SOLUTION BRIEF

Fortinet Secure SD-WAN for Healthcare

Enabling the Latest Advances in Patient Care While Protecting Against Cyberattacks

Executive Overview

Adoption of new digital technologies is driving the 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.

Remote Healthcare Services Pose an Expanding Risk

While digital technology is transforming every industry, the trend is perhaps more visible in the healthcare industry than in many others. Internet-of-Medical-Things (IoMT) devices are being developed and deployed to help prolong life, improve its quality, and make the relationship between the patient and care providers less transactional. They give medical teams untethered access to real-time device data as well as electronic medical records to provide the best care possible in any situation or environment.

One interesting outcome of the global COVID-19 pandemic is that it has largely sped up the digital transformation of healthcare and boosted innovation in how patients can receive and consume care.[1] Telemedicine and virtual visits have enhanced patient access to medical providers globally, allowing providers to care for patients across a borderless ecosystem. In addition, digital technology enables providers in different healthcare organizations to coordinate care more seamlessly. But such breakthroughs in quality of care also bring greater complexity, fragmentation, and risk to hospital networks.

At the same time, market forces and government policies are causing significant consolidation in the healthcare industry. And the resulting mergers, acquisitions, and partnerships between healthcare organizations further complicate network infrastructures. The result is a ballooning attack surface, an increasing number of third-party users accessing network resources, and the proliferation of connected devices—many of which were never designed with security in mind. As a result, organizations must now also deal with myriad subsequent problems related to infrastructure management, visibility, control, and operational efficiency.

And if that weren't enough, on top of greater exposure comes stricter accountability. The U.S. healthcare industry is highly regulated, with the Health Insurance Portability and Accountability Act (HIPAA) placing a high degree of responsibility on institutions with regard to managing patient medical information.

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.[2]

Research shows increased provider reliance on telehealth since the COVID-19 pandemic presents a new slate of risks to patient data.[3]

In combination with expanded risk exposure, healthcare facilities have become an increasingly popular target for attacks over the past year.[4] Cyber adversaries understand that downtime or other disruptions can threaten human lives, impact revenue, and damage an organization's brand reputation. Cyber criminals leverage this knowledge to extract ransoms from desperate organizations. Sensitive data (both medical and financial) is also a valuable target for exfiltration, demanding a high price on the dark web.

The Emergence of SD-WAN

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, and others must operate with minimal latency, and care should be taken that adversaries cannot penetrate a less secure remote site and then move laterally across the organization.

In light of these pressing needs in the healthcare industry, SD-WAN solutions stand to play a critical role. SD-WAN technology allows network traffic to move over more affordable public internet connections—as opposed to 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 skyrocketing costs.[7]

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

Fortinet Combines Advanced Networking and Security for Distributed Healthcare

Because SD-WAN is a built-in capability of FortiGate next-generation firewalls (NGFWs), **Fortinet Secure SD-WAN** and **Fortinet SD-Branch** natively combine robust SD-WAN networking and enterprise-class security in a unified solution. This approach enables fast-growing healthcare networks to scale their operations with high performance while ensuring that data, applications, and resources are protected right out of the box. The Fortinet integrated security fabric approach also supports local-area network (LAN) edge consolidation and integration with wireless access points, 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 branch outposts by enabling such things as access control, Internet-of-Things (IoT) security, and traffic inspection. And all of this is managed and orchestrated through a single-pane-of-glass management system.

Fortinet SD-WAN solutions can help revolutionize a healthcare organization's capabilities by transforming the corporate WAN while leveraging multi-cloud connectivity to deliver high-speed application performance at the WAN edge or branch, sites such as clinics, hospitals, service centers, urgent care centers, and long-term care centers. Critical use cases include:

- Providing multi-cloud connectivity support and integration to accelerate cloud adoption within healthcare

In November 2020, federal agencies warned of increasing ransomware attacks targeting the U.S. healthcare sector just as hospitals face a nationwide surge in COVID-19 cases.[5]

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.[6]

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.[8]

- Increasing resiliency, thereby ensuring high availability of critical patient care locations by providing and maintaining secure multi-WAN connections
- Reducing the total cost of ownership (TCO) of WAN connections while supporting things like large data flows from cardiology and radiology through high-bandwidth applications

Application Awareness and Automated Path Intelligence

Fortinet Secure SD-WAN and SD-Branch use "first-packet identification" to intelligently identify applications on the very first packet of data traffic. Such broad **application awareness** not only ensures rapid access to critical applications but also helps network teams see which applications are being used across the enterprise, enabling them to make well-informed decisions regarding SD-WAN policies. Fortinet Secure SD-WAN references an application control database of over 5,000 applications, a number that continues to grow as both the threat landscape and digital network evolve.

