CHECKLIST

# Choosing an SD-WAN for Secure WAN Edge Transformation: 7 Requisite Capabilities

While software-defined wide-area networks (SD-WANs) offer major performance and convenience advantages over the traditional WAN, these benefits come at the expense of centralized security from backhauling traffic through the organization's main data center. In addition, with wireless WAN (i.e., LTE/5G) connectivity on the rise, improper integration and management with SD-WAN can lead to added complexity.

Vulnerabilities associated with an expanding branch network attack surface, increasing infrastructure complexity, and a rapidly evolving threat landscape call for **security-driven networking**—namely, deep integration between networking, including wireless WAN, and security capabilities at a platform level. This deep integration protects both the LAN and all WAN connectivity including wireless WAN. Effective SD-WAN also requires sophisticated, unified **management** and **orchestration** capabilities for automatically selecting the best network paths including LTE/5G based on contextual factors such as the specific application in use, business priorities, and security risks.

## 7 Requisite SD-WAN Capabilities

Many vendors currently offer some form of SD-WAN, with many claiming their solutions include security. But in many cases, comprehensive full-stack security is not integrated into the solution—leaving the network vulnerable to attack or requiring the purchase of additional security devices. Furthermore, there is no tight integration between wireless WAN and SD-WAN. When doing initial exploration of SD-WAN, network engineering and operations leaders can use the following checklist of questions to determine which solution is best:

- ☑ **1. Risk exposure**

  How will my risk posture change if I adopt this SD-WAN solution?

- ☑ **2. Threat protection**

  Are there limits to the types of threats that can be detected?

- ☑ **3. Compliance**

  Does the solution support all of the applicable regulatory requirements for industry standards and data privacy obligations—including tracking, auditing, and reporting functions?

- ☑ **4. Orchestration**

  Does the solution offer automated capabilities for application awareness and path intelligence to select the best network connections, including LTE/5G wireless WAN, based on changing variables?

- ☑ **5. Management**

  Can the solution provide full visibility as well as be easily deployed and remotely managed (via the cloud)?

- ☑ **6. Total cost of ownership (TCO)**

  Is there an operational cost to implementing the SD-WAN and wireless WAN solution? If so, what is it?

- ☑ **7. Third-party validation**

  Has the solution been thoroughly tested and recommended by independent industry experts?

Deployment of an effective SD-WAN solution that can ensure reliable and secure WAN connectivity including wireless WAN offers distributed organizations the chance to solve both the networking and security problems of traditional WAN at the same. But in order to achieve that, network engineering and operations leaders should carefully compare the comprehensive capabilities of competing products against the full set of their solution needs.

www.fortinet.com



January 20, 2022 11:56 PM

429013-A-0-EN