

An IDC InfoBrief, Sponsored by Fortinet | June 2019



SD-WAN: Security-Driven Networking

Research by Lynne A. Dunbrack, Research Vice President, IDC Health Insights

Executive Summary

IT infrastructure modernization is well underway as healthcare organizations need to be more agile in their response to digital transformation initiatives. Legacy architectures simply cannot keep up with the pace of change associated with value-based health and rapidly evolving technical requirements. Constrained IT resources require solutions that improve operational efficiencies and optimize resources.

This IDC InfoBrief presents a case study that describes how a customer deployed Fortinet Secure SD-WAN to improve network and application performance while reducing total cost of ownership (TCO).

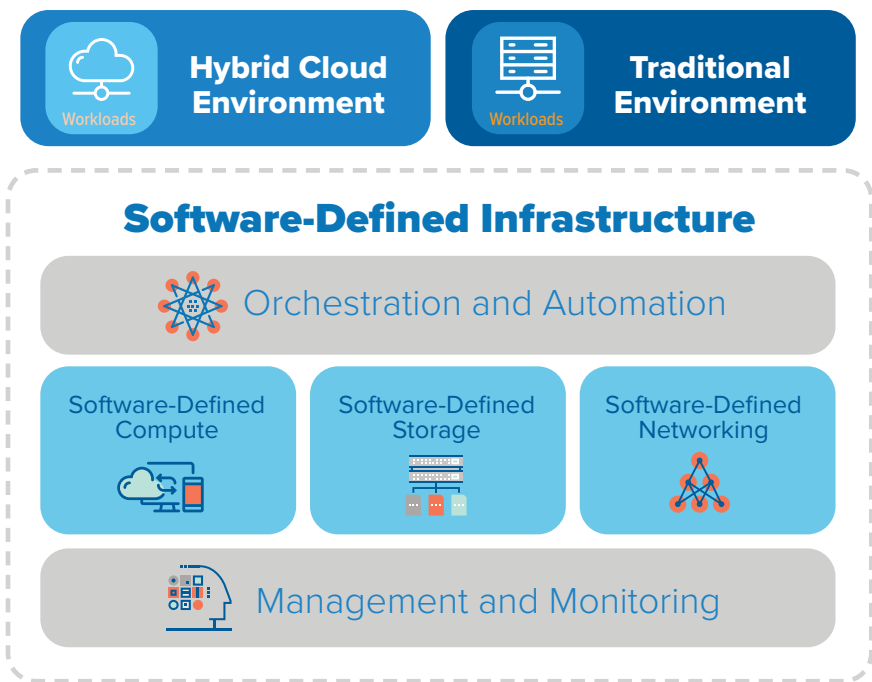
KEY FINDINGS

- » Security must be built into networking solutions from the ground up to improve both the healthcare organization's security posture and network performance.
- » Software-defined wide area networks (SD-WAN) with integrated security enable direct Internet access and the ability to move mission critical workloads to multiple cloud environments.
- » SD-WAN improves network performance, reliability, and resiliency. It also reduces WAN complexity and simplifies WAN management.



Healthcare Transformation Requires an Agile and Modern Infrastructure

The enterprise IT infrastructure market is undergoing a once-in-a-generation change due to ongoing digital transformation and the impact of cloud computing.



60% of **payers** and **65%** of **providers** in healthcare organizations are making investments to modernize the underlying IT infrastructure technology.



Demand is on the rise for technologies and architectures that can lower costs while improving levels of operational efficiency and security, which has driven strong growth for solutions such as software-defined compute, software-defined storage, and software-defined networking.

Why SD-WAN?

A major catalyst for deploying SD-WAN is security-driven networking and moving workloads to the cloud.



Security must converge and be built into the network from the ground up



Connections to multiple cloud environments across a distributed enterprise can optimize network performance for cloud applications



Eliminates the need to backhaul network traffic, which increases latency and results in a suboptimal user performance



Internet of medical things at the edge need to be connected and secured



SD-Branch simplification

50% of healthcare organizations currently have **workload portability capabilities** to run applications/workloads **in multiple cloud environments**.

IT Professionals Benefit from Deploying SD-WAN



Software-defined networking provides healthcare IT organizations **greater flexibility, operational efficiency, and integrated security.**



Historically, networking and security were separate functions with separate budgets to be managed. With security built in from the beginning, SD-WANs address the security challenges of multiple point solutions that lack a consistent approach to security. SD-WANs enable secure connectivity to the cloud, which in turn enables healthcare IT organizations to accelerate their digital transformation.

Healthcare Professionals Also Benefit from Deploying SD-WAN



**Increased access to data
improves care.**

Bandwidth optimization improves application performance, which enables faster access to critical patient health information stored in electronic health records (EHRs), imaging systems, and other clinical and financial systems. SD-WAN improves secure access to data across multiple hybrid cloud environments.

CASE STUDY



Solution Snapshot

Organization: Smile Brands Inc.

Operational challenge: Expensive WAN costs, poor performance of legacy circuits

Solution: Fortinet Secure SD-WAN

Benefits: Integrated security in Fortinet SD-WAN, direct Internet connections, improved network resiliency and speed, reduced total cost of ownership, simplified network and branch management

Lessons learned: A comprehensive logistics and communication plan is essential for a smooth deployment across hundreds of dental practice sites

Smile Brands Group Improves Security Posture and Application Performance at Scale – While Reducing TCO – with Fortinet Secure SD-WAN

“Standardized configurations, so that you can scale, make all the difference in the world.”

