

Securing the transformation to the SD-WAN powered branch

 By [Doros Hadjizenonos](#)

13 Jun 2019

Traditional WAN infrastructures are struggling to keep up with the growth of SaaS applications providing critical business functions in enterprise branch offices - especially those that require reliable and high-performance connections, such as teleconferencing or voice.



Doros Hadjizenonos, Regional Director – SADC at Fortinet

Of course, the pressure to push these applications across the WAN isn't going to stop. Few organisations are willing to curtail business development due to bandwidth issues. According to one recent report, 60% of companies have already begun to adopt SaaS applications. And that adoption rate is projected to only increase, with the worldwide SaaS market expected to grow at over 21% per year through 2023. To meet this demand, organisations are having to rethink how they push data to their branch offices. MPLS connections, though fast, are too rigid for the meshed interconnectivity that digital transformation requires. Traffic backhauling across a traditional hub and spoke network simply can't handle the performance strain that cloud-based services introduce. And the problem is more than just bandwidth. Limited visibility and control across complex layers of meshed tunnels between branches and resources also introduces unacceptable levels of risk. **Replacing the WAN with SD-WAN** SD-WAN has emerged as a much better alternative to MPLS, providing things like intelligent load sharing of traffic across multiple broadband connections for greater network efficiency. However, most SD-WAN solutions still only address some of the requirements of today's digital branch office. An effective SD-WAN solution also needs to include:

- **Built-in security:** SD-WAN productivity is only valuable if its connections are secure. Which is why a recent Gartner survey revealed that 72% of respondents identified security as their top WAN concern. Unfortunately, most solutions on the market fall short because they require users to try and weave their existing security into their SD-WAN connections. To be truly effective from day one, SD-WAN needs to provide a full range of integrated security tools, such as NGFW, IPS, web filtering, antimalware, and antivirus, as well as high-performance SSL-encrypted traffic inspection and sandboxing.
- **Automatic application identification:** For proper controls to be put in place as quickly as possible, applications need to be immediately identified, ideally on the very first packet of data traffic. And it needs to be able to differentiate between thousands of known applications, as well as identify and classify new applications, even when are encrypted.
- **Extended visibility and control:** Individual employees need to be able to easily install cloud-based applications without involving IT management. And yet, the IT team needs to have full visibility and control of those applications the moment they are deployed. According to Gartner, while Shadow IT represents 30% to 40% of IT spending in large enterprises, only 8.1% of those applications meet data security and privacy requirements, with predictable results.
- **Compliance:** Tracking and reporting helps ensure adherence to privacy laws, security standards, and industry regulations, which in turn reduce the risks of fines and legal fees in the event of a breach. SD-WAN solutions need to track real-time threat activity, facilitate risk assessment, detect potential issues, and mitigate problems.

The other problem with SD-WAN solutions that rely on an overlay security deployment is that IT staff are then required to manage WAN optimisation and security functions through two different interfaces. They can create critical gaps in their ability to see and respond to threats. By integrating WAN networking and security controls together, however, they can be managed through a single management interface, allowing administrators to ensure that security and networking policies support common objectives, and enable seamless integration and orchestration of policies and protocols. Even better, this does not only apply to the local SD-WAN connection, or even the extended branch ecosystem but across the entire distributed network. This not only ensures that branch deployments are no longer seen as separate and isolated network environments, but that a single, holistic security framework can be applied consistently across the extended and interconnected digital enterprise. "To better respond to the demands of today's digital marketplace, organisations are having to rethink their branch strategy. For many, new requirements mean transitioning away from the static MPLS networks of the past to provide fast and efficient interconnectivity between their branch offices and other critical resources. SD-WAN solutions hold the promise of providing the agility and flexibility today's digital businesses require. However, far too many of them do not adequately address the issue of security, leaving far too many organisations exposed to increased risk—and just at a time when cybercriminals are increasingly targeting branch offices as one of the weakest links in an organisation's security strategy." **Conclusion** Enterprises that implement SD-WAN without an integrated security solution put themselves at higher risk for malicious attacks and data breaches that are able to exploit gaps introduced by incomplete or poorly integrated overlay security solutions. By combined advanced security with WAN and LAN functionality, organisations can reduce complexity, lower TCO, and ensure that their flexible and responsive next-gen branch network doesn't expose them to new and unnecessary risks.

ABOUT DOROS HADJIZENONOS

Doros Hadjizenonos is Regional Sales Director Southern Africa at Fortinet

- ▀ Local eateries going digital now at risk of cybercrime - 24 Aug 2020
- ▀ How to have strong cyber hygiene - 26 May 2020
- ▀ How to approach data breaches - 11 May 2020
- ▀ Employees must be educated about mobile cyber threats - 13 Feb 2020
- ▀ Stay ahead of emerging cyber threats - 8 Jul 2019

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>