

# The Top 5 SD-WAN 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 avoid making these common mistakes!



**1 Don't expect 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 continue to use their MPLS service.

**2 Take caution when sourcing SD-WAN from ISPs**  
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 final decision.

**3 Be sure to involve your 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.

**4 Avoid paying too much**  
Now that the market has evolved, many providers include SD-WAN capabilities as part of their security or networking platforms, giving today's customers the opportunity to pay less overall.

**5 Account correctly for indirect costs**  
Costs associated with managing multiple vendors, building manual reports across an enterprise, and ensuring compliance across a complex network architecture can quickly exceed the initial outlay of cash by many multiples.

The SD-WAN market is expected to reach **\$4.5B** or more by **2022**

**62%** of enterprise attendees at the London WAN Summit anticipate keeping MPLS for the next **3-5 years.**

SD-WAN will be in **50%** of WAN infrastructure refreshes by **2020**

## SD-WAN + Security = Optimal IT Benefits

Be careful to not introduce gaps in coverage at the remote site. Are you opening the location up to direct attacks if you only deploy Cloud-based security? Is your branch office security comparable to HQ? When looking at the overall business requirements for your SD-WAN deployment, security is almost always a consideration. Therefore, the cost and simplicity benefits of an all-in-one solution consistently outweigh the other options.

	Core SD-WAN Features	Optional SD-WAN Features*	Enterprise-Grade Security	Reduced Network Complexity	Lowest Overall Cost
SD-WAN appliance with <b>embedded security</b>	✓	✓		✓	
SD-WAN appliance with <b>Cloud-based security</b>	✓	✓			
SD-WAN appliance with <b>security appliance in line</b>	✓	✓	✓		
Network security appliance with <b>SD-WAN embedded</b>	✓		✓	✓	✓

\*SD-WAN with a dedicated backbone is an optional feature not required with all deployments.

### WatchGuard SD-WAN

It's only natural that we deliver SD-WAN functionality delivered on our award-winning security platform so you can optimize your networking architecture while maintaining a strong, consistent security posture across your organization.

**WatchGuard SD-WAN features:**

- Dynamic path selection based on real-time link measurements
- Zero-touch deployment with RapidDeploy service
- Centralized management tools including Dimension visibility and reporting
- VPNs for secure transmission over public Internet with failover capabilities



**Best yet, all the value of SD-WAN comes included with your Firebox and active support license – no additional charges apply. You just turn it on to get started!**

Get ready for your SD-WAN deployment by downloading the SD-WAN Buyers Guide at [www.watchguard.com/sdwan](http://www.watchguard.com/sdwan)

