How NetOps and SecOps Can Unite to Resolve Security Threats

Using the same network monitoring tools increases visibility and speeds the time to threat resolution

Distributed denial of service (DDoS), ransomware, malware attacks – these serious network security incidents can dramatically affect business at every company, but they're especially troubling for healthcare organizations (HCOs). If clinical care teams can't access online lab results, diagnostic tests, medical imaging or patient health records when they need them, patient care is significantly impacted. In critical situations, delays due to slow networks, for example, can even result in serious injuries or death.

"This past year has been sort of the perfect storm for healthcare IT," explained Eileen Haggerty, Assistant Vice President, Product and Solution Marketing, NETSCOUT. "Healthcare workers are working at capacity while innumerable devices – workstations, a cart on wheels, a smart bed, mobile devices – are being connected to the network. They've had to support more telehealth appointments and devices for employees working at home. The sheer volume of traffic coming through the core network has been slowing down the healthcare delivery system exactly when time is of the essence."

Responsible for monitoring and maintaining networks that directly impact patients' health and safety, network operations (NetOps) and security operations (SecOps) teams have traditionally operated in silos. But expanding network and cloud architectures have opened up more ways than ever for cyberattacks, making collaboration a critical part of network and security roles.

> *“Network monitoring is the key to maintaining the performance of your applications and protecting yourself from some of these threats. Having the proper level of visibility across the entire digital infrastructure … enables you to see signs of compromise … .”*
>
> **Tom Bienkowski** | Director of Product Marketing | NETSCOUT

NetOps the first line of defense

Phishing is the most common entry point for network compromise. A majority of respondents (89%) to the 2020 *HIMSS Healthcare Cybersecurity Survey* cited this kind of security incident as a top concern.[1]

The first line of defense against these attacks are NetOps teams, who now find their networks supporting a vast array of applications, devices and systems. As a result, network infrastructure and security are becoming one and the same, blurring the lines between NetOps and SecOps roles. Once security finds something suspicious, for example, they need to know how widespread it is across the network to address the threat.

A proactive, collaborative approach is crucial

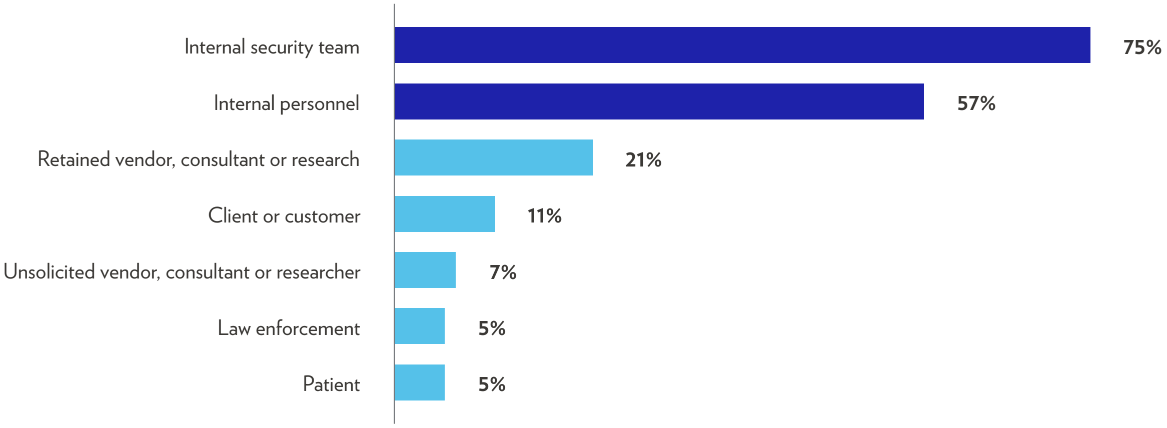
In addition to detecting threats, NetOps and SecOps teams are responsible for investigating and remediating them. Anti-virus software, firewalls and routers to block malicious communication can help prevent attacks only as much as they are properly maintained or updated, however.

“Network monitoring is the key to maintaining the performance of your applications and protecting yourself from some of these threats,” explained Tom Bienkowski, Director of Product Marketing, NETSCOUT. “Having the proper level of visibility across the entire digital infrastructure – no matter where it may reside – enables you to see signs of compromise like weird traffic going to places it shouldn’t be or a large increase in bandwidth due to a DDoS attack.”

As HCOs’ network environments evolve and become more complex, they must support a combination of legacy systems and new hybrid cloud environments. Internal resources are their primary defense for ensuring these systems stay secure and operational (Figure 1).

“When clinical care workers call to say they can’t get through to a data center or access their patient records, IT teams can lose a lot of time figuring out the disruption and who’s responsible for fixing it,” explained Haggerty. “When NetOps and SecOps use different tools, it slows down collaboration. Using a single source of truth means they can rectify the situation that much faster.”

Figure 1. How survey respondents learn about significant security incidents



Source: HIMSS. 2020 HIMSS Healthcare Cybersecurity Survey. Chicago: Author

> *"Healthcare IT teams had to invest in a variety of different alternatives this last year on a real quick turn. Now their goal should be to optimize for the services they need, taking a NetSecOps approach where both roles work together more efficiently to reduce the risk of breaches that could jeopardize the network."*
>
> **Eileen Haggerty** | Assistant Vice President, Product and Solution Marketing | NETSCOUT

By using the same set of tools, NetOps and SecOps have a unified, holistic view of network performance that streamlines the resolution process. With less back-and-forth across departments when an issue arises, the team saves valuable time, and can even quickly share evidence with any third-party vendors that may be the source of the threat.

Optimize IT investments for security

Not only is using one set of tools for different teams more efficient, but it's also cost-effective. Especially when health IT budgets are lagging: Only 6% or less of the information technology budget is allocated for cybersecurity, according to the 2020 *HIMSS Healthcare Cybersecurity* Survey.[2]

Considering the increasing complexity of network environments, growing number of vendors involved, and growing number of security incidents, HCOs might have to get creative. Leveraging current employee talents and network monitoring tools can help HCOs stay ahead of today's malicious actors and tomorrow's threats.

"Healthcare IT teams had to invest in a variety of different 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 NetSecOps approach where both roles work together more efficiently to reduce the risk of breaches that could jeopardize the network."

Collaboration between NetOps and SecOps is more important than ever in an increasingly hostile digital environment. To learn more about the tools that can help optimize network performance, visit netscout.com/healthcare.

References

1. HIMSS. 2020. HIMSS healthcare cybersecurity survey. Nov. 16. https://www.himss.org/resources/himss-healthcare-cybersecurity-survey.

2. Ibid.

NETSCOUT

About NETSCOUT

NETSCOUT assures digital business services against disruptions in availability, performance, and security. Our market and technology leadership stems from combining our patented smart data technology with smart analytics. We provide real-time, pervasive visibility and insights customers need to accelerate and secure their digital transformation. Our approach transforms the way organizations plan, deliver, integrate, test, and deploy services and applications. Our nGenius service assurance solutions provide real-time, contextual analysis of service, network, and application performance. Arbor security solutions protect against DDoS attacks that threaten availability and advanced threats that infiltrate networks to steal critical business assets.

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