WHITE PAPER

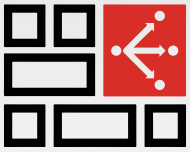
SD-WAN in the Age of Digital Transformation

Achieving Business Agility Without Complicating Network Security

Executive Summary

Most organizations are in the midst of some form of digital transformation (DX), transforming how they bring products and services to the market—and ultimately deliver value to their customers. But DX initiatives also bring complexity for the network operations team. With business-critical services distributed across multiple clouds, this leads to potential performance issues, especially at branch locations.

Given these realities, it is no wonder that software-defined wide-area network (SD-WAN) technology is rapidly going mainstream. Unfortunately, SD-WAN is an example of the paradox of DX: transformative technology can potentially move the business to the next level, but the expanded attack surface it creates can expose the organization to significant risk. That is why an SD-WAN deployment, like every other DX effort, should be accompanied by a security transformation (SX) that rethinks outdated principles, broadens protection beyond the data center, and integrates the security architecture for centralized visibility and control.



Digital transformation is driving more services to the cloud, which are clogging traditional network architectures and pushing organizations to embrace SD-WAN.

DX Sets the Agenda

DX is arguably the most important business trend involving IT in organizations today. It empowers businesses to operate with more agility and scale more quickly—which is absolutely essential in many industries.[1] Moving beyond the digital-enabled enterprise, DX creates fully digital enterprises that "are hyper-connected, adaptive, intelligent, and agile with technology highly integrated into new operational processes, policies, and organizations that unlock its transformative capabilities."[2]

DX looks a little different at each organization, but it is almost always marked by increasing reliance on hybrid cloud architecture. For the network operations team, this means bringing existing on-premises resources together with multiple external cloud networks and ensuring their availability and performance, no matter where a user is located.

SD-WAN Addresses DX Networking Needs

As more services move to the cloud, it becomes increasingly clear that "conventional network architectures … were not built to handle the workloads of a cloud-first organization."[3] This has resulted in the rapid growth of another key DX technology—SD-WAN. And rapid is the operative word: research conducted by IHS Markit shows that 74% of firms conducted SD-WAN trials in 2017, and many of those firms are deploying the technology this year.[4]

SD-WAN provides high-performance access to cloud applications for users located away from headquarters, enabling a more agile network and facilitating automation at branch locations to a degree previously not possible. Specific benefits include:

1. **Direct cloud access.** SD-WAN eliminates the need for backhauling—routing all cloud and branch office traffic through the data center. This enables direct access to critical cloud services for all users, regardless of location.

2. **Better application performance.** An SD-WAN can be configured to prioritize business-critical traffic and real-time services like Voice over Internet Protocol (VoIP) and steer it over the most efficient route. Having several options for moving traffic helps reduce packet loss from overloaded circuits and latency due to heavy traffic, improving performance and user experience.[5]

3. **Increased business agility.** Network planners no longer need to plan weeks or months in advance to deploy additional multiprotocol label switching (MPLS) bandwidth for a traditional WAN. In addition, the need to ensure network performance at multiple branch locations no longer inhibits other DX initiatives from moving forward quickly.

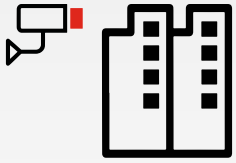
4. **Cost savings.** SD-WAN allows traffic to be routed efficiently over multiple channels—including not only existing MPLS circuits but also the public Internet via LTE and broadband.[6] This reduces the cost of new MPLS bandwidth.

SD-WAN Can Also Disrupt Network Security

It is hard to argue with the benefits of an SD-WAN network architecture in a world of DX. But SD-WAN also has a glaring disadvantage. Each SD-WAN-enabled site with local Internet access is a further expansion of an organization's attack surface—and another weak link in the network security chain. This exacerbates an existing problem, since branch locations often have lower levels of security than headquarters even before the introduction of SD-WAN.

Of course, most other DX-inspired technology deployments also expand an organization's attack surface, and security is often seen as the biggest roadblock to DX initiatives.[8] To be successful, every DX initiative—including SD-WAN deployment—must be accompanied by a corresponding SX.

74% of organizations conducted SD-WAN trials in 2017, and many of them are deploying solutions this year.[7]



SD-WAN necessitates a security transformation—a rethink of long-standing principles of enterprise security, including protection of the perimeter.

