Beyond Healthcare Compliance: Are You Doing Enough to Ensure Visibility Across Your Entire Network?

To keep your data secure and compliant, you must understand what makes up your network, what's connected to it and what's at risk

For anyone working in healthcare IT, security is the biggest concern and greatest challenge – especially now.

More hackers than ever are targeting healthcare organizations to get access to patient data for impersonating identities, receiving free healthcare or filing fraudulent claims. In fact, 2021 was the worst year for healthcare data breaches, beating 2020's record of 642 data breaches.[1]

At the same time, hospitals and healthcare organizations are streamlining and improving quality of care by adopting more internet-enabled medical equipment and devices. While needed, these advancements – supported by web and cloud-based technologies – threaten network security and compliance.

With so much at stake, healthcare IT professionals need a complete and accurate inventory of the devices on their network to prevent unintended access. In an increasingly complex environment that expands as each new device connects to it, visibility across the entire network is critical.

To protect your network, you must see everything connected to it

Keeping a close eye on all network connectivity is a sound security strategy, but understanding what applications and devices are running on your network – configured connectivity – is far more important. It's all about seeing who really has access to your network.

"It's the difference between what you see in your car's rear-view mirror versus what you see on the dashboard," said Sean Finn, Senior Global Solutions Architect at RedSeal. "Observed traffic is evidence of what has happened in the past, and while it is helpful in identifying fires that need to be put out, this kind of 'retrospective data' has limited ability to help you avoid an obstacle in front of you and actually prevent problems."

Whether organizations are maintaining compliance with the Health Insurance Portability and Accountability Act (HIPAA) in the U.S. or General Data Protection Regulation (GDPR) in Europe, understanding configured access is the key to mitigating ransomware attacks and prioritizing vulnerabilities across the network. "In our experience, we find that while evidencing compliance for external requirements is important, healthcare organizations need to meet a separate set of internal requirements in order to continue their central mission of providing healthcare services," Sean noted. "There are a lot of facets to it. Focusing on 'periodic compliance' as an end game basically assigns it to a role of an overhead function, without necessarily providing operational benefit to the organization. Automating key parts of the operations can enable network segmentation compliance to be effectively maintained, as a natural part of 'business as usual.' This can provide effective proactive security, with compliance evidence available automatically, and on-demand."

"In our experience, we find that while evidencing compliance for external requirements is important, healthcare organizations need to meet a separate set of internal requirements in order to continue their central mission of providing healthcare services."

SEAN FINN | Senior Global Solutions Architect | RedSeal

> *"The ultimate goal of compliance is to ensure the systems – and healthcare – remain available. When compliance is intrinsically integrated with daily operations, the scope is minimized, and it becomes part of business as usual."*
>
> SEAN FINN

Without visibility, operational efficiency suffers

Today's network environments are complex. Visibility across the entire network can help healthcare organizations increase efficiency, as well as save time and money. This is especially helpful when resources are tight and your IT team still needs to perform regular maintenance or troubleshoot issues with an ever-expanding number of devices and ever-evolving software updates. "To have an accurate understanding of what the aggregate network is today can minimize the risk of misconfiguration and maximize the efficient use of staff time," Finn explained.

Having a clear understanding of what the network is – and what's on it – is crucial. An endpoint management system only provides security for the endpoints that it's installed on. "The authoritative source of 'What is on your network' is the network itself, of course ... but it's just not feasible to harvest and reconcile all of the detailed information manually. An automated collection of network configuration information enables automated reconciliation of the different types of data located on myriad devices across your network, providing insights that would be otherwise unobtainable," he said.

Instead of manually verifying the current state of the network, automation can make the process more efficient while ensuring people are taking action based on accurate understanding of the network today. "Unfortunately, asking an endpoint management system, 'Which endpoints are you not installed on?' is like saying, "Everyone not in this meeting, please say 'aye.' Without external feedback and auditing, most systems are limited in their ability to ensure that they are providing comprehensive coverage. Again, automation is key to achieving this type of insight and feedback," Finn said. "Automating the validation for the comprehensiveness of the coverage is the best advice I have for ensuring the effectiveness of security as a whole."

Beyond meeting compliance mandates

So many healthcare organizations are facing tight budgets and IT staff that are stretched thin. Staying on top of audit reporting and compliance can easily become a burden of distraction from primary operations. "The ultimate goal of compliance is to ensure the systems – and healthcare – remain available," he pointed out. "When compliance is intrinsically integrated with daily operations, the scope is minimized, and it becomes part of business as usual."

The rise of intelligent data-collecting devices is only going to make having visibility even more necessary. Nearly 25% of healthcare diagnostics by volume will involve quantified-self solutions by 2027.[2] "The richness of what's interconnected – and the consequence of what's interconnected – is going to continue to increase, and with that, effectively securing the functionality of the information system is critical to securing the delivery of healthcare services," Finn concluded.

Only by knowing what's on your network, what's connected to your network and what's at risk can healthcare IT professionals build a strong foundation for preventing cyberattacks.

To learn more, visit www.Redseal.net. To see RedSeal in action, sign up for demo here or Cyber Threat Hunt here.

References

1. The HIPAA Journal. December 30, 2021. Largest healthcare data breaches of 2021. https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2021/
2. Research and Markets. March 2022. Quantified self in healthcare market by technology, devices and applications 2022 - 2027. https://www.researchandmarkets.com/reports/5313938/quantified-self-in-healthcare-market-by

---

REDSEAL

About RedSeal

RedSeal—a security solutions and professional services company—helps government agencies and Global 2000 companies see and secure their on-premise networks and cloud environments. The RedSeal award-winning security solution verifies that networks align with security best practices, validates network segmentation policies, and continuously monitors compliance with policies and regulations. It also prioritizes mitigation based on each vulnerability's associated risk.