Versa SD-WAN: Intensive Care for the Enterprise WAN

The impact of network downtime or service disruption, for most businesses, can result in significant financial or business losses - for the healthcare industry, it could actually jeopardize patient well-being and safety. With so much at stake, the healthcare industry has very little tolerance for failure.

Healthcare is arguably one of the world's most information technology-intensive sectors, and the opportunities to leverage cutting-edge technology to improve service quality, encourage affordability and enhance the patient experience is vast. Also, being one of the more highly regulated industries, technology has always been a critical business enabler for healthcare providers to meet security and compliance standards.

Healthcare providers across the globe are using disruptive technologies like cloud, IoT and Internet-connected medical devices to create an IT infrastructure that meets the need for flexible and round -the-clock healthcare services; all with the added advantage of keeping costs low (See Fig 1.). However, the move to a more digitalized, automated approach also highlights the bottlenecks created by traditional WAN and networking technologies. This whitepaper provides insights into some of the most pressing challenges faced by the healthcare industry, and how Versa Network Secure Cloud IP Platform addresses some of those challenges.

How Healthcare Providers are Using Digital Technologies

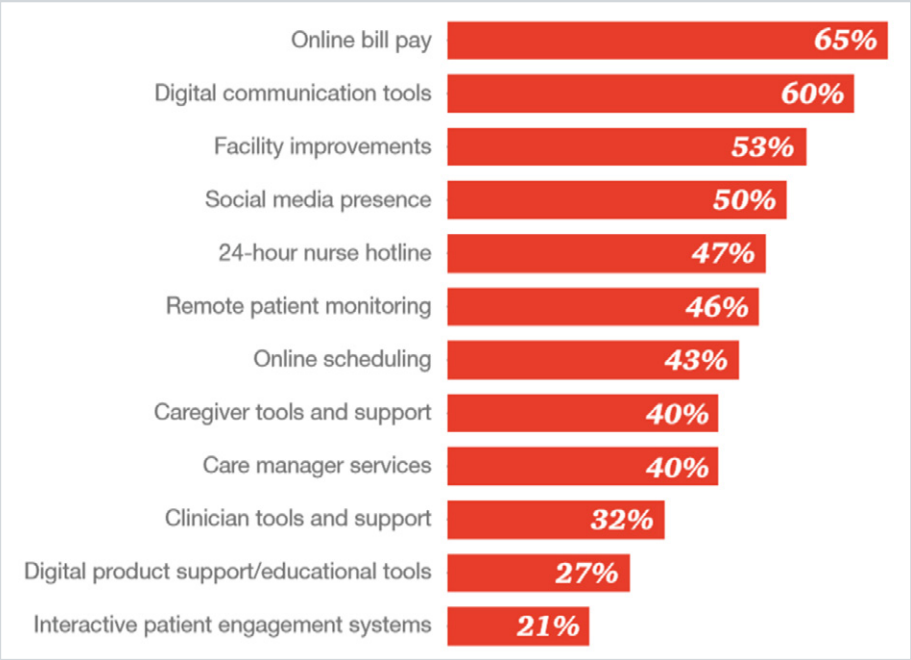

Fig 1. Source: PwC Health Research Institute Provider Executive Survey, 2017

Challenges in Healthcare

The rapid and wide-scale digitalization of distributed networks has resulted in a negative effect on the performance of traditional WANs. The traditional static WAN infrastructure was not designed for the dynamic, shifting workloads and resources that today's digital environments demand.

Most IT teams struggle with challenges, like inconsistent application performance, decreased efficiency, loss of productivity and the disruption of critical services. These deficits can lead to serious negative impacts to a healthcare provider's reputation and client satisfaction. Additionally, conventional WANs have evolved over the years as a convolution of standalone solutions creating an extremely complex network environment. As more devices and applications are brought into the mix, IT teams use more single-point solutions that make securing and managing interconnected devices a herculean task.