SX Can Make SD-WAN Secure

SX involves rethinking of long-standing principles of enterprise security—including the perimeter-based model, which declines in effectiveness every time another cloud service is rolled out and is completely unworkable with SD-WAN. SX also requires that security should be an integral part of DX planning, rather than an afterthought. For every DX initiative, planning and deployment teams should follow the principle of security by design, security by default.

When it comes to SD-WAN deployment, the network security and network operations functions should share in the decision-making process for a solution, and a security strategy should be in place when the final selection is made. Traditionally, these teams operate in silos—and sometimes function in mild competition with each other.[9] Butwhen these teams work together, they can strategically address the legitimate security concerns surrounding SD-WAN:

- Securing an expanded attack surface created by DX initiatives and the SD-WAN infrastructure itself[10]
- Ensuring that malware that does enter the network does not travel horizontally[11]
- Compensating for the lack of trained IT security staff at some remote locations
- Providing networkwide visibility and centralized security controls for the entire enterprise

Integration Is a Key to SX

In a recent survey, the typical organization saw 20 cyberattackrelated intrusions over a two-year period, with four of those resulting in breaches that caused damage—data loss, downtime, or a compliance event.[12] Part of the problem is that it takes more than six months (197 days) to even detect the typical attack, enabling attackers to move laterally within an organization.[13] The majority of these are advanced threats, designed to bypass conventional security measures. If not deployed strategically, SD-WAN and other DX initiatives can potentially worsen these threat problems.

As organizations deploy SD-WAN in support of DX, they need to ensure that SX is a part of the equation. With network traffic bypassing the data center, the network security architecture needs to broaden—but not by adding silos to the security architecture. With a truly secure SD-WAN solution, security is integrated with the network and expanded across a multisite, distributed enterprise environment. This enables centralized visibility and control, true automation of security processes, dynamic sharing of threat intelligence, and a more resilient network.

Making SD-WAN Successful with SX

SD-WAN offers organizations a great opportunity to deliver tangible value to their branch networks. Some of the things IT and security leaders need to remember include:

- SD-WAN is a critical DX linchpin for many organizations.
- The business value of SD-WAN is tangible, facilitating clouddelivery to branch offices, providing increased applicationperformance, enhancing business agility, and reducing cost.
- SD-WAN expands the attack surface and can be the weakest security link for many organizations.
- SX is required to make SD-WAN secure.
- Integration is pivotal when it comes to secure SD-WAN.

20 cyberattack intrusions affected the typical organizations over the past two years. With detection of the intrusion taking over six months, the traditional security paradigm crumbles—exposing organizations to data theft, ransomware, and operational outages.

[1] Michael Krigsman, "Digital transformation and the CIO: Everything you need to know today," ZDNet, May 25, 2018.

[2] Benson Chan, "Digital transformation reimagines everything," Strategy of Things, September 7, 2017.

[3] Kelly Ahuja, "A digital-first enterprise needs SD-WAN," Network World, June 7, 2018.

[4] Andy Patrizio, "Enterprises are moving to SD-WAN beyond pilot stages to development," Network World, May 7, 2018.

[5] Lee Doyle, "How does SD-WAN manage real-time network performance?" TechTarget SearchSDN, January 9, 2018.

[6] "Traditional WANs vs Next Gen SD-WAN," Infosecurity, December 12, 2017.

[7] Andy Patrizio, "Enterprises are moving to SD-WAN beyond pilot stages to development," Network World, May 7, 2018.

[8] "Security Implications of Digital Transformation Report," Fortinet, July 26, 2018.

[9] Erin O'Malley, "Driving the Convergence of Networking and Security," SecurityWeek, May 15, 2018.

[10] Steve Garson, "Warning: security vulnerabilities found in SD-WAN appliances," Network World, November 28, 2017.

[11] Lee Doyle, "What are the options for securing SD-WAN?" Network World, July 12, 2018.

[12] "Security Implications of Digital Transformation Report," Fortinet, July 26, 2018.

[13] "Advanced Threats in Financial Services and Retail: A Study of North America & EMEA," Ponemon Institute, May 28, 2015.

FORTINET

www.fortinet.com

April 6, 2021 3:19 AM

D:\Fortinet\2021RebrandedtemplatesMarketingorCommsRequest\March\BrandingRefresh\945079-SD-WANintheageofdigitaltransformation\wp-sdwan-age-of-digital-transformation-462021\wp-sdwan-in-the-age-of-digital-transformation-462021

253349-B-0-EN