FORTINET

WHITE PAPER

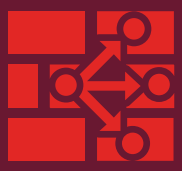
SD-WAN in the Age of Digital Innovation

Achieving Business Agility While Reducing Disruption

Executive Summary

Most organizations are in the midst of some form of digital innovation (DI) - leveraging technology to achieve specific goals—and ultimately deliver greater value to their customers. But DI also brings disruption. Disruption in the form of an expanded attack surface and the introduction of a more sophisticated threat landscape. Disruption can also lead to increased complexity as organizations try to counter these new threats with a range of new security solutions. Finally, maintaining compliance with relevant industy and regulatory standards such as the General Data Protection Regulation (GDPR) becomes even more of a challenge.

However, despite these issues, one key DI has rapidly going mainstream - software-defined wide-area network (SD-WAN). Unfortunately, SD-WAN is a prime example of the paradox of DI: a transformative technology that can potentially move the business to the next level, but the expanded attack surface it creates can expose the organization to significant risk. The challenge is how to take advantage of SD-WAN while offsetting the potential disruption than can come with it.



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

Digital Innovations in Parallel

Although it may not be thought of today as a digital innovation, moving workloads and infrastructure to any number of public clouds has had and continues to have a major impact on how organizations operate. The wide-scale acceptance of the use of public clouds allows businesses to operate with more agility and scale more quickly.

How public clouds are used looks a little different at each organization, but it is almost always marked by a hybrid cloud architecture. Since an application can be anywhere at any given point of time – on-premises or in the public cloud and can be moved between the two environments easily – the agility enabled by the use of public cloud can cause significant disruption for the network operations team in managing the wide area network.

SD-WAN Addresses DI Networking Disruption

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."[1] This has resulted in the rapid growth of another key DI 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.[2]

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.[3]
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 digital innovations 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. 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 digital innovations. 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 DI-inspired technology deployments also expand an organization's attack surface, and security is often seen as the biggest roadblock to these initiatives.[5] To be successful, every DI initiative—including SD-WAN deployment—must include a realistic assessment of the security implications of the initiative and how to counter it before the actual implementation.

74% of organizations conducted SD-WAN trials in 2017, and many of them are deploying solutions this year.[4]

SD-WAN necessitates a rethink of longstanding principles of enterprise security, including protection of the perimeter.

Making SD-WAN Secure

Securing digital innovations involves rethinking of longstanding 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. It also requires that security should be an integral part of the DI planning process, rather than an afterthought. For every digital 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.[6] But when these teams work together, they can strategically address the legitimate security concerns surrounding SD-WAN:

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

Integration Is a Key to SD-WAN Success

In a recent survey, the typical organization saw 20 cyber-attack related intrusions over a two-year period, with four of those resulting in breaches that caused damage—data loss, downtime, or a compliance event.[7] The majority of these are advanced threats, designed to bypass conventional security measures. If not deployed strategically, SD-WAN and other digital initiatives can potentially worsen these threat problems.

As organizations deploy SD-WAN, they need to ensure that security 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 multi-site, 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

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 linchpin for many organizations.
- The business value of SD-WAN is tangible, facilitating cloud delivery to branch offices, providing increased application performance, enhancing business agility, and reducing cost.
- SD-WAN expands the attack surface and can be the weakest security link for many organizations.
- Security must be a key focus of any SD-WAN deployment.
- Integration is pivotal when it comes to secure SD-WAN.

20 cyber-attack 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] Kelly Ahuja, "A Digital-first Enterprise Needs SD-WAN," Network World, June 7, 2018.

[2] Andy Patrizio, "Enterprises Are Moving to SD-WAN Beyond Pilot Stages to Development," NetworkWorld, May 7, 2018.

[3] Lee Doyle, "How Does SD-WAN Manage Real-time Network Performance?" TechTarget SearchSDN, January 9, 2018.

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

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

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

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

FORTINET

www.fortinet.com

March 26, 2020 3:41 PM

253349-B-1-EN

wp-FA-sd-wan-in-the-age-of-digital-transformation-A4