Being application-aware opens the doors to **automated path intelligence**—prioritizing routing across network bandwidth based on a specific application and user. Offering a per-application level service-level agreement (SLA), Fortinet's automated path intelligence dynamically selects the best available WAN link/connection for the situation.

FortiGate NGFWs that feature the industry's first, and only, application-specific integrated circuit (ASIC) designed to accelerate security, connectivity, and SD-WAN functionality—the SoC4—enable the fastest application steering in the industry, including unrivaled application identification performance. This includes deep secure sockets layer (SSL)/transport layer security (TLS) inspection with the lowest possible performance degradation. Related features include:

- **WAN path remediation** utilizes forward error correction (FEC) to overcome the most adverse WAN conditions. This delivers a better user experience for business-critical applications, such as voice and video services. FEC also discards duplicate packets and re-orders out-of-order packets at the receiving end to improve the quality of real-time applications.
- **Tunnel bandwidth aggregation** provides per-packet load balancing and delivery by combining two overlay tunnels to maximize network capacity should an application require greater bandwidth.
- **Automatic failover** capabilities change to the best available link when the primary WAN path degrades. This automation is built into FortiGate NGFWs, reducing complexity for end-users while improving user experience and productivity.

NGFW Security and Compliance

Fortinet provides healthcare organizations with enterprise-class security and branch networking capabilities in a single-box solution—the FortiGate NGFW. Critical security features of Fortinet Secure SD-WAN and SD-Branch solutions include:

- **SSL/TLS inspection and threat protection** to provide visibility and prevention against malware that obviates the need for separate encryption inspection appliances
- **Web filtering service** to enforce internet security and reduce complexity, eliminating the need for a separate Secure Web Gateway device
- **Complete threat protection** including sandboxing, anti-malware, and intrusion prevention systems (IPS)
- **Highly scalable overlay virtual private network (VPN) tunnels** with high throughput to ensure that traffic is always encrypted and remains confidential
- **Granular SLA analytics**, including application transactions for quick remediation

Fortinet's tracking and reporting support helps ensure adherence to privacy laws, security standards, and industry regulations while reducing the collateral risks of fines and legal costs in the event of a breach. These features track real-time threat activity, facilitate risk assessment, detect potential issues, and mitigate problems. They also monitor firewall policies and help automate compliance audits.

Simplified Management, Orchestration, and Overlay Control

As healthcare enterprises adopt SD-WAN and SD-Branch, they need the right tools to seamlessly deploy and manage them across widely distributed infrastructures. 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, FortiGate devices are true plug and play. Centralized policies and device information can be configured with FortiManager, and the FortiGate devices are automatically updated to the latest policy configuration.

FortiGate NGFWs, featuring the SoC4 ASIC, deliver the fastest SD-WAN security performance in the industry. This includes acceleration for responsive **overlay VPN** and a better overall WAN user experience across the enterprise. **Cloud overlay controller** orchestration, powered by FortiCare 360 Bundle subscription services, simplifies overlay VPN deployment with cloud-based automated provisioning. The flexibility of single-pane-of-glass management includes scalable remote security and network control via the cloud for all branches and locations.

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 integrates firewalls, switches, and access points (APs) into a single, consolidated FortiGate NGFW. This simplified architecture reduces the need for on-site IT resources, which in turn lowers operating costs.

The move to public broadband connections means that expensive MPLS links can be replaced with more cost-effective options. With Fortinet transport-agnostic solutions, enterprises can utilize the entire available bandwidth by using connections in active-active mode. And its single-pane-of-glass management interface optimizes staff efficiency while enabling proactive risk management. In the most recent NSS Labs for SD-WAN Group Test report, for example, Fortinet received the coveted "Recommended" rating while showcasing the lowest TCO per Mbps among all vendors, combined with providing zero-touch provisioning of new branches in under six minutes.[9] Zero-touch deployment reduces the burdens and overhead expenses associated with initial setup as well as with business growth over time.

A Perfect Fit for the Changing Shape of Modern Healthcare

As healthcare networks increasingly depend on digital innovations to provide anywhere/anytime services to patients under all conditions, cybersecurity issues will expand in lockstep. As the fallout of COVID-19 has shown, 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] Christopher Jason, "How COVID-19 Accelerated the Digital Transformation of Healthcare," EHRIntelligence, September 22, 2020.

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

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

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

[5] "Ransomware Activity Targeting the Healthcare and Public Health Sector," CISA, November 2, 2020.

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

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

[8] Ibid.

[9] "Fortinet Secure SD-WAN: Certifications," Fortinet, accessed December 2, 2020.

FORTINET

www.fortinet.com

December 9, 2020 8:22 AM

861056-0-0-EN

D:\Fortinet\Solution Brief\Red Solution Brief\Healthcare SD-WAN\sb-fortinet-secure-sdwan-for-healthcare-V2-1292020\sb-fortinet-secure-sdwan-for-healthcare-V2-1292020