The New Normal: Cybersecurity and Performance Optimization

As healthcare organizations scramble to keep pace with a massively complex application, network and threat landscape, comprehensive visibility remains crucial

For healthcare organizations (HCOs), protecting internet-connected hardware, software and data applies to an ever-growing list of connection points, everything from electronic health records (EHRs) to remote patient monitoring devices to email platforms. Medical devices with legacy systems no longer supported by the manufacturer and the shift to nonclinical staff working remotely during the coronavirus pandemic only add to the challenge of keeping patient information, intellectual property and financial data secure.

These days, however, health information technology (IT) professionals must focus on much more than protecting the network. They have to optimize the performance of everything connected to it once it's protected, so clinical care teams can access the information they need – wherever it resides – exactly when they need it.

Recent research from the U.S. Department of Health and Human Services (HHS) underscores the importance of maintaining performance for patient outcomes: At hospitals that experienced a data breach, the death rate among heart attack patients increased.[1] With every second critical to clinical care teams, health IT teams must deliver seamless operation and accessibility to clinical applications from anywhere, anytime, over any device. And time is of the essence.

"The network has become really important to healthcare organizations, almost more than ever before," explained Tom Bienkowski, Director of Product Marketing, NETSCOUT. "When COVID-19 hit, they had to shift nonmedical personnel out of the hospitals to work remotely and ramp up telehealth and virtual meeting systems. And everything was relying heavily upon the network."

The complexity of maintaining systems and applications across distributed hybrid cloud environments was already challenging enough before the pandemic. But when HCOs were forced to rapidly deploy telemedicine and other clinical apps, the increase in traffic across their network and security infrastructure slowed down networks just as clinical care teams needed them most.

Cyber threats on the rise

Making matters worse, in the first half of 2020, there was an almost a 50% increase in the number of reported breaches in hospitals and healthcare providers' networks, according to HHS.[2]

"The entire threat landscape has exploded," Bienkowski explained. "One of the most fundamental things healthcare organizations can do right now to protect the performance, availability and security of their systems and data, is ensure they have holistic visibility across the entire network."

To do that, health IT teams must embrace a dual role of both protecting and enhancing clinical, business, security and network applications' performance in a complicated environment. Being able to detect potential threats and resolve them quickly may be a top priority, but keeping all of the supported systems and applications up and running properly – even when working at capacity – is equally important. Maintaining network performance in today's complex health ecosystem is more easily accomplished with a shift in how health IT teams approach working together.

Get creative

It's no secret that HCOs lag behind other industries when investing in infrastructure to support technology systems. According to the *2020 HIMSS Cybersecurity Survey*, 61% of healthcare leaders surveyed acknowledged they don't have effective mechanisms to maintain proper cybersecurity.[3]

"They say countless problems in networks and application management occur because a change happened in the environment. ... The good news is that you can have your network and security teams looking at a common source of network-based data to come up with the solutions to issues caused by changes, whether it's performance- or security-related."

Eileen Haggerty | Assistant Vice President, Product and Solution Marketing | NETSCOUT

But health IT teams can often get more value when they delve into the investments their hospital or organization has already made. One often overlooked way to beef up cybersecurity features, for example, is to see if the Security Operations (SecOps) team can leverage the tools the Network Operations (NetOps) team is already using, according to Bienkowski.

Remain proactive

"Healthcare IT professionals know there's no good time to schedule downtime to do system maintenance or upgrades. Friday night could be the busiest time in an ER, and you have to be up," explained Eileen Haggerty, Assistant Vice President, Product and Solution Marketing, NETSCOUT. "Using real evidence from your own network can help you plan when best to perform some of those necessary upgrades."

At the same time, network analysis tools can help you identify what's likely to disrupt performance, whether they're bottlenecks, increases in unknown traffic or time-of-day changes. NetOps and SecOps teams can set up alerts to notify them of suspicious behavior patterns like these so they can address issues well before they have an impact on patient care.

Standardize procedures

"They say countless problems in networks and application management occur because a change happened in the environment," explained Haggerty. "You put in a new router, upgraded the software on a device or migrated an application to the cloud and then something else breaks. The good news is that you can have your network and security teams looking at a common source of network-based data to come up with the solutions to issues caused by changes, whether it's performance- or security-related."

