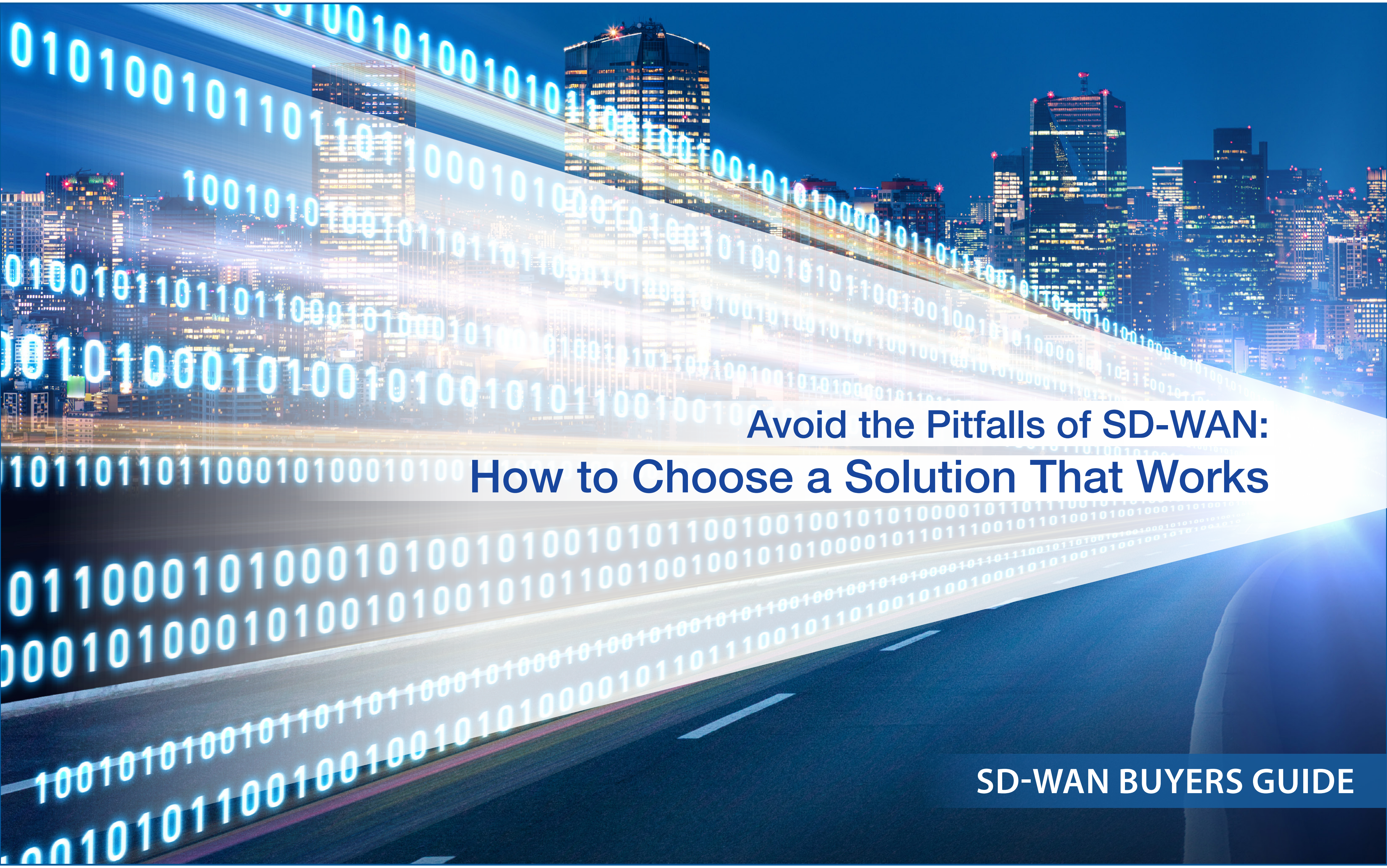


Avoid the Pitfalls of SD-WAN: How to Choose a Solution That Works

SD-WAN BUYERS GUIDE

Table of Contents

Avoid the Pitfalls of SD-WAN:
How to Choose a Solution that Works

If you operate a business with more than just a few sites, you face unique challenges. You have greater complexity in how you manage networks – needing to ensure that all locations receive the performance necessary to make effective use of VoIP, video and other business-critical applications. Given IT resource shortages, you struggle to find a way to keep technology up to date without technical staff at each location to deploy it. Furthermore, you seek creative ways to keep from blowing up your budget as bills from ISPs and MPLS (multiprotocol label switching) services escalate out of control.

