Security, connectivity and control:

The challenges and opportunities of SD-WAN

White Paper

Introduction

For the modern business leader, digital transformation is increasingly seen as the key to growth and competitive advantage. Cloud computing, big data, mobile, social tools and more offer the prospect of building a more agile, innovative, customer-centric and successful organization. It's no surprise that IDC predicts spending on these technologies to grow at a CAGR of nearly 18% to reach $2 trillion by 2020.

Yet legacy wide area networks (WANs) simply aren't set-up to cope with the extra strain of supporting these transformational technologies, costs are mounting and performance to cloud-based applications most often suffers at remote offices. That's forced organizations to take a closer look at their networks and investigate a new model: SD-WAN (software-defined WAN).

SD-WAN offers businesses the opportunity to drive digital transformation projects, providing the connectivity to extend cloud connections out to branch offices and other remote locations and support unified comms, SaaS apps and other business critical services. The result? Faster connectivity, improved control and lower costs. IDC claims the SD-WAN market is seeing "remarkable growth" and its CAGR of nearly 70% will reach over $8bn by 2021.

But as with any new technology implementation, cybersecurity is an ever-present challenge. With SD-WAN, security devices must be put in place at each remote location to deal with internet-based threats. Yet the built-in security capabilities of many SD-WAN appliances are inadequate for today's increasingly advanced threats. With several options to choose from, decision-makers may feel unsure what set-up best suits their needs.

That's where this white paper can help.

Barracuda Network polled hundreds of IT leaders around the world to find out more. We wanted to know how widespread SD-WAN deployments are, how organizations are securing them, what benefits they're seeing and what challenges – if any – persist.

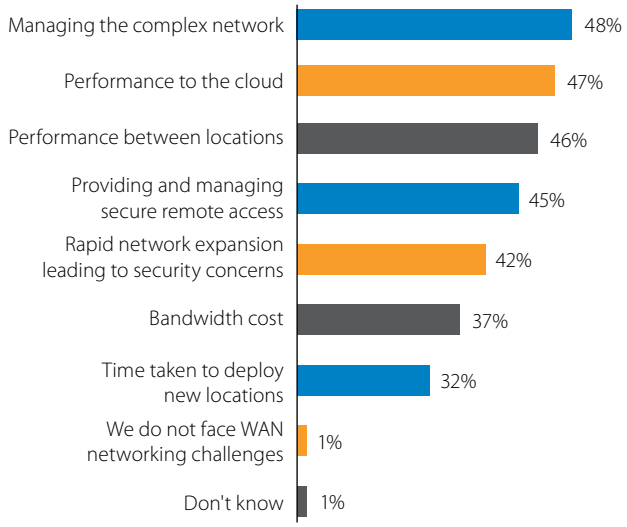
As we'll see, SD-WAN is an increasingly popular option for organizations across many sectors who are struggling to support digital transformation with their current WAN infrastructure. In fact, they're saving millions in costs which would otherwise have been spent on expensive MPLS. With the mitigation of cyber risk a number one concern for these IT leaders, a large number favor deploying advanced security and SD-WAN in one appliance at each gateway edge.

Methodology

We commissioned Vanson Bourne to poll 910 global IT leaders and networking and security professionals in organizations about their security challenges, SD-WAN deployment experiences and concerns over SD-WAN security. Respondents came from companies ranging from 1,000 to 5,000+ employees across multiple sectors, ranging from healthcare, finance and education to manufacturing, public sector and retail.

SD-WAN deployments on the rise

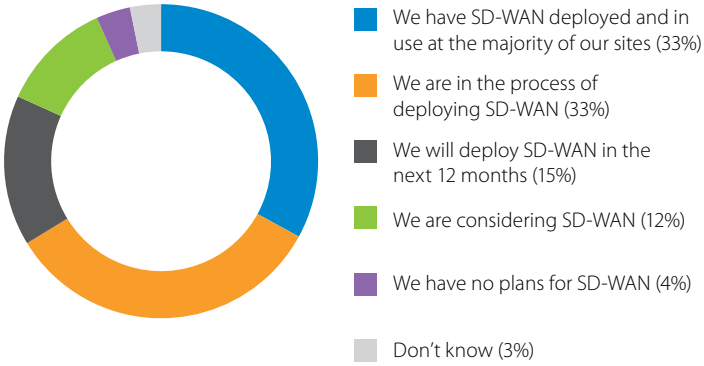
What are the biggest WAN networking challenges facing your organization?



