Network Visibility: How to Eliminate Blind Spots That Impact Your Organization's Security and Performance

See your entire network; ensure your security and monitoring tools are receiving all the data they need — and only the data they need

It's no secret that healthcare organizations are under attack – and those attacks are on the rise. Since the COVID-19 pandemic, the rate of ransomware attacks has soared across all industries, with healthcare being the most targeted sector for data breaches.[1] The 2020 HIMSS Cybersecurity Survey revealed most organizations are experiencing significant security incidents, and that sobering fact is expected to hold true for the foreseeable future.[2]

At the same time, hackers are expanding their attack methods, thanks in part to the rise of remote working, telehealth and the growth of connected medical devices. Critical patient records, provider data and IoMT tools like monitors and medicine pumps are being targeted in new and creative ways. From 2021 to 2026, the healthcare industry is projected to spend $134 billion on cybersecurity.[3] Even so, attackers are outpacing most medical enterprise abilities, according to 96% of IT professionals.[4]

One reason healthcare organizations continue to be at a disadvantage: The security and monitoring tools they've invested in can only do so much without the right data.

Get a complete picture of your network

According to Bill Canter, Manager Healthcare Business Development, Keysight Technologies, adding security tools to your network is only part of the equation. Just like physicians need to have a full medical history to treat patients effectively, healthcare organizations need the ability to see across the entire network to successfully analyze and monitor emerging threats.

"Depending upon security and monitoring tools alone is not enough because they can't analyze what they don't see – and what you don't see can harm you," he pointed out. "Ensuring these tools have all the right data is key to finding that needle in the haystack."

A network visibility architecture suitably taps key network segments across the entire healthcare network and feeds only the needed data to each security and threat detection tool so it analyzes 100% of the needed data – and nothing more. "Hackers are exploiting the blind spots from tools not being configured correctly or not receiving the relevant data to analyze," explained Canter. "A visibility architecture eliminates those blind spots, allowing your tools to better identify potential threats hiding on your network."

> ***"Depending upon security and monitoring tools alone is not enough because they can't analyze what they don't see – and what you don't see can harm you."***

BILL CANTER | Manager Healthcare Business Development | Keysight Technologies

> ***"With a visibility architecture in place, your security tools can effectively detect any anomalous behavior, like an older connected device running on Windows 7 sending data to somewhere outside of the network, and you can quickly assess and take action on the risk."***
>
> BILL CANTER

Visibility crucial to IoMT devices

The growing use of IoMT (internet of medical things) devices for remote patient care and monitoring means healthcare organizations have to secure more connected medical devices than ever before. This hasn't escaped the attention of cybercriminals, who are developing more sophisticated techniques to attack these points of patient contact, gain access to valuable data and health system, then hold it for ransom.

"At the end of the day, the tools are no better than the data they analyze," he said. "Missing data from network blind spots, data drops, duplicate or unnecessary data, encrypted data – those are going to impact the efficiency of these tools. You have to be able to see everything. Visibility architecture allows you to capture data from your entire network, eliminating those blind spots, and then feeding only that needed data to each security tool."

For example, a healthcare provider might have 50 facilities where it needs to connect the data that sits on all of its clinical systems, security and monitoring systems, and hardware. "Network visibility is especially important for detecting risk for connected health devices spread across a large enterprise," Canter explained. "With a visibility architecture in place, your security tools can effectively detect any anomalous behavior, like an older connected device running on Windows 7 sending data to somewhere outside of the network, and you can quickly assess and take action on the risk."

In short, according to Canter, a visibility architecture that spans across data centers, edge locations such as clinics and hospitals, should be an essential part of your cyber strategy.

Beat hackers by thinking like a hacker

Once your security and monitoring tools are analyzing all the data across the entire network, you cannot simply set and forget your security stack. The threat landscape is constantly evolving.

Breach and Attack Simulation (BAS) tools enable you to hack your own network to see known threats and test your security posture to ensure tools are configured correctly. Most healthcare organizations do penetration testing every six or 12 months to remain in compliance. But having a breach and attack simulation tool as part of your visibility architecture lets you continuously validate your network and endpoint security controls.

"Using a good Breach and Attack Simulation tool, you can safely assault your security systems and teams with the latest threats to see what can get through undetected – the way a real hacker would – so that you can spot the gaps and close them," Canter noted.

As healthcare organizations continue to be popular targets, security investments that include a visibility architecture and BAS tools will help them prepare efficiently for the threats ahead.

References

1. U.S. Department of Health and Human Services. HHS Cybersecurity Program Ransomware Trends 2021. June 3, 2021.
2. Healthcare Information and Management Systems Society. 2020 HIMSS Cybersecurity Survey.
3. Attacks Predicted to Triple in 2021, Black Book State of the Healthcare Industry Cybersecurity Industry Report. November 13, 2020.
4. Ibid.