Not surprisingly, SD-WAN solutions sound like the ultimate answer – offering centralized management for complete visibility across your distributed network, simplified deployment procedures that even the non-technical worker can handle, and dynamic WAN selection technology for high network performance experiences while stabilizing Internet service costs at the same time. The potential benefits of SD-WAN have made the product a hot topic among CIOs and IT professionals of multi-site companies. Though, it's hard to know whether these inquiries represent a genuine intent to deploy, or healthy skepticism in a product that maybe seems too good to be true.

In this guide, we look at the promise of SD-WAN, and offer perspectives that will help you identify the right solution for your organization. We'll also examine common deployment pitfalls and share advice on planning for a successful implementation. Should you move forward with an SD-WAN project, we hope that the information provided will help you to facilitate a smooth installation and deliver predictable results.

What Is SD-WAN?

SD-WAN refers to software-defined wide area networking, and this term represents the product or feature set that is used to automate the selection of a WAN interface, given multiple WAN options, based on the type of traffic and how the real-time measurement of the performance metrics for each connection compares to the minimum requirements defined in policy. The key feature of an SD-WAN product is the "dynamic path selection," though many have broadened the definition to include features that reduce the costs and complexity of management and administration – realizing that branch offices are typically working with fewer IT staff and less specialized expertise.

The following areas are commonly cited as the functional requirements for an SD-WAN product:

- Perform the WAN routing necessary to distribute traffic across multiple WAN transport mediums (e.g. MPLS, Internet, 4G/LTE, etc.)
- Allocate traffic dynamically based on user-defined policies and near real-time measures
- Provide a simplified management GUI and zero-touch branch site provisioning
- Include integrated VPN technology with 128-bit (or higher), encryption, and allow direct connection of other network appliances such as firewalls and WAN acceleration

What's Driving SD-WAN Product Consideration?

Companies are experiencing the following IT conditions, and so are evaluating every product or technology that can help to address them.

- **Cloud-based applications and web services...**as more and more applications migrate to the public Cloud, hybrid WAN architectures are preferred over traditional hub and spoke approaches to reduce the application performance issues caused by latency.
- **WAN costs**…annual expenditures for Internet service continue to grow year over year as performance and bandwidth requirements grow, and companies are looking for smarter ways to meet budget without impacting network performance.
- **Network complexity**…WAN management and configuration are difficult and often overly manual, contributing to high staff utilization and cost of ownership.
- **Resourcing challenges**…it's getting harder to recruit and keep experienced IT staff, especially for staff based outside of corporate HQ or large sites, requiring organizations to deploy and manage infrastructure from afar.

SD-WAN Providers

There are different types of companies offering SD-WAN solutions. They can be categorized as follows:

- **SD-WAN providers:** Viptela, Silver Peak, Versa, Talari, etc. (some reports track 23 different vendors). These companies formed to meet this market with a specialized SD-WAN product, and base their value largely on their software and management platform. Large network infrastructure companies such as Cisco (Viptela), Citrix, and VMware (VeloCloud) have been acquiring SD-WAN point product providers in order to leverage their relationship with large customers to consolidate all networking including SD-WAN.

- **Security providers:** WatchGuard, Fortinet, SonicWall, Meraki, etc. Security appliances are at a critical control point at all corporate network sites, and most already include routing and networking features. So, adding SD-WAN features to their platforms is a natural fit. The advantage of these solutions over other SD-WAN options is that they are willing to provide SD-WAN at no/little cost in order to earn the security business. Over time, this will make it hard for other providers to charge extra for SD-WAN except where they offer SD-WAN features beyond what security solutions typically provide, such as a dedicated Internet backbone for backhauling and prioritizing traffic (Cato, Bigleaf).

- **ISPs:** Verizon (Cisco Viptela or Meraki), AT&T (VeloCloud), CenturyLink (Versa Networks), Deutsche Telekom, British Telecom (Nuage) and others have packaged SD-WAN solutions for businesses, many of which are OEM solutions from the SD-WAN providers listed above. Ironically, these are the same companies profiting from MPLS and other WAN connections, which may cause some potential customers to be naturally skeptical of the efficacy of their SD-WAN offering.

