Security, Resilience and Agility in Times of Change

The New Tomorrow for Healthcare

Gigamon®

Introduction

For the healthcare industry, the world has changed. Within a short period of time, COVID-19 and its aftermath has changed the way the industry thinks and operates both today and in the future.

In the context of IT teams, this means supporting a newly distributed administrative workforce, accelerating digital initiatives around telehealth and enhancing security to contend with ever increasing threat levels. Furthermore, with the cost and revenue changes forced on the healthcare industry by the crisis, it means doing all of these things with already over-stretched teams, budgets and networks.

The healthcare industry was already faced with dramatic changes and historic challenges before the COVID-19 crisis; now these changes are being forced on the industry at an unprecedented rate. But for organizations with the resilience, agility and resources to embrace these challenges, there is also the opportunity to re-imagine and re-build a patient-centric delivery model based on the latest thinking and technologies.

Overview

This paper looks at IT priorities that healthcare organizations will need to address now, in the Return To Work transition and in The New Tomorrow:

TODAY

The imperative is to ensure the best possible levels of patient care, customer and internal user experiences and business continuity, while also ensuring organization security. In most cases, this has to be achieved with frozen budgets and resources.

RETURN TO WORK

Organizations were forced to transition the majority of their administrative and support staff to Work From Home (WFH) in a matter of days, but the Return To Work (RTW) process will most likely take place over several months and will require a flexible staffing and IT model.

THE NEW TOMORROW

Faced with uncertainty, challenges and opportunities, healthcare organizations must develop models that cover a number of possible future states and build an agile network and security infrastructure to support these models.

We would like to share our thoughts on how organizations can best navigate these unprecedented times based on what we are seeing across our customer base of leading organizations in the healthcare industry.

Today

As the immediate impact of the COVID-19 crisis has settled, healthcare IT teams are now faced with a new set of challenges driven by the four business imperatives.

Deliver the Best Possible Patient Care

Delivering the best possible patient care remains the essential mandate for all healthcare organizations. Achieving this through the COVID-19 crisis has forced dramatic changes in the approach most healthcare delivery organizations have adopted towards patient care. These changes have ranged from creating physically separate treatment facilities for COVID-19 patients; deploying a WFH model for administrative staff; cancelling revenue-generating elective surgeries and the use of telehealth systems as the first line of interaction between patients and their healthcare teams.

At the IT level, this has meant developing and supporting new SaaS and internally built applications, adding new network segments and ensuring the security of a massively increased attack surface.

Optimize Today's WFH Model

For most healthcare organizations, the shift to a WFH model left IT teams with little time to plan or scale their remote access infrastructure. However, although some organizations experienced some issues bringing this infrastructure online, most have now stabilized their WFH capability and are focused on optimizing this environment to provide the best possible user experience to their employees.

This WFH capability is often dependent upon video conferencing applications such as Zoom, WebEx and Microsoft Teams. While these apps are SaaS-based and can rapidly scale, they can place a heavy load on network bandwidth often resulting in a poor user experience. Additionally, well-publicized security weaknesses in some of these apps and in the way that organizations and individuals use these apps may pose potentially serious security issues.

Secure the New Network

Bad actors quickly exploited the COVID-19 pandemic to compromise newly expanded network infrastructure, applications and users who had not been fully trained in remote working procedures. This challenge was compounded in cases where remote workers used inadequately secured mobile phones, personal computers or home networks to access the corporate network.

This led to a variety of security issues. For example, Mirai botnet–type attacks that infected the organization's network or dropper-based attacks that loaded malware to steal users' credentials and ultimately lead to ransomware attacks or data exfiltration. Even the mandated use of VPNs does not fully solve the problem, especially if endpoints have not been adequately secured.

There has also been a spike in state-sponsored security attacks on lab and research facilities as reported recently in the *Wall Street Journal*[1]. In this report, U.S. officials suggested that Chinese and Iranian hackers are targeting universities, pharmaceutical and other healthcare firms that are working to find a vaccine for COVID-19, in an attempt to disrupt this research and slow the development of a vaccine.

In the short-term, the imperative is for IT organizations to optimize their existing infrastructure, tools and applications investments.

