A Step-by-Step Guide To Securing SD-WAN

When it comes to supporting digital innovations, a traditional WAN simply won't suffice. Today's cloud applications demand a simplified, flexible, and cost-effective alternative that can ensure peak performance of critical applications and provide direct access to them. Enter software-defined wide-area networking (SD-WAN), which provides greater application performance, centralized management across branch networks, and lowered operating costs.

There were
945 DATA BREACHES
with these incidents leading to
4.5 BILLION DATA RECORDS
being compromised.

The Importance of Security With SD-WAN

While SD-WAN technology can provide branch office staff with direct access to cloud-based applications, it can also expose organizations to crippling cyberattacks. That's particularly concerning for growing organizations whose branch locations typically have lower levels of security than headquarters.

4 Simple Steps To Secure SD-WAN

When it comes to SD-WAN deployment, organizations must rethink outdated security principles and extend protection beyond the data center by integrating the security architecture into the network infrastructure. The following four steps can help address the legitimate security concerns surrounding SD-WAN:

1. Secure an expanded attack surface created by digital innovation initiatives and the SD-WAN infrastructure itself
2. Ensure that malware that does enter the network does not travel horizontally
3. Compensate for the lack of trained IT security staff at some remote locations
4. Provide networkwide visibility and centralized security controls for the entire enterprise

The Making of A Security Strategy

Network security and network operations teams typically work in silos—two separate factions with differing priorities and sometimes competing goals. But that has to change for organizations to ensure a secure SD-WAN deployment.

By sharing in the decision-making process for a solution, these teams can create a security strategy that protects against cyber threats and prevents SD-WAN from becoming the weakest security link for an organization.

The Features You Need To Succeed

Using SD-WAN to improve WAN efficiency doesn't have to compromise security. The following next-generation capabilities can deliver the most trusted network security—and peace of mind:

- Comprehensive threat protection, including next-generation firewall, antivirus, intrusion prevention system (IPS), and application control
- High-throughput SSL inspection performance based on purpose-built security processors
- Web filtering to enforce internet security without requiring a separate secure web gateway
- Highly scalable and high-throughput IPsec VPN tunnels to ensure that traffic is always encrypted and stays confidential
- A centralized manager that enables zero-touch deployment and easy administration

Why Fortinet?

Fortinet's Secure SD-WAN solution delivers the most robust threat protection in the industry, including Layer 3 through Layer 7 security controls not commonly found in other SD-WAN-plus firewall solutions. From application control and web filtering to antivirus protection and intrusion prevention, Fortinet protects an organization's critical data and applications from a full range of threats. IT teams can manage their networks easier than ever but with improved connectivity, increased cost savings, and greater security.

To find out more about Fortinet's Secure SD-WAN solution,
visit fortinet.com