On one hand, digitalization, cloud and IoT can vastly improve the services that healthcare providers extend to their clients. While on the back-end, IT teams need an integrated solution for the following challenges:

Cloud Connectivity

Cloud solutions promise better service levels as compared to internal IT organizations - at a fraction of the cost and complexity. Cloud-based HMS (Hospital Management Solutions), collaboration and productivity apps provide healthcare via a flexible, cost-effective and agile model, for connecting hospital networks at remote locations or overseas. Healthcare providers also tend to have smaller IT teams or limited access to skilled IT resources in satellite locations. As a result, many healthcare providers have migrated to the cloud in the hopes of access to better IT services, without having to maintain an internal team of technical resources.

Traditional WANs were not built to handle today's cloud-intensive workloads. For security concerns, traditional network traffic has to traverse back and forth between branch offices and corporate data centers , to go to SaaS, PaaS or IaaS solutions. This adds latency and packet loss, slowing applications and making them unreliable, while increasing the overall volume of traffic and bandwidth consumption. Traditional WANs are expensive to maintain and static in how they treat network traffic. They also take a long time to deploy or modify, making them less than ideal for a today's cloud-driven healthcare industry, where time is of critical importance.

Data Explosion

Another practical challenge is the sheer volume of data that healthcare organizations generate every day. Medical records, patient health data, billing, MRI images and more, can lead to extensive amounts of data traveling through the provider network, skyrocketing the demand for expensive and dedicated MPLS bandwidth. Healthcare providers can benefit immensely from the flexibility and ease-of-access that lower-cost broadband can provide. However, healthcare providers also need a way to deploy secure, reliable and stable connectivity to address the public Internet's inherent problems of high latency, packet-loss, and security.

Internet of Things

Healthcare is among the few industries where Internet-connected devices were already in use before the concept got a new name (IoT). Internet-connected medical devices are holding the health system together—playing critical roles in such tasks as patient care, medical records, imaging and billing. The challenge is in securing these interconnected devices over the WAN across geographically distributed locations. Each of these devices could serve as a potential attack vector for cybercriminals, and the sheer number of devices at various locations makes securing them challenging to achieve. (See Fig 2.)

Device Vulnerabilities are being Reporated at a Record Rate

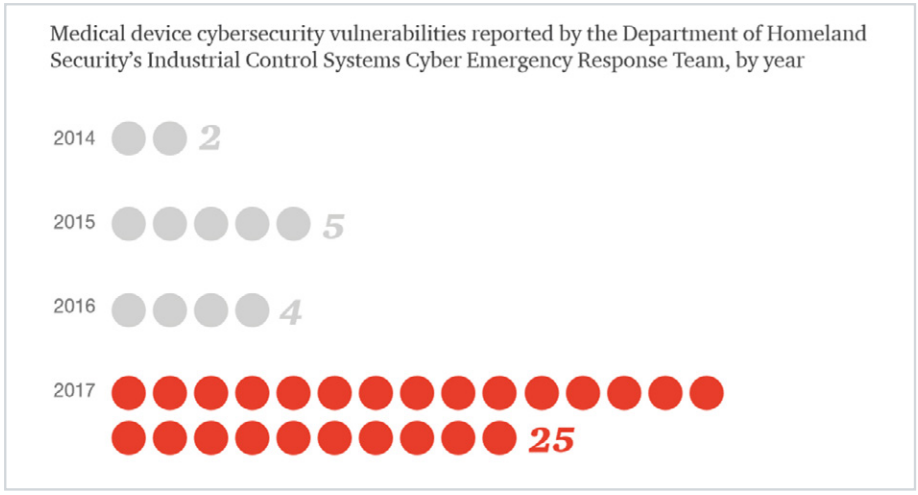

Figure 2. Source: PwC Health Research Institute analysis of Department of Homeland Security ICS-CERT security publications.