Secure SD-WAN Deployments

While SD-WAN products don't specifically require security, we typically see companies evaluating these solutions in conjunction with security upgrades at branch offices and distributed sites. In this way, the corporate network maintains a consistent security posture across the enterprise while enabling hybrid WAN benefits including direct access to Cloud applications and resources. When considering SD-WAN inclusive of security, there are four deployment models in practice, each with their own pros and cons.

SD-WAN appliances with embedded network security

✓ **PROS** Some greater depth of SD-WAN features and granular controls may be available, though it is unclear how often the additional features are needed.

✗ **CONS** Specialized SD-WAN providers are often start-ups with some networking background and little security expertise, which can mean greater business risk from breaches or continuity of product support.

SD-WAN appliances with Cloud-based network security

✓ **PROS** Some greater depth of SD-WAN features and granular controls may be available, though it is unclear how often the additional features are needed.

✗ **CONS** Functionality is still lacking compared to dedicated security appliances, and managing two vendors can lead to greater TCO. Also, scanning packets in the Cloud doesn't protect from direct attacks to the site and can moderately increase network latency as compared with inline security.

SD-WAN appliances with network security appliances inline

✓ **PROS** Some greater depth of SD-WAN features and granular controls may be available, though it is unclear how often the additional features are needed.

✗ **CONS** Two vendors to coordinate and manage can lead to greater TCO.

Firewall appliances with embedded SD-WAN

✓ **PROS** The most effective security comes from security experts. Network routing features have always been a part of firewall products and offer the best pricing/value. Getting it all from one provider simplifies management and deployment for lowest TCO.

✗ **CONS** Perhaps fewer SD-WAN configuration options such as with a dedicated Internet backbone for backhaul, though core functionality is clearly available.

Secure SD-WAN Deployments

Comparing just the two deployment options that do not require multiple vendors, we can see that most of the product differentiation appears in the security offering from each type of provider.

		Network Security Providers	SD-WAN Providers
SD-WAN	**Multiple WAN Links** including MPLS, Internet, 4G/LTE, etc. are fundamental	🟩	🟩
	Dynamic Traffic Distribution includes link monitoring for jitter/loss/latency, dynamic path selection, application traffic management, and quality of service (QoS) logic and selections	🟩 Check that your provider offers link monitoring with dynamic path selection	🟩
	Site-to-Site VPNs are commonplace, but look for differences in ease of set-up, health/monitoring, notification options and stability	🟩	🟨 Ask if a 3rd party device for site-to-site VPN is required
	Centralized, Cloud-based Management a simple GUI used for configuration, management, monitoring, and reporting	🟨 These large management platforms typically include some Cloud interfaces	🟩
	Zero-Touch Deployment means that no technical expertise is required on-site, just plug in the hardware	🟩 Make sure your provider offers a remote deployment tool	🟩
	Dedicated Internet Backbone not required for every implementation – it allows for traffic backhaul	🟨 Achieved using integrations with SD-WAN providers	🟨 Roughly half of SD-WAN providers offer this capability
SECURITY	**Stateful Firewall with HTTPS Inspection** provides essential protection for any location	🟩	🟨 This is not a typical feature for SD-WAN providers
	Standard Security Services including IPS, GAV and web filtering to protect any site with direct Internet access	🟩	🟨 This is not a typical feature for SD-WAN providers
	Advanced Security includes sandboxing and DNS filtering to prevent common evasive attacks using malicious files and connections	🟨 Inquire into each provider's unique offering – some offer more protection than others	🟥 **Not available**
	Malware Detection and Response automatically remediates threats that get past preventative defenses	🟨 Inquire into each providers unique offering – some offer more protection than others	🟥 **Not available**

Avoiding SD-WAN Deployment Pitfalls

Choosing the right product to address your unique needs is just part of what it takes to implement SD-WAN successfully. For maximum ROI, be sure to learn from others' mistakes, and avoid these pitfalls.

Expecting to get rid of MPLS entirely

- Just about every article, ad, and blog post on SD-WAN will make a reference to "eliminating MPLS," yet industry reports show the MPLS market continuing to grow and surveys indicate that early adopters haven't discontinued their MPLS service. It appears that they are using SD-WAN products to lessen how much traffic uses MPLS, and presumably lowering their expenses in the process, but they don't want to degrade performance when applications need MPLS to function correctly. Some have suggested that businesses are putting a transition process in effect, where they gradually raise the bar for traffic to use the MPLS to see if all the traffic can use other WAN options without issue or complaint. For these reasons, if your ROI for SD-WAN is largely based on eliminating MPLS, then you may first want to revisit that calculation and see if implementation makes sense while retaining MPLS at a lower rate of usage.