Working with Frozen and Reduced Budgets

It is already clear that all healthcare organizations must review their financial plans and spending budgets against a range of different financial scenarios. Many CIOs are working with their organizations' financial teams to drill into IT project and staffing costs and other expenses in order to prioritize spending and resource allocation based on these scenarios.

However, in the short term, the imperative is for IT organizations to optimize their existing infrastructure, tool and application investments. In most cases, this means a freeze on new projects and a re-allocation of both financial and human resources to support the priorities of protecting patient care, optimizing WFH capabilities and maintaining security across the organization. In summary, the need to do more with less has never been more pressing.

Return to Work

Most healthcare organizations are now planning the phased RTW process and have formed cross-functional teams with IT being a key part of those teams and process. But while these plans are being developed, what should IT, NetOps and InfoSec teams focus on? Looking at Gigamon customers, we see that they are focusing on projects that fall into three broad areas.

Plan the Return to Work

Many organizations are planning a future in which significant number of their employees will continue to work from home either on a permanent basis or for an extended period of time as part of a mixed onsite/offsite model. A survey by 451 Group taken in March[2] suggested that 38 percent of survey respondents expected this to become the new normal for their organization; however, a poll taken during a recent Gigamon Healthcare webinar[3] suggested this could be high as 75 percent.

For these organizations there are many learnings to be drawn from the WFH transition. For example, where employees are not provided with company-issued laptops and phones, ways must be found to secure personal devices and home networks that attach to the corporate network. In most cases, this will involve both endpoint and edge security, as well as ensuring employees apply security updates (with support as necessary) to their home networks.

Maybe the most serious technical challenge IT organizations face is how to provide a seamless onsite and offsite RTW experience, where the same applications, user experience and security are available in both environments.

One of the organizational learnings from the WFH is the need to maintain engagement with remote employees. Once the novelty of virtual team lunches and happy hours wears off, keeping remote employees engaged and productive will become a long-term challenge.

Keeping remote employees engaged and productive will become a long-term challenge.

Optimize Network and Application Visibility

The COVID-19 crisis has made clear the importance of network and applications visibility. Many organizations have realized that they lack visibility into their network operations and applications. This has been highlighted by the widespread use of video apps such as Zoom. A key learning from managing these apps is that, while all traffic needs be monitored, once that traffic is determined to be safe or low risk, it can be filtered to reduce overall network traffic and the burden that this places on network management and security tools

When application performance issues do arise, it is often necessary to look beyond network bandwidth issues that can be observed by, for example, frame-rates slowing or quality dropping from HD to SD to understand what is happening in the interaction between the application and the network.

In these cases, the ability to use the metadata within the application can be critical in determining where potential bottlenecks or other issues exist that cause poor application performance and user experience.

In a world where healthcare consumers and the workforce want or need to operate on an “access anywhere anytime” model, moving towards a Zero Trust architecture not only makes sense, it is close to an imperative.

Re-Evaluate Security

Healthcare InfoSec and SecOps teams are continuously assessing and tuning security models, procedures and tools. However, for many organizations, the reality is that they went into the COVID-19 crisis with significant security vulnerabilities as a result of:

+ Understaffed InfoSec and SecOps teams[4]
+ Under-trained end users
+ Rapid growth of encrypted North-South and East-West traffic
+ Massive growth in traffic and attack surface as a result of telehealth and IoMT adoption

These issues have now been compounded by the additional stress that the crisis has placed on security staff, tools and budgets.

While the correct security model will vary by organization based on their unique situation and resources, the key building blocks for a successful, agile security model are ensuring end-to-end visibility into all network traffic; AI and ML-based analytic tools that detect and prioritize anomalies and threats; and automation tools that handle mundane tasks freeing security teams to focus on the highest priority issues.

For some healthcare organizations, this security review may include an evaluation of adopting a Zero Trust model. In a world where healthcare consumers and the workforce want or need to operate on an “access anywhere anytime” model, moving towards a Zero Trust architecture not only makes sense, it is close to an imperative. At the simplest level, because the network is under constant attack from a huge array of external and internal threats, all users, devices, applications and resources must be treated as being hostile. These users and devices need to be rigorously authenticated, and data and other network assets need to be protected at a much more granular level than perimeter-based security models allowed.

