FORTINET

Unlocking the Secure WAN Edge: 10 Essential SD-WAN Transformation 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.

Vulnerabilities associated with an expanding branch network attack surface, increasing infrastructure complexity, and a rapidly evolving threat landscape call for secure networking—namely, deep integration between networking and security capabilities at a platform level. Effective SD-WAN also requires sophisticated management and orchestration capabilities for automatically selecting the best network paths based on contextual factors such as the specific application in use, business priorities, and security risks.

10 Essential SD-WAN Capabilities

Over two dozen vendors currently offer some form of SD-WAN, but only 14 are recognized in the 2023 Gartner Magic Quadrant. 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. 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:

☑ **Risk exposure**
How will my risk posture change if I adopt this SD-WAN solution?

☑ **Threat protection**
Regulatory bodies in some countries require compromise assessments. These authorities understand today's enterprise security challenges and want to ensure businesses are working from a proverbial clean slate, understanding potential risks before any damage can ensue.

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

☑ **Orchestration**
Does the solution offer automated capabilities for application awareness and path intelligence to select the best network connections based on changing variables?

☑ **Management**
Can the solution provide networkwide management and automation, be easily deployed, and remotely managed (via the cloud)?

☑ **Monitoring**
Can the solution offer comprehensive monitoring of device, link, path, and application performance to optimize user experience and simpify operations?
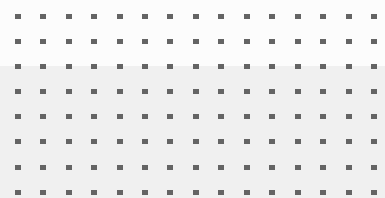
☑ **Total cost of ownership**

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

☑ **Third-party validation**

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

☑ **SASE**

Is the SD-WAN solution capable of supporting single-vendor SASE?

☑ **SD-Branch**

Can the SD-WAN solution provide migration to SD-Branch with tight integration on hardware, software, and management levels?

An effective SD-WAN solution offers distributed organizations the chance to solve 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.

F⊝RTINET

www.fortinet.com