Telemedicine, mHealth and Mobile Kiosks

A number of developing and under-developed nations, where access to superlative healthcare is still inadequate, are experimenting with telemedicine, remote analytics through mobile phone apps, Internet kiosks, video conferencing, and teleophthalmology software to diagnose patients remotely and deliver quality healthcare. The caveat here lies in the fact that these mobile healthcare units, by default, have to resort to the Internet to connect to the corporate datacenter. The need for secure, reliable Internet connectivity is indispensable in these cases.

Eliminating Network Blind Spots Resulting from Mergers and Acquisition

Many hospital chains grow through mergers, acquisitions, and affiliations. The ability to bring a new entity onboard quickly is critical to the business. Traditional MPLS circuits can take months to deploy. The practice of sending truck rolls of equipment and resources to set-up infrastructure at individual locations every time the business acquires or merges with a new entity is expensive and time-consuming.

Data Security: The Million Dollar Question

A 2018 PwC report highlights that hospitals have become a favorite haunt for cybercriminals, due to the sensitive nature of the client information held by medical facilities. In 2017, at least two U.S. hospital systems experienced problems after being hit by WannaCry, and sixteen hospitals in the U.K. were unable to access their Internet-connected devices.

Back in 2016, the PwC's Global State of Information Security Survey (GSISS) found that hospitals have thousands of medical devices connected to their networks, yet some don't even know how many devices they have, nor their level of security. The survey found that just 64 percent of providers and payers said they have performed a risk assessment of connected devices and technologies to find potential security vulnerabilities, and only 55 percent of those said they have put security controls in place for these devices.

For an extremely regulated industry where any breach can lead to compliance issues, security has emerged as one of the biggest points of concern. A compromised medical-device within the network can rapidly infect other devices, rendering them inoperable. This heightens the chance for critical records being stolen or inaccessible, and even facilities being shut down as a precaution. The reputational cost of a breach affecting client health and privacy can eclipse the lost revenue from business disruption.

Digital transformations have led to broadening of the enterprise attack surface. Factors like the cloud, geographical expansion, growing numbers of connected devices and applications, and an increased dependency on public Internet to connect medical facilities to cloud and customers alike are making healthcare low-hanging fruit for cybercriminals.

To mitigate these risks, organizations often deploy separate add-on security controls, like enhanced security suites or a next-generation firewall. However, this leaves room for security gaps as well as performance bottlenecks. This is because traditional perimeter defences are less effective in distributed environments, as the perimeter becomes wider, more complex and more difficult to monitor and manage. Effective security controls must be able to adapt to a flexible network infrastructure, as well as to the numerous devices supporting it.

Enterprises with an integrated approach to network security stand a better chance of prevention, detection and blocking of a security attack. An integrated security solution eliminates the need for add-on products and problems arising from integration and interoperability. A well-integrated solution will eliminate potential gaps between the disparate technologies and managing and operating multiple stack solutions.

Versa SD-WAN: The Healing Touch for Your Networks

Modern networks that power the underlying infrastructure for digital, cloud-first enterprises need to be intelligent and built to deliver uninterrupted, secure connectivity to cloud applications. Superior application performance, reducing deployment times and minimizing the cost and complexity of running the networks are some of the features that healthcare providers should aim to incorporate when building a future-ready WAN.

Versa's SD-WAN leverages a unique cloud-native, multi-tenant, multi-service software solution for a software-defined network that enables network teams to remove barriers that legacy WAN and branch architectures have increasingly placed on IT. Versa SD-WAN enables IT to rapidly provision new branch offices, dynamically add new network and security functions, and seamlessly scale capacity as required.

Versa's FlexVNF™ brings the following capabilities to healthcare WANs:

Unmatched Application Performance

Applications are the life-line for the healthcare industry, and thousands of lives depend upon these applications for their well-being. Poor application performance that impacts business operations or network uptime can prove disastrous for both the business and client alike.

