Opensystems

WHITE PAPER

5 KEY MISTAKES ORGANIZATIONS MAKE WITH SD-WAN SECURITY – **AND HOW TO FIX THEM**

It's tempting to think of SD-WAN security as a straightforward proposition. You install the technology at offices, plants, and other facilities and it encrypts the data that travels from one office or location to another. But, as with almost every situation and every technology, SD-WAN security is only as good as its weakest link. That's why it's important to think about the technology in a more expansive and strategic way – as a unified security platform rather than a point solution. Here are 5 common mistakes businesses make when installing or integrating SD-WAN systems – and how you can take your organization's network connectivity to a more secure and effective level.

Thinking that an SD-WAN inherently reduces risk.

MISTAKE #1

Adding connectivity across offices and other facilities ratchets up the overall complexity of IT and security. Overlaying an SD-WAN won't fix that. Industry research indicates that SD-WANs are 1.3 times more likely to suffer from a branch office security breach. There's also a need to segment and zone networks, which further increases interfaces and connection points with the cloud, SaaS applications, and internet applications. In fact, moving from an infrastructure-centric architecture to a cloud-first framework can have a ripple effect on everything from firewalls and intrusion detection to malware protection. It can also boost the need to train employees to spot phishing attempts and other social engineering tricks.

Solution

Build an SD-WAN framework that reduces risk by consolidating technologies. A well-engineered SD-WAN solution, with software-defined networking (SDN), can greatly simplify security and IT management through a unified platform that includes deep packet inspection, TLS decryption, next-generation firewall protection, and an embedded IPS as virtual security functions. By combining detection, analysis, and response at an operational level it's possible to increase overall security resilience and protect an enterprise 24x7.

Belie-ving that SD-WAN security is a set-and-forget pro-position.

MISTAKE #2

A common problem for organizations is that a new system or technology is put into motion and the focus moves elsewhere. SD-WAN is no exception. To mind the gaps, it's vital to have a plan for continuous monitoring and improvements. Innovation within the SD-WAN space must be ongoing, as the overall security landscape is constantly changing.

Solution

Consider network and security that requires a strategic approach that allows your organization to grow on a continuously evolving purpose-built platform with always up-to-date security installed and continuous proactive monitoring in place. This approach allows an enterprise to increase visibility and take control while benefiting from a team of experts monitoring the network. This collaborative approach represents the best of both worlds by integrating security features at every layer of the SD-WAN.

Viewing SD-WAN security as separate from an overall security program.

MISTAKE #3

Because organizations tend to view SD-WAN as a connectivity tool with built-in end-to-end encryption, some believe the technology doesn't require any additional attention. But while SD-WAN provides encryption of data in transit, it does nothing to protect data once it lands in a device or database. Unencrypted or unprotected data at rest poses a major risk.

Solution

To avoid dangerous security gaps, integrate the SD-WAN initiative into the overall security fabric through an agnostic SDN managed detection response approach. Security must extend beyond the SD-WAN with a sophisticated framework that incorporates policy-based controls and analytics about data at rest and in motion. In addition, a provider that offers consulting services and specialized expertise, such as a catalog of industry best practices, can serve as an extension of your team. It can, at the same time, reduce the reliance on outside consulting services and introduce a fixed-cost model rather than one where the meter is constantly running.

Consider-ring SD-WAN tech-nology as nothing more than a basic connecti-vity tool.

MISTAKE #4

It's not unusual for an organization to bolt security tools on top of SD-WAN, often in a reactive and uncoordinated way. It's vital to recognize that security stacks are by nature complex and they require orchestration. Cloud environments further complicate things – and alter risk patterns. Organizations that recognize that an SD-WAN initiative represents an opportunity to streamline security, including through more granular controls that match the user, country and regulatory environment, can improve protection while reducing complexity and costs.

Solution

Factor in SD-WAN security planning at the beginning of a project and understand how the architecture impacts a wide array of other factors, including tools, workflows, and systems. By partnering with an SD-WAN specialist it's possible to construct an environment that's transformed from rigid and complex to flexible, simple, and cost effective. This increases business agility and enables business growth.

Avoiding a more comprehensive strategic framework because it's time consuming and taxes resources.

MISTAKE #5

Many organizations avoid a more streamlined and focused SD-WAN security framework because of the time and energy required to make a wholesale change. But the financial costs and staff time associated with staying with the status quo and managing so many different tools, systems, technology platforms, and vendors is significant. The new reality is that your current and future requirements already demand an architecture that supports hybrid and multi-cloud application access as well as SaaS adoption.

Solution

Stop treating your network as a network and instead view it as your cloud. By unifying and consolidating systems, particularly through an SDN-centric approach to SD-WAN, it's possible to simplify administration, resolve issues faster, and mitigate threats more effectively. This also allows IT and security teams to focus on more strategic tasks than upgrades, patches, and fixes. The framework may also address talent gaps and technical debt – while delivering a highly scalable high-availability framework that adapts to future changes.

The Way Forward

Recent breakthrough market research by Gartner, "The Future of Network Security Is in the Cloud", revealed that appliance and infrastructure focus is not meeting current and future customer needs any longer. An unwieldy and costly site-by-site implementation of DIY WAN security solutions is no match for the sophisticated and aggressive cyberthreats that enterprises face today. Deploying a secure SD-WAN doesn't have to be a frustrating and expensive exercise in futility. You can avoid the mistakes that trip up so many enterprises while breaking free of proprietary jails that make IT and security needlessly complex.

Look for an SD-WAN provider that offers a simplified, comprehensive, unified network and security platform that combines detection, analysis, and response to protect your business today with the flexibility and capabilities to meet the secure networking challenges of tomorrow.

How can you get started?

Contact us today.

Take a look at Open Systems.

We offer a zero compromise, cloud-integrated network- and security-as-a-service framework for a digital-first world.

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.

Learn more at open-systems.com |