Buying SD-WAN from ISPs

- You've probably already received an offer for an SD-WAN managed service package from your ISP, but before you pull the trigger, be sure to get quotes from a couple other providers. More than likely, the ISP is trying to stay atop of a new technology that could disrupt their business by offering legitimate services, but because the decision of which WAN to use is now in the hands of a company who benefits financially when some choices are made versus others…it's worth it to look at alternatives before making the decision.

Not involving security teams

- More than likely, your networking team is leading the charge to implement SD-WAN. While this makes complete sense, you should insist that your security team, whether in-house or out-sourced, is also brought into the project as early as possible. It doesn't take too long to realize that SD-WAN more easily allows for a hybrid-WAN architecture…and if this is a change for your distributed sites, then it means that users and data will no longer be completely protected by the corporate security infrastructure. A new security evaluation needs to be a part of the process or else you risk accidently leaving the door open to cyber criminals.

Paying too much

- Early SD-WAN adopters had few alternatives but to purchase a stand-alone solution from an SD-WAN provider. This meant that they added infrastructure and service expenses to their existing network without combining or replacing any existing network gear. Now that the market has evolved, many providers offer SD-WAN capabilities as part of their security or networking platforms, giving today's customers the option to package it with existing solutions and ultimately pay less overall.

Underestimating indirect costs

- When looking at total cost of ownership (TCO), it's natural to focus on direct expenses and ignore the impact of indirect expenses. Yet, costs associated with managing multiple vendors, building manual reports across an enterprise, and ensuring compliance across a complex network architecture can quickly outspend the initial outlay of cash by many multiples. It helps to get network administrators engaged during the purchase process, so that they can weigh in on the cost of time to manage each solution in consideration, and you can make a more informed decision.

Is Your Company Ready to Move Forward with SD-WAN?

Complete the information below to see how beneficial SD-WAN can be to your organization!

1) Average number of WAN connections per site ____________
(if 1, then go directly to the Total line and enter 1)

2) Number of sites (branch office, store, clinic, other) ____________

3) Typical number of Cloud applications or web resources used by remote site employees ____________

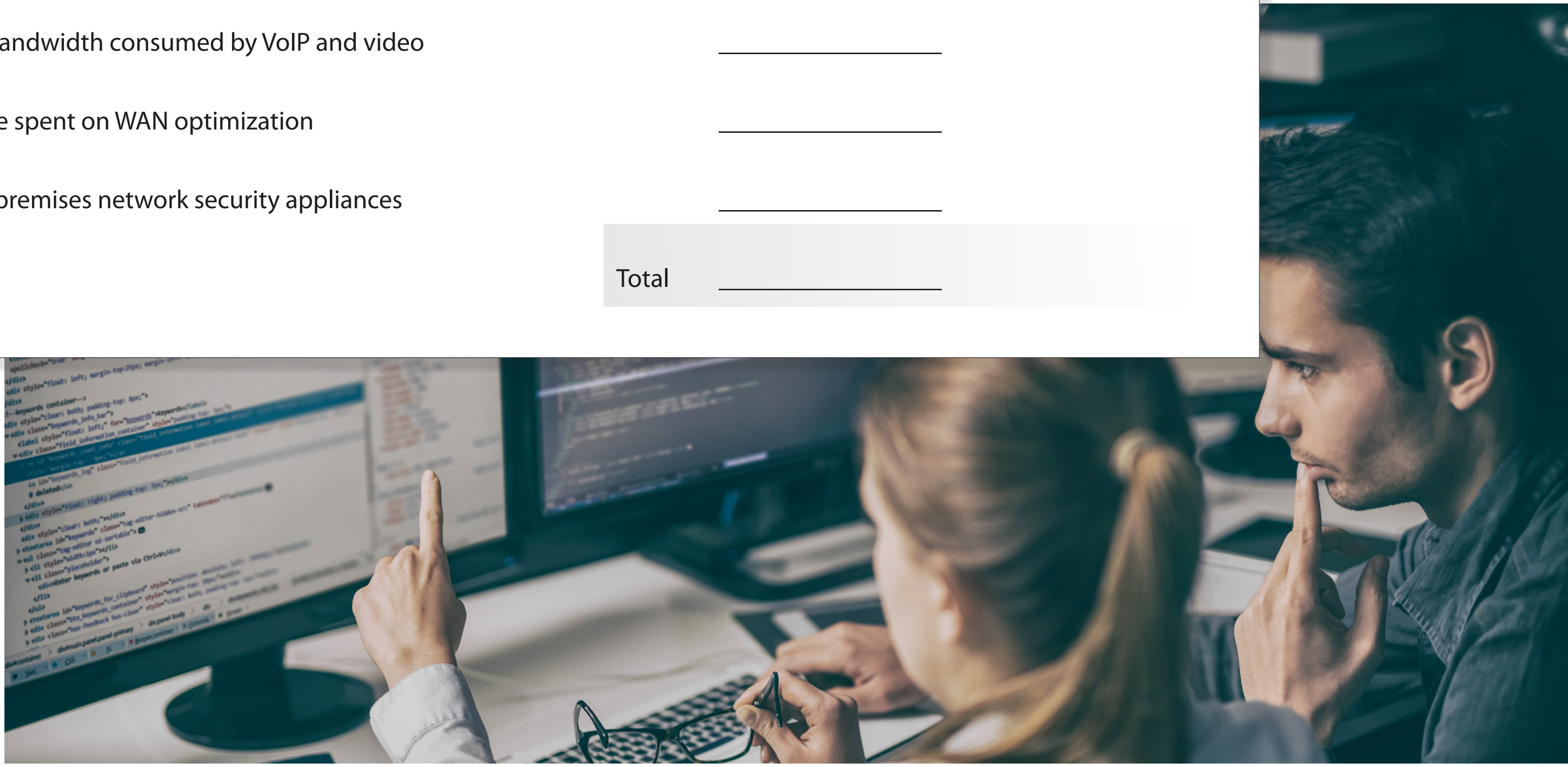
4) Percentage of IT budget spent on remote site Internet service ____________