Be it online or offline, mobile or cloud-based - Versa FlexVNF optimizes the existing bandwidth resources and enhances performance for critical applications. Through an intelligent combination of priority-based traffic routing, balancing between multiple links for data transmission and application connectivity, and outcome-based networking, Versa SD-WAN carefully maps different applications across MPLS and Internet/broadband, based on business policies and app-specific SLAs. It dynamically routes traffic across the best connection, based on real-time availability and performance, or other custom-defined policies. This enables high-bandwidth availability, interactive rich-media and enhances application performance to deliver a quality user experience.

Seamless UCaaS Experience

Telemedicine, mhealth or mobile health kiosks depend heavily on the public Internet to connect to the corporate networks. However, the public Internet is notorious for being unreliable for enterprise connectivity, and is susceptible to problems like packet loss, security, jitter and network latency. The problem compounds when the Internet is used for media-rich applications like video conferencing or VoIP. When patients are being diagnosed (or in some cases even medical surgeries aided) via video conferencing or video calls, a seamless and reliable video/voice experience is a factor that must not be compromised.

Integrated Security and Compliance

Versa's FlexVNF software-defined security solution that is closely integrated with the SD-WAN suite. It offers a broad set of software-based security functions, including stateful and next-generation firewalls, malware protection, URL and content filtering, IPS and anti-virus, DDoS and VPN/next-generation VPN. Versa's FlexVNF is also ICSA Labs certified for the firewall.

Versa's SD-WAN consolidates all enterprise connectivity circuits (e.g. broadband, LTE, MPLS, etc.) into a single virtualized network. This makes it easier for security enforcement teams to monitor and manage the entire application suite and network landscape through a single management pane. IT teams can dynamically apply role-based access and enforce security policies and configurations per application, and manage security configurations around its applications and networks through one centrally managed console.

Reduced Cost and Complexity

FlexVNF integrates low-cost Internet and broadband alongside MPLS to reduce the cost associated with increasing bandwidth demand. Healthcare providers can now rely on secure Internet connectivity to cloud-based applications, and switch over to the more reliable MPLS for mission-critical traffic.

By automating and software-defining the WAN, Versa SD-WAN also helps healthcare providers cut down on the cost of resources (hardware and human) required to manage and run the networks. All these factors significantly bring down the Capex and Opex. A cloud-based subscription model means enterprises can avoid capital expenditures and shift capacity demands with ease. A centralized software-defined approach to network management also gives IT staff greater visibility and control over the corporate network, with lower administrative costs

More Flexibility for the Cloud

SD-WAN lets IT teams proactively set-up application transport policies and network routes to cope with traffic spikes, instead of having to upgrade circuits and bandwidth. By leveraging low-cost broadband and making it more secure and enterprise-ready, Versa SD-WAN helps healthcare providers prepare for the possibility of natural disaster/pandemic events, or emergencies that can lead to increased demand for healthcare services.

Support for Business Growth

Whether the healthcare provider decides to expand to new geographical locations by opening new branch offices, or through acquisitions/mergers - IT's role is critical in quickly bringing a new location on board. SD-WAN's centralized administration and console makes it easy to turn up new services, new locations and adjust policies remotely for immediate results, without having to worry about the cost, resources, and logistics associated with setting up a new IT infrastructure at a new location.

Improving Healthcare Through Healthier Networks

While most industries strive for profits and growth rates, the healthcare industry's success is defined by how it serves the public and sustains their well-being and safety. SD-WAN enables healthcare IT leaders to create a more robust, reliable, and trusted network infrastructure to operate efficiently and safely, and to service both clients and medical staff well. By creating the perfect balance between security, manageability, operational efficiency, and performance, IT leaders can help their organizations create and deliver affordable, world-class healthcare.

To learn more about Versa's SD-WAN solutions, contact us at info@versa-networks.com or request a demo.

VERSA NETWORKS

Versa Networks, Inc, 6001 America Center Dr, 4th floor, Suite 400, San Jose, CA 95002 | Tel: +1 408.385.7660 | Email: info@versa-networks.com | www.versa-networks.com