Market Pulse

WHITE PAPER

Healthcare IT: The Convergence of Network + Security

Executive Summary

Healthcare IT is at a critical juncture. The infrastructure supporting healthcare operations has been stressed more than ever due to the pandemic, the resultant spike in telehealth, increased use of cloud-based SaaS applications, and widespread use of connected medical devices. While the need for resiliency and increased security was already apparent, it has been accelerated by the current conditions.

IDG recently surveyed 200 healthcare IT professionals from all segments of the healthcare industry to get a read on how they're handling this massive increase in demand. Among the myriad of findings, the survey revealed how healthcare IT leaders are integrating their networking and security strategies to increase the efficacy of both and seeing the value of engaging a managed service provider to shore up talent and technology shortfalls.

Introduction

Healthcare IT is under pressure like never before. The onset of the global pandemic in early 2020, and its impact on the dramatic increase in telehealth and remote doctor visits, have placed a tremendous burden on healthcare IT infrastructure. Healthcare organizations are also using more cloud-based SaaS applications and advanced technologies to support connected devices and the Internet of Medical Things (IoMT). Network resiliency and security are therefore more pivotal than ever.

While there have always been shortfalls in healthcare IT, those gaps have been exacerbated by the events of 2020. Studies from the Centers for Disease Control and Prevention show a 50% rise in the use of telehealth services from the first quarter of 2019 to the same period in 2020, and some providers report experiencing spikes of 80% to 100%.

"The biggest causes for network demand have been virtual visits, the mobile workforce, pop-up clinics, and hospitals with a growing ecosystem of locations and partners with whom

IDG SPONSORED CONTENT

MASERGY | FORTINET

they need to securely connect," says Troy Ament, Fortinet's Field CISO for Healthcare. "And equally dramatic is the move to working from home. Those have been major challenges, and with each representing different IT requirements."

Healthcare IT leaders have done their best to keep up, but how can they do better? What do they consider the most critical technologies? How are they managing staffing and talent shortages? And how are they preparing for the coming year? New IDG data reveals how healthcare IT leaders feel about these questions and how they are more frequently engaging in unified strategies with a focus on consistency, predictability, and working within managed service models.

Healthcare Network Security and Resilience Remains Critical

On behalf of Masergy and Fortinet, IDG recently surveyed 200 healthcare IT leaders from all facets of the healthcare industry, including hospitals, primary care facilities, urgent care facilities, pharmaceutical companies, and others. The primary intent of the survey was to evaluate network and security challenges, the approaches healthcare organizations take to resolve those challenges, and the importance of integrating network and security policy.

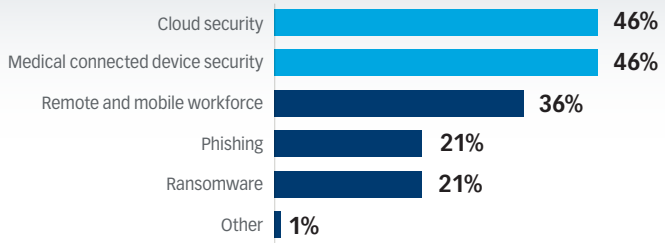
One of the critical themes emerging from the results is the vastly increased use of cloud platforms and IoMT devices, all of which has led to an equally dramatic increase in network demands. And this surge in demand must continue to operate under stringent security protections. The survey data shows healthcare IT leaders are tackling both reliability and security collectively.

Here's a closer look at three of the major trends and top-of-mind issues for healthcare IT leaders.

1. Cloud and Connected Security Challenge Healthcare IT

The first trend is the emergence of cloud security (cited by 46% of respondents) and connected device security (also cited by 46%) as the top security challenges for healthcare IT and executive leadership. With the surge of remote healthcare and increased use of IoMT devices, there are more connected devices, cloud-based applications, and cloud platforms and services driving healthcare operations than ever. This poses increased security risks, including anything from data breaches to phishing and malware attacks.

FIGURE 1. **TOP HEALTHCARE SECURITY CONCERNS**

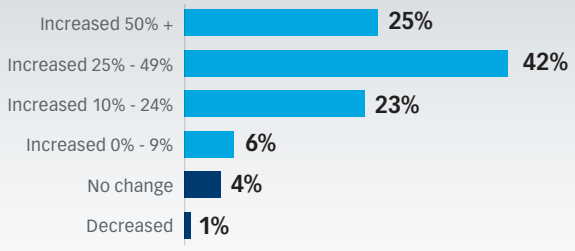


Ensuring continued healthcare security and data privacy is just as critical as ever. Ament agrees with the critical nature of healthcare security. "The attack surface of healthcare systems will continue to grow. There is still a transformation of moving paper processes to digital that continues," he says. "Now you've got healthcare systems making a significant cloud migration, so healthcare organizations are going to need to continue to focus on new risk assessments and protect those new workflows."

