

WHITE PAPER

SECURE SD-WAN –
HELPING CIOs
MEET THEIR GOALS

What are CEOs and boards
talking about with CIOs

A question was asked at an event about hybrid IT, “What are CEOs and boards talking about with CIOs?” The general consensus was (in no particular order):

1. Reducing costs
2. Becoming more agile, being able to quickly implement new technologies to support digital transformation
3. Security and compliance

This list wasn't very surprising. It's hard to imagine an IT organization out there that isn't focused on these three areas. But in looking at this list, all three of these directives seem to be counter to each other. Beyond the small cost reductions gained by squeezing vendors, how does an IT organization reduce costs when it is being constantly pushed to implement new technologies to support its digital transformation (DX), security and compliance initiatives? Quickly implementing new technologies usually adds security risk and conversely, increased security often slows technology adoption.

So, are these directives realistic? Is it possible to actually accomplish all three at the same time? Fortunately, the answer is yes. By upgrading your legacy WAN to an SD-WAN, you can reduce costs while creating an infrastructure that is purpose built to support the dynamic requirements of digital transformation. And by implementing a Secure SD-WAN, you can also increase your overall security and compliance at the same time. No wonder a recent study found that 85% of organizations are considering implementing SD-WAN. But how does SD-WAN accomplish these goals and what is the difference between SD-WAN and Secure SD-WAN?

REDUCING COSTS

For organizations with many locations, MPLS circuit costs have soared in recent years as bandwidth requirements have ballooned. With SD-WAN, organizations can leverage much cheaper internet connections in addition to MPLS circuits to meet their increasing bandwidth requirements. This decreases the size and number of required MPLS circuits, significantly reducing costs. For example, one Open Systems' customer is saving around \$5 M per year on MPLS circuits costs with SD-WAN. What CIO wouldn't like to capture savings like that?

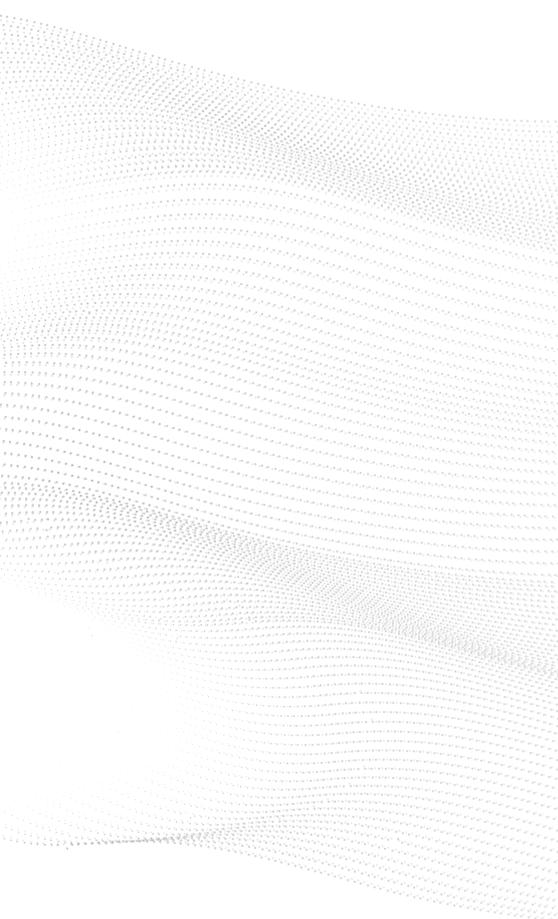
AGILITY AND DIGITAL TRANSFORMATION

While legacy WANs might use dynamic routing protocols such as OSPF or RIP, they are actually very static in their nature. These routing protocols do provide value as they reduce manual configurations and allow traffic to be automatically rerouted on a mesh network in response to a network outage or congestion. But they don't provide the flexibility that SD-WAN does. Because SD-WAN is application aware, you can route traffic differently based on the specific application. This enables both traffic shaping, and prioritization based on application criticality and requirements, something that dynamic routing protocols can't do. And because your policies are centrally managed and based on applications, new locations or services can quickly be provisioned, enabling cloud adoption as opposed to hindering it.

SECURITY AND COMPLIANCE

In addition to the benefits of SD-WAN mentioned above, Secure SD-WAN can help you accomplish your security and compliance goals. So, what's the difference between SD-WAN and Secure SD-WAN? You guessed it, security! While SD-WAN does have some limited security capabilities built in, like encryption, it doesn't include a fully integrated security stack like Secure SD-WAN does. But how important is this? Very.

“One benefit of SD-WAN is the ability to enable cloud adoption with local internet breakout.”



One benefit of SD-WAN is the ability to enable cloud adoption with local internet breakout, allowing each location to connect directly to the internet and cloud, as opposed to backhauling all the traffic to a main data center first. While local internet breakout significantly increases internet and cloud application performance, it introduces significant security and compliance challenges. Your complete set of perimeter security controls must now be implemented in every location where there is access to the internet. Instead of managing only a handful of firewalls, web proxies, IDS and DLP systems (to name a few), you might now be needing to manage hundreds of them. Ask any CISO and they will tell you that one of their biggest challenges is an extreme shortage of qualified security personnel so managing 10x or 100x more systems is next to impossible, let alone incredibly expensive, which really doesn't help with accomplishing the goal of reducing costs. But with Secure SD-WAN, all of these controls are fully integrated directly into the SD-WAN solution, reducing both Capex and Opex costs.

While replicating your entire internet security stack at each location increases internet and cloud performance by enabling local internet breakout, it really doesn't make you any more secure or compliant than backhauling all of your internet traffic to the data center. Secure SD-WAN, however, can do more than that. SD-WAN provides extensive visibility into WAN traffic flows and integrating this information with the Secure SD-WAN security stack logs significantly increases detection capabilities, minimizing dwell time and impact. But detection is just the beginning. Secure SD-WAN also allows you to automatically segment your network on the fly, reducing the impact of a breach, if and when one happens. For example, ransomware attacks often propagate over the WAN, infecting many more systems than if it had been isolated to the specific LAN where the initial infection occurred. The automatic segmentation provided by Secure SD-WAN will isolate the LAN traffic when an outbreak occurs, preventing it from using the WAN as a conduit to infect your other LANs, minimizing impact.

But, like all other technologies, Secure SD-WAN isn't without its challenges, the biggest of which is complexity, and this complexity often derails implementations. For this reason, many companies are opting for Secure SD-WAN as a service. Consequently, for everyone considering implementing Secure SD-WAN, it's critical to first ask yourself, do I have the in-house staff to manage the added complexity and increased workload? If the answer is no, Secure SD-WAN as a service is probably your best option.



Open Systems is a groundbreaking cybersecurity company delivering an experience way beyond expectations. Our obsessive care for our clients' businesses has led us to reinvent how cybersecurity is delivered to fit today's mobile, cloud-based world. Our team, based in North America, Europe, and Asia, consistently provides crazy good cybersecurity to leading organizations all over the world.