Today's organizations are struggling to manage the explosive growth of WAN traffic resulting from high business demand for cloud applications and services. The public cloud market grew over 28% year-on-year in the first half of 2017 with SaaS accounting for the vast majority (69%). As a result, almost all (98%) respondents we polled cited networking challenges with their current WAN set-up. Complexity (48%), cloud performance (47%) and performance between locations (46%) topped the list. Only 1% of respondents claimed they had no WAN challenges. Yet their focus for projects over the next 12 months — on everything from reducing cybersecurity risks to integrating cloud datacenters, driving automation, expanding to remote locations and adopting IoT — will only increase network complexity.

SD-WAN can provide an effective response for many organizations. It effectively decouples the networking hardware from the means of controlling it, virtualizing the WAN to ease configuration and routing of traffic. With SD-WAN, IT professionals can manage security policies and bandwidth at the push of a button from a centralized location rather than having to send technicians out to configure the network physically. It also adds intelligence, by monitoring the network and prioritizing traffic for mission critical applications. And because SD-WAN routes traffic over the internet, it's cheaper than legacy MPLS, as we'll see.

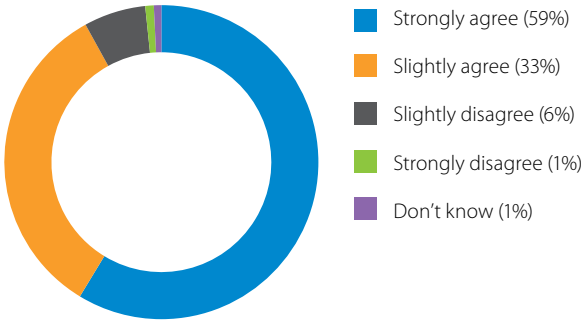
Does your organization have or is it planning to deploy SD-WAN?



These benefits all add up. That's why a third of IT leaders told us they've already deployed SD-WAN in the majority of their sites, while half (49%) are in the process of doing so or will in the next year. In fact, 70% of respondents told us they'd risk losing a competitive advantage if they don't upgrade their WAN.

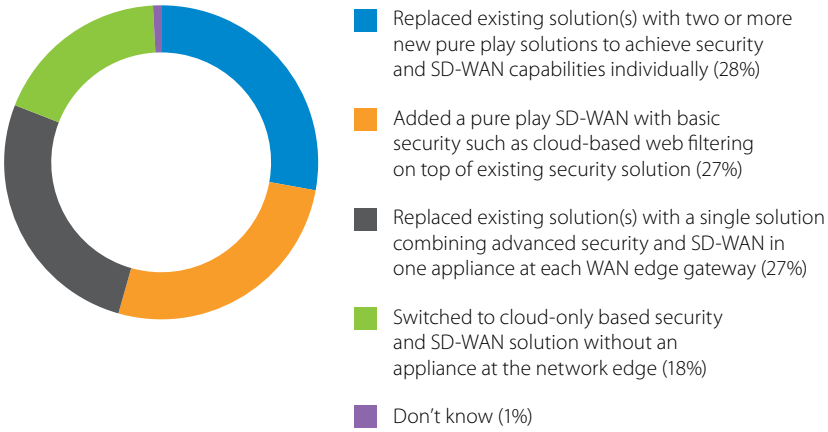
Large numbers of IT leaders favor single-box security

Security should be the number one priority when considering an SD-WAN solution



IT leaders are of course aware of the potential threats facing their organization as they upgrade. An overwhelming majority (92%) agree that security should be the number one priority when considering an SD-WAN solution. Plus, a secure SD-WAN was one of the three most invested in security measures over the past 12 months for around a quarter (25%).