2. Network Traffic Demands Surge

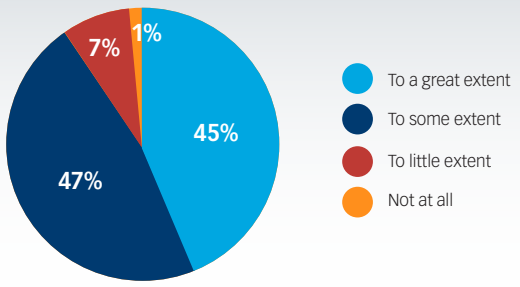
The second trend revealed by the survey data is the sheer surge in network traffic volume. The survey states nearly all respondents (95%) report an increase in network traffic since March 2020, owing to the onset of the pandemic. Most healthcare organizations have also had to increase network bandwidth capacity to accommodate an influx of IoMT devices (45% reporting to a great extent, and 47% reporting to some extent). These increases in network demands are actually shifting IT priorities, forcing healthcare IT leaders to adjust their strategy and rethink their infrastructure. More network traffic and connected devices means more to monitor and maintain when it comes to ensuring cloud application performance, data security, and HIPAA compliance.

FIGURE 2. **CHANGE IN NETWORK TRAFFIC SINCE MARCH 2020**



Market Pulse

FIGURE 3. **INFLUX OF IoMT DEVICES FORCING ORGANIZATIONS TO INCREASE NETWORK CAPACITY**



3. Budgets on the Upswing

The third trend the survey revealed is that in response to these growing demands, healthcare executives are increasing IT budgets. More than half of the survey respondents (54%) expect IT budgets to increase in 2021. So how will healthcare IT leaders prioritize this new budget capacity? What are they looking for in 2021 as they face the challenges of ensuring cloud platform and connected device security and addressing the continued increase in network demands? The survey data reveals enduring themes around convergence, simplicity, and achieving a level of certainty as it relates to network performance.

A Unified Approach for Improved Consistency, Efficiency

Healthcare IT must work in concert with healthcare business executives to establish and maintain a strong governance program. "A good governance methodology accomplishes several goals: It sets the rules of the road and the framework you need to follow, as well as aligns the business, so that different groups know what their stake is," says Ray Watson, Vice President of Innovation at Masergy. "An organization with a good governance method is one in which the business runs IT, sets priorities, knows the budget, and understands the challenges."

In achieving governance, healthcare IT leaders now prefer a single, simple, unified approach. They're interested in investing in network and security technologies as an integrated one-two punch. Previously, network and security issues were often seen as separate competing demands and were led by separate initiatives and teams. Healthcare IT leaders are now increasingly addressing those together.

"That's a truly effective strategy to ensure the network fabric you're putting down is secure," says Ament. "The benefits are cost savings, as you're able to adhere to compliance much easier, and you're more effective in terms of network reliability and security operations when they're completely integrated."

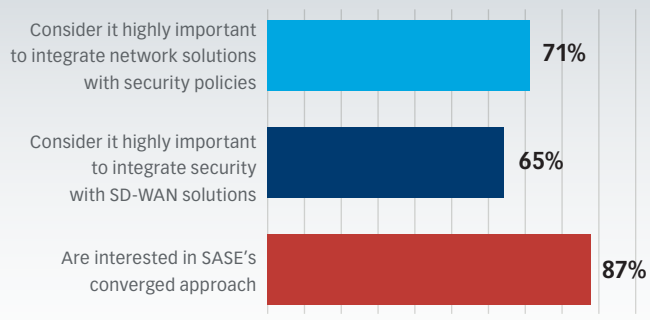
Survey respondents report a high level of interest (87%) in SASE (secure access service edge), which refers to converged offerings combining SD-WAN capabilities with network security functions. Most respondents (71%) also consider it highly important to integrate network solutions with security policies. In fact, integrating security with SD-WAN solutions is considered critical or highly important by 65% of respondents.

They also want consistency in their security and predictability in their network services. Most respondents (60%) indicate having a single security architecture delivering consistent security policies across multiple locations is highly important. Meanwhile, more than two-thirds of respondents (67%) consider an ultra-low latency network as highly or critically important.

