WHITE PAPER

Secure and Consistent Connectivity Is Essential for Dynamic Healthcare Environments

Executive Summary

One unexpected result of the global COVID-19 pandemic is that it has sped up the digital transformation of the healthcare industry and boosted innovation in how patients are able to receive and consume care.[1] Distancing restrictions have caused nonessential care to be replaced by telehealth and remote patient-monitoring solutions, all of which rely on a variety of technologies and the transmission of critical data to physicians or labs to function.

Telemedicine and virtual visits have enhanced patient access to medical providers globally, allowing providers to care for patients across a borderless ecosystem that may have had a difficult time accessing medical care. In addition, digital technology enables providers in different locales, even across different organizations, to coordinate care more seamlessly. But such breakthroughs in patient care also bring greater complexity, security fragmentation, and risk to hospital networks.

For example, to address escalating COVID-19 cases while maintaining essential emergency room (ER) services, many hospitals have opened freestanding or temporary or tent ERs to test COVID-19 patients and perform vaccine administration separately from the regular hospital population. Each of these independent sites needs to have the same rapid, secure, reliable connectivity and collaboration solutions as the hospital base. Patient information needs to be recorded, insurance information needs to be verified, online medical records need to be accessed, lab and vaccine records need to be shared with other physicians, care protocols need to be posted and checked, vital signs need to be monitored, and friends and family need status updates.

The availability of new digital technologies such as software-defined wide-area networking (SD-WAN) enable hospitals and clinics to quickly set up pop-up satellite care centers and have immediate access to critical resources. But while this technology may provide information needed to solve urgent medical challenges and improve patient outcomes, they also make distributed healthcare networks much more complex—and therefore, more vulnerable to attack.

Connectivity is a critical issue. Healthcare IT teams may have to manage hundreds of connections from remote clinics, offices, worker home networks, and patients at the same time. And if one of these goes down even once a year, that would result in several locations being off-network every day. And physicians, for the health and safety of their patients, just cannot tolerate any downtime or slowness.

Worse, while things like SD-WAN can be quickly spun up, providing adequate security to protect data and ensure privacy are a different story. Many traditional SD-WAN solutions do not include a security component. Instead, IT teams are forced to design and implement a security overlay solution that can take time and resources to set up, and cannot easily adapt to shifting network systems that modify connections to maintain a consistent user experience. This can significantly delay the ability of a hospital to deploy an emergency satellite clinic.

Problems With Rapid Telehealth Adoption

Securing the Sprawl

While digital technology is transforming every industry, the trend is perhaps most noticeable in the healthcare industry. New Internet-of-Medical-Things (IoMT) devices and new patient care applications are being developed and deployed to help address telehealth communications challenges and speed response times. They give medical teams untethered access to real-time data, such as care plans and electronic medical records, to provide the best possible patient experiences. And hospitals, labs, clinics, pop-up sites, patients, and doctors need to be able to communicate seamlessly and respond to urgent situations securely from wherever they are, on the device of their choice.

This has caused an explosion of new endpoints—all of which need to be reliable, resilient, interconnected, and secure. In fact, the number of medical apps downloaded during the COVID-19 pandemic was up 30% in the United States in 2020, and a staggering 134% in South Korea.[2] And by 2022, the number of nurses and clinicians using mobile devices is expected to top 90%, according to *The Future of Healthcare: 2022 Hospital Vision Study* conducted by Zebra Technologies.

Unhealthy Risks

Although there are many benefits to the new telehealth model, IoMT, dispersed locations such as ER pop-ups and overworked, vulnerable healthcare workers greatly expand the attack surface. Today's healthcare networks are seeing unprecedented risk exposures. Outdated IT systems, such as static multiprotocol label switching (MPLS) connections, combined with inadequate cybersecurity protocols and not enough IT staff, all contribute to putting sensitive data at risk. As a result, as of January 2021, ransomware was responsible for 46% of healthcare data breaches, according to analysis by cybersecurity researchers at Tenable.[3]

Healthcare facilities have become an increasingly popular target for attacks over the past year.[4] That's because cyber adversaries know that downtime or other disruptions threaten human lives, impact revenue, and can damage a healthcare organization's reputation. These cyber criminals leverage this knowledge to extract ransoms from desperate organizations. In addition, sensitive medical and financial data is a valuable commodity, demanding a high price on the dark web. In fact, the first confirmed case of a patient dying due to delays in receiving emergency care due to medical equipment being infected by ransomware occurred in 2020.[5]

Hackers and attackers are proficient at exploiting crises, and known vulnerabilities in healthcare networks, such as hastily constructed and deployed pop-up ERs and clinics, are an open invitation. The pandemic is no exception. Numerous phishing scams related to COVID-19, some offering basic information about the pandemic, or promoting questionable products and services, popped up within days of the public announcement. Many of these scam emails pretended to come from places like the World Health Organization or the Centers for Disease Control. Hackers have also been impersonating Zoom, Microsoft Teams, and Google Meet for phishing scams to betray personal trust and steal personal information.[6]

In addition to the expanded attack surface, many healthcare industry organizations must continue to comply with highly regulated national statutes. In the U.S., this includes the Health Insurance Portability and Accountability Act (HIPAA), which requires institutions to secure protected health information (PHI)—placing a considerable amount of responsibility on healthcare organizations to securely manage private patient medical information.

