



James Eibisch

November 2022

An IDC White Paper sponsored by GTT

IDC#EUR149843222



Realizing the Full Potential of SD-WAN

Introduction

Right now, enterprises are facing what IDC terms the Storms of Disruption: waves of interconnected economic, political, and social disruptions that will threaten businesses around the world for the next several years.

The macroeconomic situation is rapidly shifting and increasingly unpredictable. A shortage of skills is hampering companies' efforts to become truly digital enterprises. Supply chains are under threat from continuing closures and lockdowns. Inflation is biting the global economy. And the Russia-Ukraine war is disturbing energy and food markets and the movement of goods.

Faced with this global disruption, it is imperative for organizations to maximize the utility and value of their technology infrastructure and to ensure it is fully secured and optimized.

Networks need to support businesses in their move toward a cloud-native, digital-first, hybrid-working mode of operation, while ensuring flexibility and cost optimization to cope with the economic turbulence ahead.

SD-WAN has been the future of networking for several years. Now it is mature and a cornerstone of network transformation: IDC forecasts that worldwide spending on managed SD-WAN services will grow 21% per year to reach over \$15 billion in 2026.

But IDC's research for this White Paper among 650 U.S. and European organizations (of over €200 million in revenue and operating in at least two countries) finds that with rapid growth come growing pains. Initial SD-WAN deployments have grown in scale and complexity as they support a growing proportion of the business, and early solutions need a refresh. At the same time, networking and security are converging both technologically and organizationally, and the decision to entrust your network to a managed service provider or manage it yourself is more critical than ever.

This IDC White Paper on behalf of GTT explores what options enterprises have to take their use of SD-WAN to the next level and get the most out of their investment.

Conclusion

SD-WAN is maturing and taking on a growing proportion of enterprises' critical networks and applications. Its openness and flexibility means that organizations can build and secure networks in more ways than ever, resulting in a wide diversity of approaches being taken. This increases

AT A GLANCE

KEY STATS

- » 47% of U.S. and European organizations have deployed or are deploying an SD-WAN solution.
- » Improving network security is companies' top WAN-related priority.
- » Three quarters of enterprises use or will use a managed service.
- » Skills are the major challenge for businesses that self-manage their SD-WAN.

KEY TAKEAWAYS

SD-WAN's openness and flexibility is its great strength. Enterprises can build and secure networks in many ways, leading to a wide diversity of approaches.

So many choices, along with SD-WAN's growing maturity and scale, brings complexity. Managed services can help mitigate the complexity for a company while providing a range of additional benefits.

the level of complexity, and therefore increases the need to engage with expert partners to ensure that SD-WAN is implemented and managed optimally and securely to deliver the greatest advantage.

What Matters? Leading Business and Network Priorities

Organizations are responding to the global conditions outlined above in many ways, some specific to their industry or individual circumstances, some universal. We asked companies to identify their current top priorities for the business overall, and for their WAN specifically.

The left-hand column of Table 1 shows that the top three priorities for the business as a whole are: developing a data strategy in order to becoming a data-driven company; progressing their digital transformation; and addressing cost and inflation pressures. It is a sign of the economic times that cost concerns — always important but in recent years rarely in the lead group of priorities — are now near the top of the list.

TABLE 1

Top Business and WAN Priorities

Q. Which of these issues is your organization working on most intensively right now?

Q. Currently, what are your organization's most important priorities relating to the WAN?

Rank	Business Priorities	WAN Priorities
#1	Becoming a data-driven business	Improve security on the WAN
#2	Becoming a digital company	On-demand connectivity
#3	Reduce cost	Hybrid network architecture
#4	Product innovation	Improve application performance
#5	Customer experience	Internet-first strategy
#6	Business growth, market share	Reduce cost
#7	Support hybrid working	Improve access to cloud providers
#8	Agility, speed	Support more access technologies
#9		Improve resilience/availability

Note: n=650 (all companies)

Source: IDC/GTT, 2022

Data and digital are foundational initiatives: how companies will operate and grow in the future depends on them. However, although they are connected, they are not at the same level of maturity. In our survey, companies that are prioritizing digital tend to have "lagging" characteristics. For example, they have low digital maturity, are more likely to have no plans to use SD-WAN, and those that do use SD-WAN are more likely to still be on their first generation of solution.

Companies that are prioritizing data, on the other hand, have higher digital maturity and are more likely to have migrated their network fully to SD-WAN and to be using a second or later generation SD-WAN solution. More advanced companies are further ahead in their digital transformation and are moving on toward a data-driven strategy, while less advanced companies started later on their digital initiatives and are currently catching up. Digital strategy precedes data strategy.