5) Percentage of available bandwidth consumed by VoIP and video ____________

6) Percentage of IT staff time spent on WAN optimization ____________

7) Number of sites with on-premises network security appliances ____________

Total ____________



Scoring:

Add up the numbers to determine your total. If you responded that you had one WAN service per site, then the total should be "1" for your organization. Treat any percentages as a 2-digit number out of 100 (e.g. 52% = 52 for scoring purposes).

Compare your total to scoring categories below:

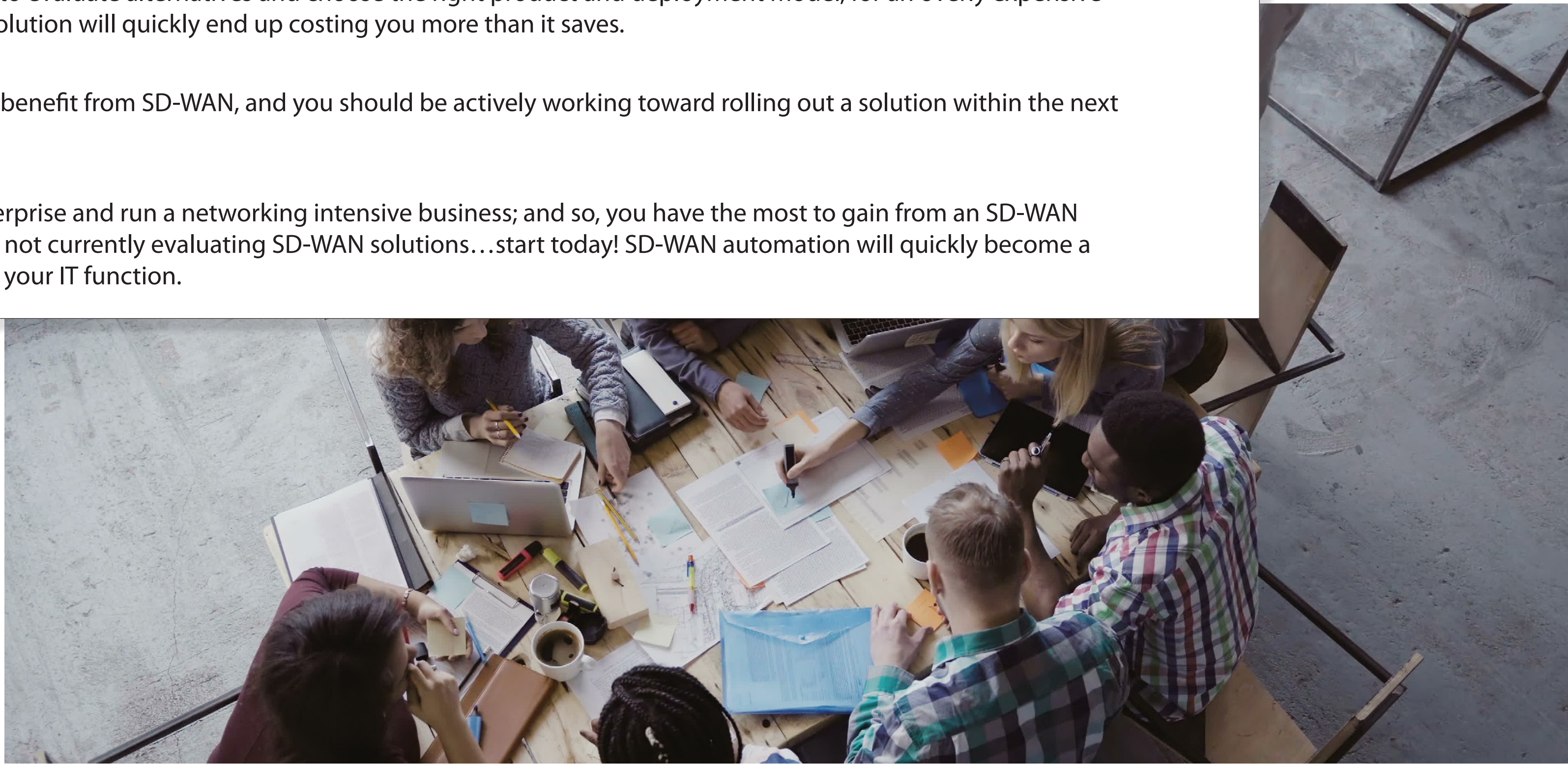
1 – 50 Your company's networking resources are not widely distributed, or you do not have a multi-WAN environment. Therefore, you would not likely see immediate value from an SD-WAN implementation. You'll want to carefully consider the direct and indirect expenses specifically related to any additional complexity from SD-WAN.