Outages are unacceptable because they often force doctors and nurses to turn patients away or revert to paper-based recordkeeping processes. That certainly explains why healthcare IT is increasingly evaluating secure SD-WAN solutions. While 46% of organizations report having piloted or installed SD-WAN, another 35% are actively researching SD-WAN. Respondents cite improved cloud application performance, branch security, and cost reduction as the top drivers for using and considering SD-WAN.

"First and foremost is the underlying infrastructure," says Ament. "All that infrastructure supporting electronic medical records, virtual visit technologies, communication technologies, and ancillary clinical systems—those are all critical."

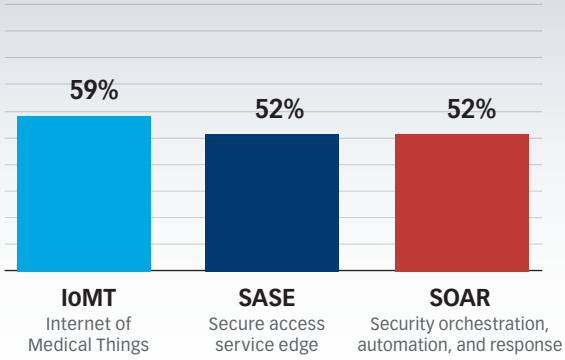
FIGURE 4. **HEALTHCARE IT'S INTEGRATED STRATEGY**



Market Pulse

Healthcare IT is also looking to improve operational efficiency with artificial intelligence (AI). Survey respondents are strong investors and firm believers in the value of AI. More than two-thirds (68%) indicate their organization is currently using AI to manage network performance, security, or both. Another 25% indicate interest in using AI.

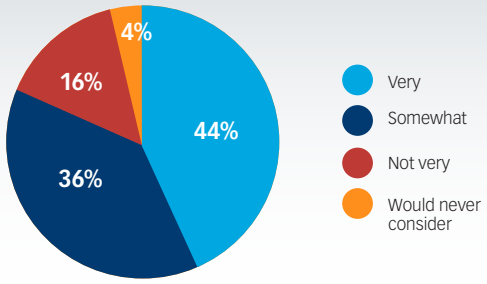
FIGURE 5. **TOP THREE CRITICAL SECURITY TECHNOLOGIES FOR HEALTHCARE IT**



Partnership Engagement Solves the Challenge of Management

Healthcare IT is not taking on these burdens by itself. Most healthcare organizations are engaging in managed service provider (MSP) partnerships, with 80% indicating they are likely and 44% very likely to engage a managed service provider to handle network and/or security services. There are multiple drivers for survey respondents to outsource network and security services, including cost savings (38%), enhanced network performance and security (37%), and improved response time (37%).

FIGURE 6. **LIKELIHOOD OF ENGAGING AN MSP FOR NETWORK OR SECURITY SERVICES**



To best manage the continued surge in network traffic and the demands of cloud security, healthcare IT leaders realize their strategic initiatives and tactical actions must be more integrated. They are eager to make that happen but are not always prepared with the right technologies or skill sets. And that is where the MSPs come in.

"Healthcare IT continues to struggle with challenges around hiring and retaining staff. Nearly all could use additional resources which focus on network security and operations," says Watson. "So, when evaluating a potential MSP, look for specific skill sets which will complement the staff you have in place."

Plan Now to Ensure Sufficient Network Resiliency and Security

Healthcare IT infrastructure has been put to the test like never before. The increased use of cloud and IoMT devices against the backdrop of the pandemic has exposed significant gaps. Telehealth is a voracious consumer of bandwidth. Additionally, there is an increased need for greater security at the network edge, as well as secure remote access to the network, cloud-based SaaS applications, and sensitive healthcare data.

Healthcare IT leaders and executives alike have recognized the aforementioned challenges and are ready to boost their infrastructure to address critical current requirements and plan for the future. Approaching IT with an integrated strategy is a smart plan. "When you're talking about network reliability or security operations," says Watson, "they are more effective and more efficient when they're working in unison. With the explosion of devices and distributed cloud workloads, utilizing a single platform to address both security and the network is often the best way to reduce complexity."

MORE INFORMATION

To learn more about how your healthcare organization can integrate its networking and security strategies to increase the efficacy of both, please visit Masergy.com/feature/healthcare-it.

MASERGY | FORTINET