In both cases, SD-WAN is a marker of technological maturity. We see this throughout the research: organizations that are most advanced in their use of technology to solve business problems also tend to be more advanced in their use of SD-WAN.

Companies also identified priorities relating to their WAN. Most of the issues relate directly to modernizing networks to support and optimize current and future workloads and applications. For example, on-demand connectivity for usage-based network consumption reflecting the cloud-based resources being accessed; hybrid network architecture to increase the flexibility of network provisioning and cost efficiencies; and improved access to cloud providers to connect to the growing networks of applications and services distributed within and between clouds. These are surefire wins for SD-WAN, and some of its main growth drivers.

Lastly, improving network security is the top WAN priority. Security is always critical, but the mix of technology changes, such as shifting to a hybrid work environment and the demand for digital-first business, plus the economic conditions we face today present a heightened level of threats. However, the options available to enterprises for securing networks and IT in an SD-WAN deployment are growing rapidly and making the right choice of vendors and partners can create a secure environment.

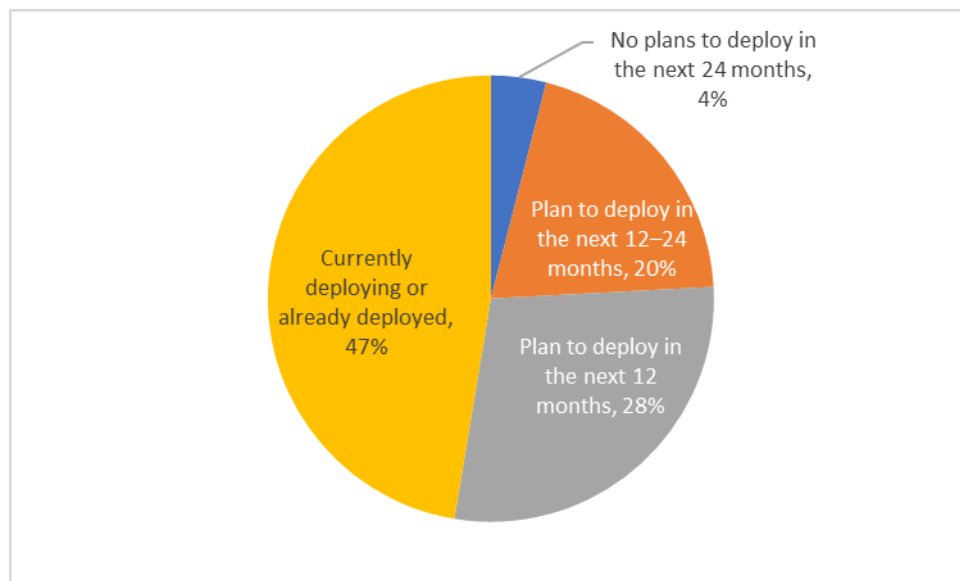
One Size Does Not Fit All: Enterprises Take Multiple Approaches to SD-WAN

Compared with earlier WAN technologies, SD-WAN is extremely flexible and open. That is its great strength and the driver for its rapid growth, range of use cases, and increasing maturity. SD-WAN solutions can be implemented and managed in many ways, and we see great diversity in the approaches that enterprises are taking in how they source connectivity, choose a management model, deploy security, and many other aspects.

How many companies are using SD-WAN today? Among the 650 we interviewed across Europe and the U.S., almost half have already deployed or are currently deploying an SD-WAN solution. Most of the remainder plan to start using SD-WAN within two years, and only a very small minority have no plans within that timeframe. In total, 96% of organizations already use, or will soon use, SD-WAN.

FIGURE 1
Half of Companies Already Use SD-WAN

Q. Does your organization currently use, or plan to use, an SD-WAN solution?



Note: n=650 (all companies); numbers may not sum to 100% due to rounding

Source: IDC/GTT, 2022

As part of the research, we categorized companies that took part in the survey as technology leaders, followers, or laggards based on their responses to questions including their level of digital maturity and how well their networks are supporting their business priorities, with the aim of identifying best practice among the most advanced companies.

We find that SD-WAN use correlates with technology leadership in a clear pattern: the higher up the technology leadership scale a company is, the more likely it is to already be using SD-WAN. We believe this is more than correlation: SD-WAN enables digital applications and workflows flexibly across the organization that help boost companies into the technology leader category.