What type of solution did you deploy as part of the SD-WAN rollout in your organization?



Although SD-WAN offers integration with security solutions, organizations could follow one of four different models. Of those that have already deployed SD-WAN:

1. 27% have added a pure-play SD-WAN featuring basic security like cloud-based web filtering or firewalls on top of their existing security. This can provide cost savings and help organizations save on bandwidth costs. But it's a two-box solution, which means less flexibility when it comes to traffic routing, and potential security gaps.
2. 28% replaced their existing solution(s) with two or more pure-play solutions to address security and SD-WAN separately. On paper this would seem to offer the best of both worlds, but it's extremely costly and will incur twice the management overhead as there are effectively two boxes not talking to each other.
3. Only 18% chose to switch to a cloud-only security and SD-WAN solution without an appliance at the network edge.

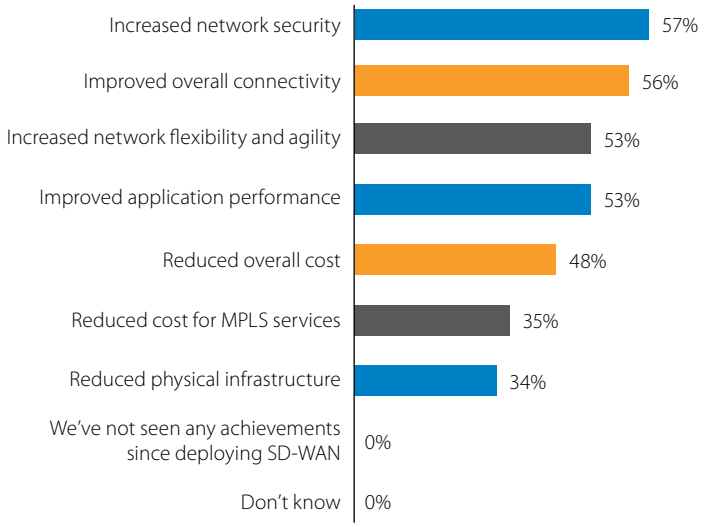
   It seems that, despite the hype over cloud-managed SD-WAN, organizations are eschewing this option. Why? Three-quarters (72%) said they are "very concerned" about disclosing confidential data like VPN credentials to a cloud-managed SD-WAN vendor. What's more, 57% said regulatory compliance prevents them from rolling-out cloud-managed SD-WAN solutions globally, while 62% said the same for cloud-hosted solutions.
4. Over a quarter (27%) replaced their existing solution with a single solution combining advanced security and SD-WAN in one appliance at each gateway edge: the option Barracuda Network provides via its CloudGen Firewall.

When it comes to their stated preference, a much larger number (42%) claimed they would favor an easier-to-administer single-box solution with the best possible security and SD-WAN connectivity and can compromise on single line WAN optimization capabilities. It's also the most popular option for those planning to deploy or considering SD-WAN (31%). Seeking out a trusted provider to offer advanced capabilities is key: 81% said advanced threat protection and centralized management was very important or crucial to their SD-WAN purchase.

Combining security and SD-WAN in one appliance can be a lower cost, more flexible and easier to deploy option — the latter benefit being especially important in remote locations. It's notable that 60% of respondents that deployed this type of solution said their main achievement was improved application performance, much higher than for those who chose the other options. Plus, over 58% claimed increased network flexibility and agility was their biggest win: again, higher than for any other deployment type.

SD-WAN offers improved security and lower costs

What have been your organization's main achievements since deploying SD-WAN?