— Brett Stetzko, Senior Network Engineer, Smile Brands Group

Smile Brands Group provides dental practice management and IT infrastructure to more than 450 U.S. dental offices in 16 states. The company continues to grow through acquiring and opening new dental offices.

Business and technology drivers for seeking a new SD-WAN solution were interrelated. Smile Brands wanted to improve its network resiliency and performance to better support the dental practices and new clinical applications they deployed. By improving network performance, the practices can see more patients and offer new services that involve more imaging, thus increasing their revenues.

As Smile Brands evaluated SD-WAN options, the IT group discovered that most SD-WANs do not have built-in security. Network traffic from the practices would have to be backhauled to run through the main office’s firewalls for security policies to be applied. This practice came at a cost to network performance and ability to access the Internet directly.

Fortinet’s origin as a security vendor of next-generation firewalls that now offer SD-WAN and SD-Branch with integrated security were major factors in selecting Fortinet

over other companies. Another important consideration was Fortinet’s Security Fabric architecture, which enables Smile Brands security professionals to manage, monitor and have complete visibility into the distributed network across Smile Brands from a single pane of glass, simplifying network and branch management. Key benefits include reduced total cost of ownership because Fortinet Secure SD-WAN with integrated security obviates the need for additional security point solutions in the datacenter. Smile Brands estimates its cost savings to be significant. When compared to multiprotocol label switching (MPLS) networks, Smile Brands found Fortinet Secure SD-WAN will be approximately one-third the cost to deploy.

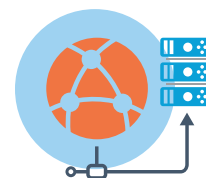
Best practices regarding rolling out technology to distributed dental practices apply to deploying Fortinet Secure SD-WAN. A comprehensive logistics and communication plan is essential. From a technology perspective, conducting pilot tests in a few offices helped the IT group identify key features needed up front and upon which to standardize. Smile Brands found that standardized configurations made it easier to scale the Fortinet Secure SD-WAN deployment. “Simple is better,” stated Brett Stetzko, senior network engineer.

Essential Guidance

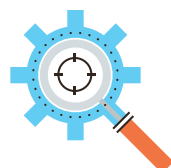
Consider the benefit of security engineering within SD-WAN enablement versus the need to acquire separate security point solutions.



Think carefully about a **long-term plan** for security **from a holistic perspective**.



Simplify branch management with deeper integration between SD-WAN and LAN to enable SD-Branch.



Identify the features you need, test thoroughly upfront, and **standardize configurations to scale deployments**.



Assure that your **security controls are integrating** with a larger visibility and intelligence platform.



Create a **comprehensive communications and logistic plan** for enterprise roll out.



Seek a strategic relationship with your security technology supplier.

A MESSAGE FROM OUR SPONSOR

About Fortinet: Fortinet is a worldwide provider of network security appliances and a market leader in Network Security (FW/NGFW/UTM). Our products and subscription services provide broad, integrated and high-performance protection against advanced threats while simplifying the IT security infrastructure. NASDAQ: FTNT

Learn more about Fortinet Healthcare Solutions at

<https://www.fortinet.com/solutions/industries/healthcare.html>

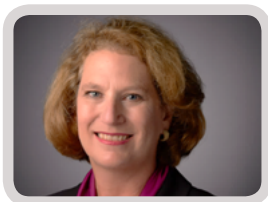
[Click here for more info on Fortinet Secure SD-WAN](#)

[Contact healthcare@fortinet.com](mailto:healthcare@fortinet.com) for a Cyber Security Threat Assessment.

[Follow us @FortinetHealth on Twitter](#)



IDC Analyst Profile



Lynne A. Dunbrack

Research Vice President, IDC Health Insights

Lynne Dunbrack is Research Vice President for IDC Health Insights responsible for the research operations for IDC Health Insights. She manages a team of analysts who provide research-based advisory and consulting services for payers, providers, accountable care organizations, IT service providers, and the IT suppliers that serve those markets. Lynne also leads the IDC Health Insights' Connected Health IT Strategies program. Specific areas of Lynne's in-depth coverage include mobile, constituency engagement, interoperability, health information exchange, privacy, and security. Technology coverage areas include clinical mobility (physician facing) and mobile health (consumer facing), health information exchange, end-to-end remote patient health monitoring for health, wellness and chronic conditions, Internet of Things (IoT), personal health records and member, patient, provider portals, kiosks, videoconferencing and online care, unified communications, aging in place, and social.

IDC Corporate USA

5 Speen Street
Framingham, MA 01701
USA
T: 508.872.8200
F: 508.935.4015
Twitter: @IDC
idc-insights-community.com
www.idc.com

IDC Custom Solutions

This publication was produced by IDC Custom Solutions. The opinion, analysis, and research results presented herein are drawn from more detailed research and analysis independently conducted and published by IDC, unless specific vendor sponsorship is noted. IDC Custom Solutions makes IDC content available in a wide range of formats for distribution by various companies. A license to distribute IDC content does not imply endorsement of or opinion about the licensee.

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.

Copyright 2019 IDC. Reproduction without written permission is completely forbidden.