Think holistically

HCOs typically have their NetOps and SecOps teams operating in silos, which can dramatically affect how quickly information needed to troubleshoot problems is shared with the right team member. But having a single source of truth for the entire network means everyone, regardless of their role, can see when a potential issue could arise.

"It's about building collaborative procedures," explained Bienkowski. "And once you have those cross-functional practices in place, you need to continuously fine-tune them. And that's where the rubber meets the road. You can learn from an incident and adjust your playbooks and plans accordingly. But it all starts with an attitude change."

Use a single source of truth

Commanding a big-picture view that can reveal a problem or problems, whether they're from an internal source or an external solution from an outside vendor, gives IT teams visibility into how all of the specific applications, network and cloud tools, and databases are operating.

In order to foster the collaboration that will simplify managing a complex health IT environment, CIOs and CTOs need to think more strategically about the advantages of having NetOps and SecOps teams use the same data sources for decision-making.

"By always using the same consistent network-based data, both your network and security teams can focus on solving the larger issue, whether it's performance- or security-related," explained Bienkowski. "Ultimately, they're responsible for speeding the time to threat resolution and keeping all applications and systems running seamlessly to ensure patient safety and quality of care."

When clinical care workers call to say they can't get through to a data center or access their patient records, for example, IT teams can lose a lot of time figuring out the disruption and who's responsible for fixing it.

"When NetOps and SecOps use different tools, it slows down their ability to collaborate," said Haggerty. "Using a single source of truth means they can rectify the situation that much faster."

"Once you have those cross-functional practices in place, you need to continuously fine-tune them. And that's where the rubber meets the road. You can learn from an incident and adjust your playbooks and plans accordingly. But it all starts with an attitude change."

Tom Bienkowski | Director of Product Marketing | NETSCOUT

"By always using the same consistent network-based data, both your network and security teams can focus on solving the larger issue, whether it's performance- or security-related."

Tom Bienkowski

Streamline roles

"I was listening to one of our colleagues talk to one of our customers recently," explained Bienkowski. "And the customer said, 'I have an IT Team, a NetOps team and a SecOps team. And it's like the lines are blurring between them all the time. We're actually going to change it to TechOps because we don't see a distinction between the teams anymore.'"

This is especially true when NetOps and SecOps work on the same project, such as upgrading the capacity of the virtual private network controllers, firewalls, or the wide area network Inter-Switch Link.

"This kind of project is already clearly oriented toward a combination effort," explained Haggerty. "So it's perfect for them to shift their attitude so they work together toward an overarching goal that meets the deadline, budget and operation needs of the hospital."

Working together to see across the entire network

Ultimately, visibility across the entire IT infrastructure enables health IT teams to measure the performance of the network and all of the applications, systems and devices it supports. Gaining end-through-end visibility is key to evaluating data, traffic, voice, video and other network factors in order to identify issues or disruptions throughout the infrastructure.

Adopting a high-level, collaborative approach is also cost-effective. Especially when health IT budgets are lagging: Only 6% or less of the IT budget is allocated for cybersecurity, according to the *2020 HIMSS Healthcare Cybersecurity Survey*.[4]

Considering the increasing complexity of network environments and growing number of security incidents, leveraging current employee talents and common network monitoring tools can help HCOs stay ahead of today's and tomorrow's threats.

"Healthcare IT teams had to invest in a variety of … alternatives this last year on a real quick turn," explained Haggerty. "Now their goal should be to optimize for the services they need, taking a collaborative approach where both roles work together more efficiently to reduce the risk of breaches that could jeopardize network performance."

For more healthcare security resources and to learn more about NETSCOUT's network, business and application performance management solutions, visit netscout.com/healthcare.

References

1. Akpan, N. 2019. Ransomware and data breaches linked to uptick in fatal heart attacks. Oct. 24. *PBS Newshour*. https://www.pbs.org/newshour/science/ransomware-and-other-data-breaches-linked-to-uptick-in-fatal-heart-attacks.
2. Hackett, M. 2020. Number of cybersecurity attacks increases during COVID-19 crisis. June 4. *Healthcare Finance News*. https://www.healthcarefinancenews.com/news/number-cybersecurity-attacks-increase-during-covid-19-crisis.
3. HIMSS. 2020. HIMSS healthcare cybersecurity survey. Nov. 16. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey.
4. Ibid.

Produced by HIMSS | www.himss.org | ©2021