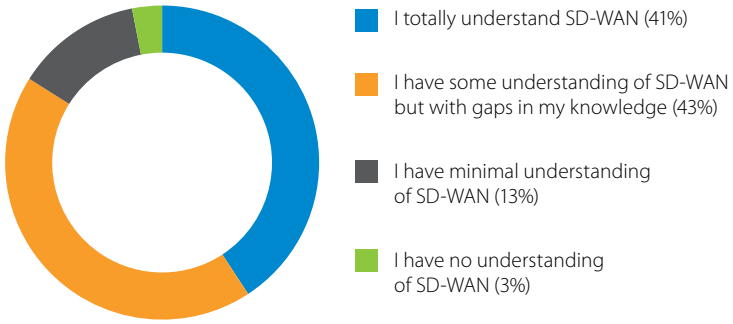
It's good to see SD-WAN is living up to its billing, with 99% of respondents claiming to have seen benefits from their implementation. Most common is improved network security (57%), followed by connectivity (56%) and improved network flexibility and agility (53%). With the right type of solution in place it's certainly possible to enhance legacy security, although organizations must also consider the trade offs with some of the models highlighted above. For the best chance at increased flexibility and agility plus maximum security, a single-box solution should be favored.

Even better: nearly half of respondents said they'd reduced overall costs thanks to SD-WAN, while over third (36%) had reduced costs specifically for MPLS services. Organizations estimate they could **save over $1.3m on MPLS networking costs** across a 12-month period by deploying SD-WAN.

The notoriously high per-megabit costs of MPLS become particularly unsustainable to run for increasingly popular but bandwidth-heavy services like videos, cloud applications, IoT and augmented/virtual reality applications. This is where SD-WAN offers a great alternative, allowing organizations to intelligently route that traffic over much cheaper internet broadband links.

Skills challenges persist

How much understanding do you have around SD-WAN technology?



Although overall understanding of SD-WAN appears to be good, a sizeable minority of respondents (43%) admitted gaps in their knowledge. Why is this an issue? Because it could be restricting the choices they make on security and even their ability to roll-out the technology to remote locations.

Over a third (35%) of those organizations that don't currently have SD-WAN admitted that one of the biggest barriers to investing in it is their lack of in-house capability to deploy, and 24% claimed it's because they don't know enough about it. Even organizations with SD-WAN often face internal skills shortages and a lack of understanding how to deploy (37%). Nearly two-thirds (64%) think there isn't enough training or education on SD-WAN deployment in their organization.

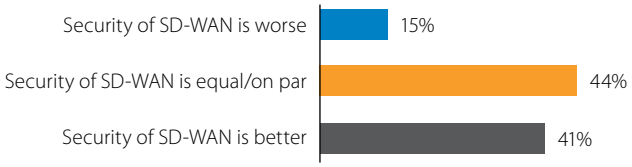
Given the huge benefits we've outlined for SD-WAN, it's clearly important for organizations to improve their technical know-how, especially in remote locations where security needs to be deployed. Failure to do so may allow their competitors to gain an advantage, or in a worst-case scenario result in them implementing SD-WAN insecurely or in a way that incurs extra cost and management overheads.

Reducing skills gaps is a challenge for the entire industry, especially in IT security, where shortages are predicted to reach 1.8m professionals globally by 2021. That's why it's good to see 56% of respondents claiming they invested in training following an SD-WAN deployment while 50% hired external experts. A single-box solution could arguably require less manpower to operate and deploy than the other appliance-based options, enabling firms to maximize their limited resources.

The cost of new equipment and services was cited as another top barrier to SD-WAN deployments, although it must be remembered that single box solutions are far more cost effective than others.

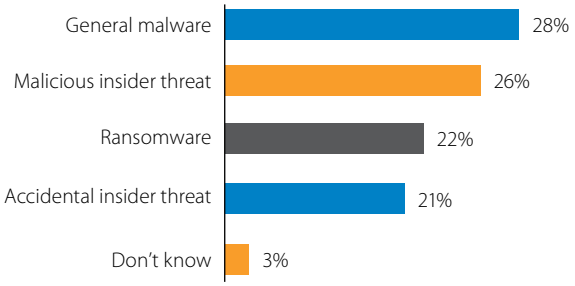
Respondents back security of SD-WAN but remain cautious

How would you rate the security of your organization's SD-WAN solution in comparison to your organization's corporate firewall/VPN solutions?



