use that.

“We’ve seen a huge rise in ransomware attacks against hospitals worldwide. The NHS has been pounded quite a lot over the last few years. This is an escalating trend and needs addressing.”

Alan says that, looking ahead, the healthcare sector is set to be influenced by several key trends, including the rollout of 5G technology, the increased application of AI and machine learning and the continued growth of telehealth services. “These developments will drive the need for more sophisticated networking solutions,” he says. “We cannot underestimate the critical role that networking solutions play in the healthcare sector’s digital transformation and, ultimately, in the health of the nation.”

Neil adds that the growth in the use of GenAI in cyberattacks will give rise to the potential for more advanced attacks that can discover IoT and OT devices on the network. “More malware will be created to specifically identify and connect industrial and medical-specific devices, and cybersecurity teams will need to adapt their strategy in turn,” he says. “We will also see the rise of traditionally air-gapped systems join the network, and they may lack updates or patches – and so require protection where no patches or vendor support is available anymore.”

Aaron Walton

expel

expel.com

> *“More than ever, organisations recognise the considerable threats against their industry, while at the same time knowing they’re strapped for cash.”*