

Five Requirements for SD-WAN

SD-WAN solutions must meet five key requirements to provide the value required by today's lean digital businesses



Software Defined Wide Area Networking (SD-WAN) describes a series of techniques that, when employed together, abstract the underlying network topology and links from the sites, users, and systems that consume them. This allows businesses to think of their WAN in business terms—applications, sites, performance, security, and compliance—rather than as a series of networking rules, protocols, or rarely-compatible features.

As a fundamentally transformational technology, it comes as no surprise that myriad vendors are claiming to provide an SD-WAN solution, hoping to capitalize on the value proposition that SD-WAN provides, even if peddling an incomplete solution. Our goal in this manifesto is to describe in no uncertain terms what SD-WAN is and the capabilities a solution must include to be considered an SD-WAN solution.

Requirement 1. Business-Centric Policies

For the past three decades, connecting and configuring networking devices has required a tremendous technical translation of business needs to underlying rules and protocols. This complexity has driven an entire ecosystem with deep yet expensive technical proficiency that has wedged a chasm between business need and deployment.

SD-WAN solutions must provide an opportunity to bridge this chasm and allow businesses to deploy, configure, and manage their WAN using policies that directly correlate to the business intent rather than complex, fragmented, low-level rules. SD-WAN solutions must define policies using language that is natural to business around performance, security, and compliance, and these policies must be associated with applications, sites, and links.

Requirement 2. Uncompromised Cloud-Readiness for Remote Offices

Traditional WAN architectures are no longer serving business. Legacy models backhaul application traffic from remote offices over expensive low-bandwidth WAN links through centralized data centers where perimeter technology for monitoring and security is deployed. Forcing this architecture can compromise performance for cloud and Software-as-a-Service (SaaS) applications by adding latency and bandwidth constraints.

SD-WAN solutions must take advantage of the best performing path—whether it is direct Internet or private WAN—without compromising security or visibility. SD-WAN solutions must continually monitor performance for all applications and all WAN links to adapt traffic handling decisions based on these indicators and provide an experience for cloud and SaaS applications that is not hindered or compromised by a legacy WAN architecture.

Requirement 3. WAN Transport, Carrier Agnostic

Most enterprise WANs were designed to connect to private multiprotocol label switched (MPLS) networks to provide secure interconnection between remote offices, campuses, and data centers. Telecommunications carriers have simplified WAN deployment by providing managed offerings for circuits, on-premises equipment (routers), and ongoing management. This trifecta of lock-in has made businesses unequivocally chained to their carrier and the circuits they offer.

SD-WAN solutions must reduce dependency on carriers and specific classes of WAN transport. Businesses must be able to enjoy freedom to choose the WAN transport for each of their locations from the most appropriate carrier based on price, performance, service-level agreements (SLAs), and customer support requirements. Further, businesses must be able to seamlessly transition from one provider to another without disrupting their business should their service provider not be fulfilling their SLA obligations.

Requirement 4. Modular, High Performance Software

The majority of networking devices sold today are built using compute, memory, and storage technologies that are more than five years old and not designed to operate or function on general-purpose computing environments (such as Intel x86). Most networking device vendors develop and incubate their new product platforms for at least two years prior to selling to customers, and maintain a product lifecycle of ten years. This means that, for the majority of businesses, devices deployed in their network could be using technology that is a decade old or more. Antiquated technology cannot keep up with the demands of modern businesses, especially when it comes to transforming their WAN from one dominated by esoteric networking commands to one that is managed according to business policy. Further, this antiquated technology is not virtualization friendly, meaning, businesses are unable to deploy these devices virtually on general-purpose compute hardware of their own choosing.

SD-WAN solutions must break this chain and give businesses the ability to deploy networking functions on platforms that provide flexibility and diversity of form factor. That is, businesses must be able to take advantage of both discrete networking devices and run the same networking device software on virtualized hardware of their choice. Businesses must be afforded the opportunity to design and deploy their I/T architecture—including networking—using platforms and form factors that enable them and empower them, rather than hinder them.

Requirement 5. Actionable Analytics, Self-Healing

With legacy networking devices that are practically blind to the intricacies of application performance, businesses have been forced to augment their network infrastructure with a host of performance monitoring and visibility solutions. While these solutions are compelling and complete, they require significant investment in terms of servers, storage, and management, and provide limited value in scenarios where application traffic is not seen by these systems, which is common in direct Internet scenarios.

SD-WAN solutions must extend perimeter technology to each location—including security, performance visibility, and ongoing monitoring. Further, this data must be exposed to the business without requiring additional servers, storage, or management infrastructure. The data must have detailed awareness of key performance indicators related to the overall application experience, and be actionable in that businesses can quickly understand root causes when issues arise.

Most importantly, SD-WAN solutions must use this same data to learn and understand how applications are performing, and remediate issues when performance, security, or compliance policy requirements are not met.

Summary

Several solutions have surfaced claiming to provide SD-WAN capabilities though they lack key fundamental architectural components. These five requirements are presented to help establish a standard definition for what constitutes an SD-WAN solution, with the primary goal being enablement and empowerment of businesses, allowing them to enjoy more agility, reduce costs, simplify management, improve overall user experience, and maximize employee productivity. While any solution lacking in one of these five requirements may provide incremental value, that value pales in comparison to an SD-WAN solution that is full-featured and addresses each of these five core goals, and severely limits the overall benefit a business would enjoy.

SEE FOR YOURSELF

SEE CLOUDGENIX IN ACTION FOR YOURSELF!
VISIT WWW.CLOUDGENIX.COM/TRIAL TO REGISTER FOR A NO-RISK FREE TRIAL TODAY.

ABOUT CLOUDGENIX

CloudGenix provides a software-defined WAN solution with AppFabric technology that enables you to build a global WAN based on business policies for application performance, compliance, and security, across all sites and users. Unlike router-based solutions, CloudGenix AppFabric allows you to define top-down global policies based on business intent rather than fragmented bottoms-up configuration changes based on technical implementation. With CloudGenix, you can easily integrate heterogeneous WAN connections for any site, take advantage of cloud and SaaS applications, improve visibility for app performance and SLAs, and dramatically simplify network operations.