The good news is that the vast majority (85%) of those organisations that have already implemented SD-WAN believe that its security is equal to or better than their corporate firewall/VPN solution. That's what we want to see. SD-WAN offers intrinsic benefits over legacy networks in that traffic is end-to-end encrypted by default, while its software-defined architecture allows for security and policy to be integrated into connectivity. However, organizations must find the right security model and provider to drive ROI.

What have been your organization's main achievements since deploying SD-WAN?



Respondents are rightly aware that there are new threats to consider with SD-WAN. That's why 72% are very or extremely concerned about their network becoming more vulnerable after deploying it. While organizations have historically secured their WANs centrally in the datacenter, providing direct internet access at each remote location comes with its own challenges. Respondents saw malware (28%) as the biggest, followed by malicious insiders (26%), ransomware (22%) and accidental insiders (21%).

These concerns are understandable. After all, insider threats were blamed for over a quarter of data breaches last year, according to Verizon, while ransomware, zero-day threats and sophisticated targeted attacks are a constant threat for firms.

However, these threats can be tackled with the right security implementation, deployed at each remote location. By leveraging a one-box solution containing not just URL filtering, IPS and stateful firewall but also advanced sandboxing, organizations can reap the benefits of SD-WAN safe in the knowledge they are protected from even the most sophisticated threats. That's the peace of mind you need to drive digital transformation.

Conclusion

Organizations across the globe are turning to SD-WAN to help upgrade their networks for the digital age. In so doing, they can become smarter about how they manage traffic, while cutting costs compared to MPLS and reducing the operational burden on stretched networking teams. Security understandably remains the number one priority when implementing these new networks. And although IT leaders are split on what kind of security set-up works best for them, increasing numbers are favoring a single box solution combining advanced security and SD-WAN in one appliance at each gateway edge. It's by far the best choice for those who prioritize application performance and network flexibility and agility.

Virtually all organizations that have implemented SD-WAN have already seen benefits, with improved security and major cost reductions leading the way. But persistent skills challenges must be tackled to remove any lingering barriers to secure deployment of SD-WAN.

Finally, it's reassuring to see IT and security professionals aware of the potential risks associated with implementing SD-WAN. That's what makes it so important to find the right security model and provider. Done right, security can help organizations drive digital transformation and growth on the back of more efficient, intelligent and cost-effective networks.

How Barracuda CloudGen Firewalls help implementing Secure SD-WAN:

Barracuda CloudGen Firewalls combine full next-generation security including Advanced Threat Protection with advanced SD-WAN capabilities in a single box solution that allows customers to experience vastly reduced line costs, to increase overall network availability, to improve site-to-site connectivity and to ensure direct uninterrupted access to applications hosted in the cloud from any remote location.

Comprehensive Central Management and a rich feature set including true Zero Touch Deployment, Dynamic Bandwidth Measurement, Performance Based Transport Selection, and our own powerful TINA VPN protocol make Barracuda's CloudGen Firewalls the perfect fit for today's dispersed network architectures. All of this is available as hardware platform, virtual or even cloud based with no need to divulge VPN credentials - ever. For more detailed information visit www.barracuda.com/SD-WAN.

SS Labs Inc., recognized globally as the most trusted source for independent, fact-based cybersecurity guidance, independently tested the Security- and SD-WAN capabilities of Barracuda CloudGen Firewalls. Details are available with NSS Labs: www.research.nsslabs.com/reports.

About Barracuda Networks

Barracuda simplifies IT with cloud-enabled solutions that empower customers to protect their networks, applications and data regardless of where they reside. These powerful, easy-to-use and affordable solutions are trusted by more than 150,000 organizations worldwide and are delivered in appliance, virtual appliance, cloud and hybrid deployments. Barracuda's customer-centric business model focuses on delivering high-value, subscription-based IT solutions that provide end-to-end network and data security. For additional information, please visit barracuda.com.

Barracuda

Barracuda Networks
3175 S. Winchester Boulevard
Campbell, CA 95008
United States

t: 1-408-342-5400
1-888-268-4772 (US & Canada)
e: info@barracuda.com
w: barracuda.com