That's a snapshot of where companies are today. Figure 2 shows three views of where they are in their SD-WAN journey over time. Individual companies can use this chart to measure their own maturity by plotting where they are on each line. Given the association between SD-WAN use and technology leadership, companies that consistently place at the low end could take that as an indication to check their overall technology strategy and maturity against peers to avoid losing advantage. For example, a company that delays migrating from, or implementing SD-WAN over, an existing MPLS network will be at a relative disadvantage compared with faster moving competitors in terms of efficiently accessing cloud services and getting the full cost advantage of hybrid networks.

- **Extent of SD-WAN deployment** — SD-WAN users are fairly evenly split in terms of the reach of their implementation within their organization. Smaller companies and those that self-manage their network (“DIY” users) tend to run limited-reach networks, while larger companies and those that use managed SD-WAN services have deployed more

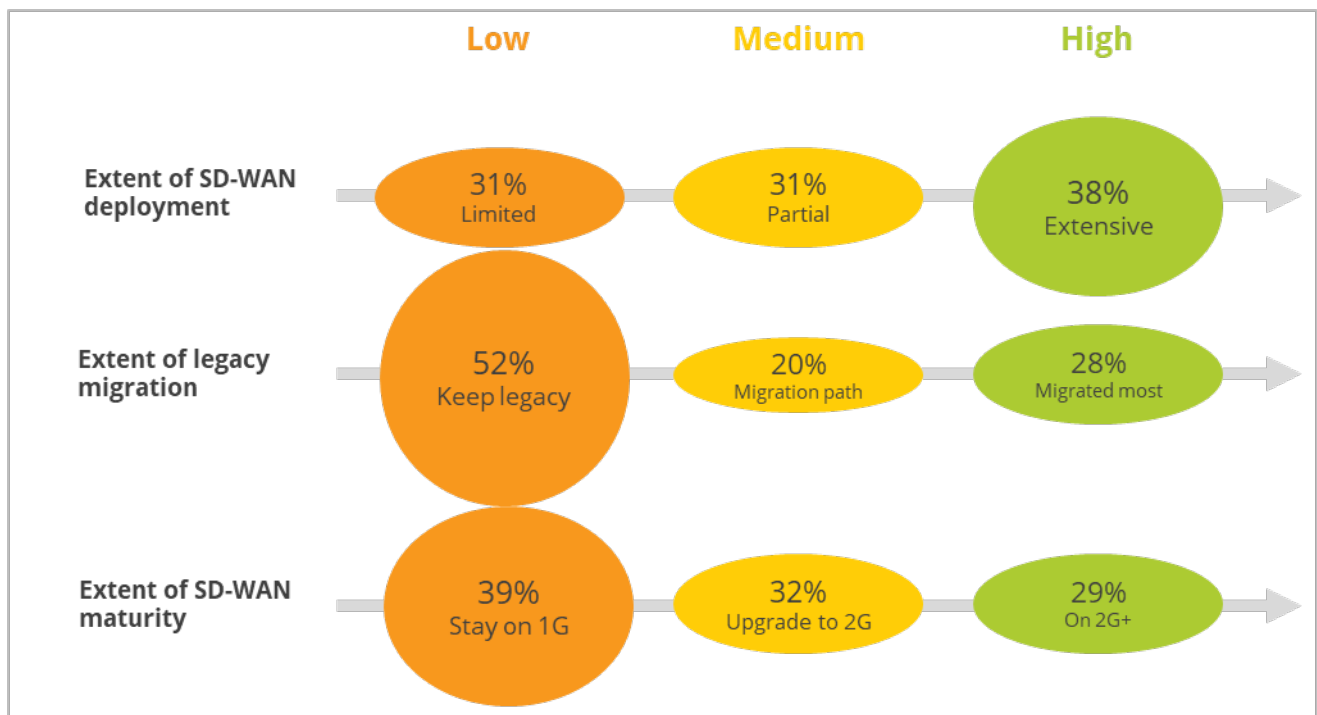
extensively. This is a sign that companies may find it difficult to scale up DIY networks that we will revisit below.

- **Extent of legacy migration** — Half of all companies in the survey plan to keep their existing networks relatively untouched over the next two years, many of them using SD-WAN for new deployments but not actively migrating the legacy base. The other half are actively migrating, and a small minority of 8% have already completed the process.
- **Extent of SD-WAN maturity** — Most SD-WAN users are still on their first-generation solution, with about half of those unlikely to upgrade within two years (disproportionately DIY users). Around a third (primarily the technology leaders) are already on their second or later generation.

The figures in this chart are moving to the right over time, toward greater SD-WAN use. At a minimum, companies should ensure that they keep up with the pace of migration within their industry, understanding that SD-WAN, along with other services like multicloud overlays and hyperscaler cloud WAN services, will increasingly take over from today's installed base of legacy networks.