The New Tomorrow

Many forward-thinking healthcare organizations are already looking beyond today's crisis recovery situation and re-imagining their business model in what people are calling the New Normal, the Next Normal or The New Tomorrow.

As in any period of economic turmoil, The New Tomorrow will bring new challenges and opportunities. While the degree of change, challenge and opportunity will vary based on the risk-tolerance of individual healthcare organizations, those that thrive in The New Tomorrow will share a number of characteristics that will be common to their business culture, models and supporting infrastructure.

These organizations will be resilient, innovative and forward looking. They will develop business models that are resilient, agile and can respond quickly to changing market and consumer needs. And they will have IT infrastructures that mirror these core values.

VISIBILITY

You can't manage what you can't see and gaining visibility into all network traffic will become a survival issue for many organizations. The physical, virtual and cloud-based visibility into both encrypted and unencrypted data that Gigamon provides is already trusted by many of the world's most demanding organizations, including leading global banks, healthcare, service providers, SaaS companies and government departments.

GROWTH

Many organizations will need to significantly upgrade their networks as they deliver new online experiences to their customers, innovative digital capabilities and embrace emerging technologies such as IoMT. In addition, the financial stress that the COVID-19 has placed on the healthcare industry means that the process of consolidation that was already a major factor in the industry's development will accelerate in 2020 and beyond, a process that will drive the need for network consolidation in many organizations.

AGILITY

As recent events have shown, agility doesn't just mean handling the pressures of growth and innovation; it also means handling unforeseen and unprecedented change. In this situation, it is critical that organizations' networks and security capabilities can support continued changes in working practices and new tools deployment.

CLOUD

For reasons of time-to-market and scalability, the cloud is the preferred application deployment platform for The New Tomorrow, whether these are SaaS-based apps or custom-based applications that reflects an organization's unique needs and capabilities. As cloud adoption accelerates, maintaining visibility into all information — regardless of whether it is on-premises or in the cloud — and having the ability to secure it, will become an increasingly important mandate for successful healthcare organizations.

Final Thoughts

The COVID-19 crisis has set off a chain reaction of events that will profoundly affect not only the healthcare industry, but also the economy and our society. Healthcare organizations and their IT teams have responded successfully to the initial shock of the crisis, but the hardest challenges — and greatest opportunities — lie ahead. To survive those challenges and take advantage of those opportunities, healthcare organizations will need resilience, agility and visibility into every aspect of their operations.

[1] Lubold, Gordon, and Dustin Volz. "U.S. Says Chinese, Iranian Hackers Seek to Steal Coronavirus Research." The Wall Street Journal. May 14, 2020. https://www.wsj.com/articles/chinese-iranian-hacking-may-be-hampering-search-for-coronavirus-vaccine-officials-say-11589362205.

[2] Crawford, Scott, Dan Kennedy, Fernando Montenegro, Eric Hanselman, Garrett Bekker, and Aaron Sherrill. "COVID-19 and Beyond: Will the Work-From-Home Explosion Revolutionize Enterprise Security Architecture?" 451 Research. April 2, 2020. https://go.451research.com/2020-mi-covid-19-will-work-form-home-revolutionize-enterprise-security-architecture.html.

[3] Poll taken during a HIMSS Gigamon webinar. April 22, 2020.

[4] "2020 Cyberthreat Defense Report." CyberEdge Group. March 2020. https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf.

About Gigamon

Gigamon provides network visibility and analytics on all traffic across your physical, virtual and cloud networks to solve critical security, performance and business continuity needs. The Gigamon Visibility and Analytics Fabric delivers optimized network and security performance, simplified management and accelerated troubleshooting while increasing your tools' return on investment. Gigamon's comprehensive solutions accelerate your organizations' ability to detect and response to security threats including those hidden in encrypted traffic. Trusted by 83% of the Fortune 100 and 4,000 organizations worldwide, Gigamon ensures that your business can run fast and stay secure in The New Tomorrow.

Gigamon®

Worldwide Headquarters
3300 Olcott Street, Santa Clara, CA 95054 USA
+1 (408) 831-4000 | www.gigamon.com

05.20_01