CHECKLIST

The 5 Keys to Self-Healing, Secure SD-WAN

SD-WAN solutions have become increasingly popular as organizations request fast, scalable, and flexible connectivity among different network environments, and seek to lower overall total cost of ownership (TCO) while preserving user experience. But the wrong SD-WAN solution can significantly inhibit an organization's ability to quickly adapt to changing business demands, not least because it creates new security headaches.

Here are five requirements for a Secure SD-WAN solution that's flexible, scalable, and fit for the needs of today's distributed enterprises.

☑ It goes beyond the branch.

SD-WAN is perhaps best understood for supporting complex branch deployments and helping organizations reduce their reliance on branch routers and other legacy technologies. Effective SD-WAN solutions go well beyond branch office needs, however. Their functionality can extend to home office and teleworker use—especially appliances with built-in LTE for consistent connectivity—and among distributed clouds. SD-WAN solutions also need to come in virtual versions that are available in multi-cloud environments and have deeper integration to enable cloud on-ramp, enabling efficient SaaS adoption.

☑ It offers intuitive orchestration and zero-touch deployments.

Both of these features enable faster configuration rollouts at scale, often within minutes, to enable the best possible performance of collaboration applications such as VoIP, videoconferencing, and various SaaS applications, even for remote users based far away from the corporate data center. Orchestration enables overlay (VPN) automation for the most complex network with intuitive workflows.

☑ It prioritizes critical applications and enables self-healing WAN.

Connectivity alone isn't enough, especially in a remote work-heavy environment. A solution needs to identify a broad set of applications to meet all use cases, while advanced self-healing WAN automation will provide consistent user experience on any transport for any user. Many SD-WAN solutions only support limited use cases, limited numbers of users, and/or specific environments. Caveat emptor.

☑ It includes integrated security.

The difference between SD-WAN and Secure SD-WAN is that the latter is a solution, while the former is a connectivity offering providing another conduit for the bad guys to attack your network. An overlay security solution can't adapt to dynamic connectivity environments; security needs to be embedded into each SD-WAN device, enabling home users, branch office users, and the data center to use a common set of security policies and enforcement criteria. In true Secure SD-WAN, networking, connectivity, and security functions are so tightly integrated they're the one solution meeting three needs, instead of three discrete solutions.

☑ It offers comprehensive analytics and reporting.

A Secure SD-WAN solution needs to help organizations gain visibility into network and application performance (both real-time and historical statistics). That includes enhanced analytics as well as enhanced compliance. A single console and rich SD-WAN analytics can help customers fine-tune their business and security policies to improve quality of experience for all users.