5 Myths About Enterprise SD-WAN

Debunking The Myths Around SD-WAN

Regardless of industry, today's enterprises constantly strive to improve productivity and reduce costs. Software and commodity internet connections now play a key part in achieving both: SD-WAN (short for software-defined wide area networking) represents a revolutionary way of thinking about how to connect locations.

As with many technologies, what started off as hype for the bleeding-edge is maturing into real solutions that can make an impactful difference, even for large, distributed organizations. With every new way of thinking comes misconceptions or "myths" that spread like wildfire before they are properly vetted.

It's time to debunk these SD-WAN myths. A Secure Enterprise SD-WAN approach is here, with SD-WAN connectivity and NGFW security managed together at scale to connect and protect your organization like never before.

Myth #1 and 2

SD-WAN is just about replacing MPLS to save money

MPLS services are expensive. They can even be difficult to get rid of, since they are typically bought as part of a long-term contract. But beyond putting a cap on spending, there is a better reason to implement SD-WAN: it's far more versatile than MPLS.

Using fast, commodity broadband instead of slower, expensive MPLS not only can save money, it can provide a "10x" increase in capacity. It provides resilience for business continuity, protecting sites from the legendary enemy of buried cabling—the backhoe. SD-WAN gives your expanding organization options for how to connect new locations where adding MPLS capacity is cost-prohibitive, slow to provision or may not even be available.

SD-WAN does more than save you money. It provides agility and options, boosts capacity, improves resiliency and accelerates new locations.

SD-WAN doesn't replace the internet but does facilitate connectivity.

SD-WAN takes the place of the internet

Some SD-WAN vendors try to sell their customers proprietary network connections and provide a front-end private network for getting to the internet. Such link-specific solutions are often only available in limited geographies and can be very slow to provision.

SD-WAN is about choices, enabling you to mix and match whichever links are most appropriate for each location (e.g., cable, DSL, fiber, 4G/LTE). It provides a way to facilitate and manage connectivity, but should never attempt to limit or take the place of any websites or internet applications.

Myth #3

SD-WAN eliminates the need for on-premises hardware

SD-WAN is frequently used to direct traffic for particular applications across specific links. This is especially important for reducing the latency needed to connect to highly interactive cloud apps like Office 365 while increasing the available bandwidth. It can be used to enforce techniques like encryption, which provides privacy for accessing cloud apps that aren't already relying on SSL/TLS and keeps data safe in transit.

But even with SD-WAN, you still need onpremises equipment to plug into your various network links. Strong security is an absolute must no matter where you're attached to the internet, and a firewall with built-in intrusion prevention and cloud security technologies (e.g., CASB, web security), whether part of each site's NGFW or as cloud-based services, can achieve this.

SD-WAN has some equipment at each location to plug into your ISP links and potentially provide necessary security.

Myth #4

SD-WAN solutions all come with high availability, easy manageability, and excellent security

SD-WAN has exploded in popularity, but that doesn't mean that all SD-WAN vendors do the same thing. Some only connect organizations or can only handle a few locations, and therefore have management systems geared towards a relatively small number of sites. These vendors may wrongly assume that all sites use the same types of connections.

Look for secure enterprise SD-WAN solutions for efficiency at scale.

A new generation of enterprise-grade SD-WAN solutions is emerging that:

- Connects thousands of locations over whatever type of network links are available and appropriate for each site
- Provides always-on resilience for around-the-clock productivity
- Tightly integrates security with connectivity to prevent gaps
- Offers 360° visibility into user behaviors and the flow of data everywhere, from branches to main offices, data centers to the cloud
- Enables common policies to be expressed once and reused automatically wherever needed
- Expresses special requirements for particular locations efficiently without disrupting normal operations
- Automates connectivity tasks like setting up VPNs among sites so that new sites can be added quickly and reliably
- Pushes policies to modify how sites are connected or secured
- Updates networking and security infrastructure without taking sites offline

Myth #5

SD-WAN already has security built into it

According to Gartner, branches need the same level of enterprise-grade security that is employed at headquarters for primary internet gateways. Many first-generation SD-WAN solutions enforce encryption of traffic over commodity broadband links using Virtual Private Network (VPN) technologies. This keeps data and communications between different sites private but doesn't make the sites more secure.

The new generation of enterprise-grade SD-WAN solutions has security that is fully distributed, instead of centralized like that of hub-and-spoke network topologies. This keeps attackers from sneaking into your stores, branches, or remote offices and protects the use of SaaS applications. Advanced Secure Enterprise SD-WAN uses techniques such as "service chaining" to apply security capabilities like web traffic protection and CASB to automatically secure data transmitted to cloud-based apps.

Secure Enterprise SD-WAN from Forcepoint

Forcepoint NGFW is used by organizations around the world to connect and protect highly distributed stores, branches and remote offices. Forcepoint eliminates gaps that come from having separate networking and security systems, providing the ability to manage thousands of devices from a single console and push updates to every location in minutes with just a few clicks. Our graphical VPN set up replaces laborious spreadsheets with immediate drag-and-drop to add new sites to even the most complex topologies in minutes. With Forcepoint, it's easy to augment or replace expensive MPLS lines with whatever commodity broadband links are available in each location.

Forcepoint Secure Enterprise SD-WAN for highly distributed organizations in the cloud era.

› Learn more

You need true secure enterprise SD-WAN, with more than simple traffic encryption

Forcepoint

forcepoint.com/contact

About Forcepoint

Forcepoint is the leading user and data protection cybersecurity company, entrusted to safeguard organizations while driving digital transformation and growth. Forcepoint's attuned solutions adapt in real-time to how people interact with data, providing secure access while enabling employees to create value. Based in Austin, Texas, Forcepoint creates safe, trusted environments for thousands of customers worldwide.

[5-Myths-About-Enterprise-SD-WAN-Ebook-EN] 25Nov2020