The Ideal Security Model for the Healthcare Industry

Secure SD-WAN

To address the compounding factor of expanding network attack surfaces and corresponding increased threat volume, healthcare enterprises need to simplify and secure their vastly distributed network infrastructures. In particular, connections to off-premises locations such as doctors' offices, clinics, and pop-ups must operate and cooperate with minimal latency, maximum visibility, and absolute security.

SD-WAN leverages the corporate WAN as well as multi-cloud connectivity to deliver high-speed application performance at the WAN edge. One of the primary benefits of SD-WAN for healthcare organizations is that it provides dynamic path selection among connectivity options—MPLS, 4G/5G, or broadband—so hospitals, clinics, and doctors always have an optimized route to telemedicine and other cloud applications.

Telehealth will see a compound annual growth rate of nearly 40% between now and 2025. As artificial intelligence (AI) and robotics technologies come into play, reliable, high-speed connections will become increasingly important.[7]

Research shows increased provider reliance on telehealth since the COVID-19 pandemic presents a new slate of risks to patient data.[8]

According to public sources, 10% of all organizations hit by targeted ransomware between January and September 2020 were hospitals and other medical institutions.[9]

But connectivity is only half of the story. Security and compliance are equally important. The challenge is that the traditional overlay security solutions provided by most SD-WAN technologies simply cannot adapt to the dynamic connectivity environments that most healthcare environments rely on. Instead, security needs to be embedded into each SD-WAN device, enabling remote doctors, dispersed locations, and the data center to adhere to a common set of security policies and enforcement criteria. Unlike traditional SD-WAN solutions, a Secure SD-WAN solution integrates networking and security capabilities together, providing connectivity and seamless protection across the WAN edge, access layer, and endpoints.

	SD-WAN
Complexity	If security is not automatically built-in, teams need add-on options
Visibility	Broad application visibility
Cost	Consolidated services greatly reduce TCO
Performance & Availability	Enables MPLS, broadband, LTE for high speed
Scalability	Expand to add secure connectivity with full mesh

Secure SD-WAN builds security directly into the connection with fully integrated enterprise-grade firewalls and virtual private network (VPN) functions (as well as additional security functions, such as encryption, intrusion prevention system, antivirus, web security and filtering, and sandboxing). It also offers intuitive, zero-touch deployments, saving precious healthcare IT resources. And centralized VPN orchestration automates dynamic connectivity across the most complex network with intuitive workflows, the prioritization of critical applications, and self-healing WAN connections.

A clinic-in-a-box Secure SD-WAN solution comprises next-generation firewalls (NGFWs), secure wired and wireless access, cloud on-ramping, accelerated application access, and robust connectivity, along with centralized management and comprehensive analytics and reporting. This also enables healthcare IT security teams to consolidate essential functions into a unified solution to help troubleshoot problems and respond more rapidly to cyber incidents.

Conclusion

A Secure SD-WAN solution provides advanced visibility, flexible connectivity, enterprise-grade security, and advanced protection for today's rapidly expanding and evolving healthcare networks. Implementing a Secure SD-WAN solution is imperative for healthcare networks looking to establish fast, scalable, and flexible connectivity across all network environments. It enables the rapid implementation of an ideal healthcare security solution—one that is safe, resilient, reliable, and responsive, just like the practitioners who need them.

[1] Christopher Jason, "How COVID-19 Accelerated the Digital Transformation of Healthcare," EHR Intelligence, September 22, 2020.

[2] Conor Stewart, "Growth in the number of medical apps downloaded during the COVID-19 pandemic by country in 2020," Statista, October 22, 2020.]

[3] Danny Palmer, "Ransomware attacks now to blame for half of healthcare data breaches," ZDNet, January 15, 2021.

[4] Scott Ikeda, "Wave of Cyber Attacks Hits US Healthcare System as FBI Warns of Coordinated Criminal Campaign," CPO Magazine, November 10, 2020.

[5] Patrick Howell O'Neill, "A patient has died after ransomware hackers hit a German hospital," MIT Technology Review, September 18, 2020.

[6] Tom Kelly, "How hackers are using COVID-19 to find new phishing victims," Security Magazine, June 23, 2020.

[7] Nirav Shah, "SD-WAN: More Than A Retail Solution," Network World, July 15, 2020.

[8] Kat Jercich, "Telehealth is biggest threat to healthcare cybersecurity, says report," Healthcare IT News, September 10, 2020.

[9] Jonathan Langer, "Looking ahead to 2021– Healthcare security predictions for the upcoming year," Security Magazine, January 22, 2021.

FORTINET®

www.fortinet.com

March 15, 2021 11:12 PM

D:\Fortinet\2021 Rebranded templates\White paper\March\Healthcare SD-WAN\wp-secure-and-consistent-connectivity-is-essential-V1-3132021\wp-secure-and-consistent-connectivity-is-essential-V1-3132021

924413-0-0-EN