SOLUTION BRIEF

Secure Telehealth With Fortinet SD-WAN

Executive Summary

Adoption of new digital technologies is driving rapid evolution in healthcare. While digitization provides tools and capabilities to help solve urgent medical challenges and improve patient outcomes, they also make distributed healthcare networks much more complex—and therefore more vulnerable to attack. When considering additional factors such as increasing dependence on remote access for telemedicine, frequent mergers and acquisitions in the industry, and rigorous regulatory requirements, today's healthcare networks are seeing unprecedented risk exposures.

A secure software-defined wide-area networking (SD-WAN) solution addresses these issues by integrating networking and security capabilities across the WAN edge, access layer, and endpoints. In this way, Fortinet Secure SD-WAN and SD-Branch solutions are able to provide advanced visibility, security, and protection for today's rapidly expanding and evolving healthcare networks.

As many hospitals and healthcare businesses embrace remote work arrangements for the first time, securing remote networks and endpoints has become a primary focus for IT teams.[1]

Simplify and Secure Network Infrastructures

Shifting market forces and more complex government policies are driving mergers, acquisitions, and partnerships between healthcare organizations. The resulting convergence of technologies only further complicates network infrastructures already inundated by Medical Internet of Things (MIoT) and the need to support the rapid adoption of telehealth. The result is an expanded attack surface due to an increasing number of tele-users—whether nonclinical revenue cycle or administrative staff, medical personnel, or patients—accessing network resources, and the proliferation of connected devices, whether end-user devices or connected medical solutions, many of which were never designed with security in mind. As a result, organizations must address myriad subsequent problems related to infrastructure management, visibility, control, and operational efficiency.

To address the compounding issues of an expanding network attack surface and increasing threat volume, healthcare enterprises need to simplify and secure their increasingly distributed network infrastructures. Connections with distributed locations such as doctors' offices, clinics, vendors, temporary clinics, and standalone ERs to address COVID-related issues must operate with minimal latency. Special care must also be taken so adversaries cannot penetrate a less secure remote site and then move laterally across the organization.

In light of these pressing needs, SD-WAN solutions stand to play a critical role in today's distributed healthcare networks. SD-WAN technology allows network traffic to move over more affordable public internet connections—as opposed to the traditional WAN's expensive multiprotocol label switching (MPLS) links. This can, for example, ensure high-bandwidth connectivity for real-time video and diagnostics information to pass between patients and providers. This not only helps extend quality healthcare to remote locations but it also ensures that patients can receive care without exposure to undue health risks. And the efficiencies provided by SD-WAN also help ensure that these services can be provided without the usual skyrocketing costs.

But the majority of SD-WAN solutions available on the market today are limited to providing simple networking and connectivity capabilities. They lack sufficient security to protect the affordable public internet connections that SD-WAN solutions often use, leaving the challenge—and expense—of building a separate security overlay to their customers.

Fortinet Advanced Networking and Security for Telehealth

Because SD-WAN is a built-in capability of the FortiGate next-generation firewall (NGFW), Fortinet Secure SD-WAN and Fortinet SD-Branch natively combine robust SD-WAN networking and enterprise-class security into a unified solution. This model enables the rapid expansion of healthcare networks by allowing them to scale their operations with high performance while ensuring that data, applications, and resources are protected from the onset.

The Fortinet integrated security fabric approach also supports local-area network (LAN) edge consolidation and integration with wireless access points (APs), switches, and endpoint security to extend security from the connection point to deep inside the local branch LAN. In addition to simplifying infrastructure, Fortinet SD-Branch provides efficient protection and consistent policy enforcement across all clinical locations by enabling such things as access control, MIoT security, and traffic inspection. And all of this is managed and orchestrated through a single-pane-of-glass management system.

Fortinet SD-WAN solutions are helping to revolutionize the capabilities of healthcare organizations by transforming the corporate WAN while leveraging multi-cloud connectivity to deliver high-speed application performance at the WAN edge or branch, including sites such as clinics, satellite hospitals, labs, urgent care centers, standalone emergency centers, and long-term care centers.

Critical use cases include:

1. Providing multi-cloud connectivity support and integration to accelerate cloud adoption within healthcare
2. Increasing resiliency, thereby ensuring high availability of critical patient care locations by providing and maintaining secure multi-WAN connections
3. Reducing the total cost of ownership (TCO) of WAN connections while supporting things like large data flows due to the high-bandwidth applications and information provided from such groups as cardiology and radiology

SD-WAN solves several challenges at the same time, including rapid deployment, fast connectivity to cloud applications and resources, and unified management to reduce IT overhead. It also enables organizations to add more bandwidth inexpensively, while providing users with direct and high-quality access to internet-based resources.[3]

Self-healing Capabilities and Resiliency

As healthcare enterprises adopt SD-WAN and SD-Branch, they need them to include the right tools to seamlessly deploy and manage them across their widely distributed infrastructures. The new Secure SD-WAN technologies provided in FortiOS 7.0 now provide things like self-healing capabilities by using adaptive WAN remediations, making the application experience much more resilient. Fortinet has also expanded passive application monitoring for Software-as-a-Service (SaaS) and multi-cloud applications for a better user experience for users working from anywhere.[2]

Fortinet's solutions can be administered through FortiManager, a single intuitive and unified management console. It includes options for a cloud-based or hosted solution for remote control and orchestration across thousands of locations. With FortiManager in place, FortiGate devices are truly plug and play. Centralized policies and device information can be configured and devices are automatically updated to the latest policy configuration.

Total Cost of Ownership

Fortinet's approach reduces both capital expenses (CapEx) and operating expenses (OpEx) for healthcare organizations by consolidating security and networking infrastructure into a simplified and secure all-in-one solution. Fortinet SD-Branch goes further by integrating firewalls, switches, and APs into a single, consolidated FortiGate solution. This simplified architecture approach reduces the need for on-site IT resources, which in turn lowers operating costs.

The Healthy Security Solution

As healthcare networks increasingly depend on digital innovation to provide telehealth services to patients under all conditions, from anywhere to anywhere, cybersecurity issues will grow in lockstep. And one consequence the pandemic has made clear is that remote locations need their own defenses that conform to the unique risks they present.

As natural extensions of the integrated Fortinet Security Fabric architecture, Fortinet Secure SD-WAN and SD-Branch solutions provide a secure platform for today's increasingly distributed and complex healthcare organizations—providing visibility and protection across the entire network, and all the devices that connect to it.

[1] "The State of Healthcare Cybersecurity During Covid-19," CSO, November 10, 2020.

[2] John Maddison, "FortiOS 7.0: Consistent Security Across All Networks, Endpoints, and Clouds," Fortinet, February 4, 2021.

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

March 18, 2021 9:08 AM

D:\Fortinet\2021 Rebranded templates\Solution Briefs\March\SD-WAN for healthcare\sb-secure-telehealth-with-fortinet-sdwan-V2-3182021\sb-secure-telehealth-with-fortinet-sdwan-V2-3182021

926375-0-0-EN