51 – 100 Your organization has one or two characteristics of companies exploring the benefits of SD-WAN solutions. You'll want to identify the specific areas of potential benefit and understand if SD-WAN generates the best ROI as compared to other alternatives.

101 – 300 You've extended your operation across multiple geographies and have network demands that would benefit from SD-WAN. Take the next 18 months to evaluate alternatives and choose the right product and deployment model, for an overly expensive or poorly implemented solution will quickly end up costing you more than it saves.

301 – 500 Your company is likely to benefit from SD-WAN, and you should be actively working toward rolling out a solution within the next 12 months.

Over 500 You are a distributed enterprise and run a networking intensive business; and so, you have the most to gain from an SD-WAN implementation. If you're not currently evaluating SD-WAN solutions…start today! SD-WAN automation will quickly become a key strategic initiative for your IT function.



THE WATCHGUARD SECURITY PORTFOLIO

Network Security

In addition to delivering enterprise-grade security, our platform is designed from the ground up to focus on ease of deployment, use, and ongoing management, making WatchGuard the ideal solution for SMB, midsize, and distributed enterprise organizations worldwide.

Secure Wi-Fi

WatchGuard's Secure Wi-Fi Solution, a true game-changer in today's market, is engineered to provide a safe, protected airspace for Wi-Fi environments, while eliminating administrative headaches and greatly reducing costs. With expansive engagement tools and visibility into business analytics, it delivers the competitive advantage businesses need to succeed.

Multi-Factor Authentication

WatchGuard AuthPoint™ is the right solution to close the password-driven security gap that leaves companies vulnerable to a breach. It provides multi-factor authentication on an easy-to-use Cloud platform. Our unique approach adds "mobile phone DNA" as an identifying factor to ensure that only the correct individual is granted access to sensitive networks and Cloud applications.

Find out more

For additional details, talk to your authorized WatchGuard reseller or visit **https://www.watchguard.com.**

About WatchGuard

WatchGuard® Technologies, Inc. is a global leader in network security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by nearly 10,000 security resellers and service providers to protect more than 80,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for distributed enterprises and SMBs. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Pacific, and Latin America. To learn more, visit WatchGuard.com.

WatchGuard

North America Sales: 1.800.734.9905 • International Sales: 1.206.613.0895 • Web: www.watchguard.com

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. ©2018 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and are trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE671390_112818