FIGURE 2
SD-WAN Maturity Snapshot: Most of the Potential Still Lies Ahead

- Q. What is the extent of SD-WAN deployment within your organization?
- Q. Overall, which best describes the status of your organization's WAN today?
- Q. Where is your organization in its SD-WAN deployment journey?



Note: n=308 (companies that currently use SD-WAN), 650 (all companies), 308 (companies that currently use SD-WAN)

Source: IDC/GTT, 2022

So, the state of SD-WAN use has moved on significantly over the last 2-3 years, even over the last 12 months. Aside from general sentiments about agility and scalability, what is driving organizations to adopt it? As it matures, companies are using SD-WAN for an increasingly diverse set of purposes. It is no longer just a more flexible approach to networking; it is a cornerstone of a modern application-centric technology environment.

Survey respondents told us why they use or plan to use SD-WAN. As with many aspects, the reasons are diverse and wide ranging, and no single one stands out as a universal touchstone. Instead, drivers are spread across the following categories.

1. Creating an overlay that abstracts and spans multiple networks, providers, and IT environments

- *“Centralized or automated network management across the WAN or multiple networks”* — Abstracting the network underlay while providing centralized and programmable management creates consistency across disparate networks: Internet, MPLS, Ethernet, 4/5G, etc.
- *“Gain independence from our main network operator(s) through self- or co-management”* — SD-WAN decouples the network from the network provider, loosening ties to incumbent operators. The ability to self-manage or co-manage with a range of third parties creates further independence.
- *“Improve optimization of multicloud or hybrid IT architectures”* — Connecting disparate cloud and IT environments over disparate networks while responding to application-level requirements is only practical with SD-WAN.

2. Reducing cost, complexity, and time to serve

- *“Opportunity to save money or reduce TCO”* — While cost reduction is not the most important factor in using SD-WAN and the cost benefit over MPLS in major markets can be slim, it will become more pressing over the coming years. Opportunities to mitigate cost will grow as new competitive underlay networks are rolled out.
- *“Reduce quantity and complexity of IT support”* — Centralized and increasingly automated management reduces the support burden. But even so, it takes considerable resources and skills to run production networks in-house and companies should go into a DIY deployment with realistic expectations.

Large Europe-headquartered global dairy producer: “Over the next 3–4 years we don’t want to do DIY. We don’t want a big skills requirement in-house right now — we want to outsource.”

- *“Faster network deployment and provisioning”* — Pre-integrated, auto-configuring SD-WAN devices and cloud-based SD-WAN services reduce the time to connect new sites dramatically, assuming availability of underlay connectivity.

3. Addressing strategic technology imperatives: cloud, security, and user experience

- *“Access cloud direct rather than through our MPLS network”* — Cloud access is critical to the modern enterprise, and needs to be efficient, flexible, functional, and secure.
- *“Ability to improve and integrate network security”* — Improving security is the top WAN-related priority that companies have, and SD-WAN provides the platform for the ongoing convergence of networking and security: 39% of companies regard Secure Access Service Edge (SASE) as a high priority and about the same number have already integrated their networking and IT security teams. In addition, the range of security functions from multiple vendors allows enterprises to explore many options across best of breed and integrated approaches, without being locked into a single vendor or network provider.
- *“Better application performance or end-user experience over the WAN”* — Application-specific routing policies and SLAs, as well as dynamic routing over available access circuits, make SD-WAN a good fit for delay-sensitive applications.

*U.K.-headquartered global travel food service operator:
“Our business depends on how fast we can get new sites
connected. With auto-configuring SD-WAN devices we deployed 37
locations in just three hours.”*

Diversity underpins SD-WAN. Along with these varied reasons driving SD-WAN use, companies have a wide choice of partner/service provider, a choice of deployment models, and a growing choice of approaches to security, among other options. As a result, they are taking a wide variety of approaches to implementing SD-WAN solutions.

This multiplicity of approaches, alongside SD-WAN’s growing maturity and scale within organizations, creates complexity. Consequently, enterprises face challenges on multiple fronts, depending on the approaches they’re taking, that are experienced in almost equal measure across the user base.

TABLE 2
SD-WAN Implementation Throws Up Diverse Challenges

Q. What were the main challenges encountered by your organization when the SD-WAN was implemented?

Rank	Challenge
#1	Challenges related to management of the solution
#2	Challenges related to managing multiple partners
#3	Applications were not optimized as expected
#4	The underlying technology partner did not deliver to expectations
#5	A managed services partner did not deliver to expectations
#6	Integration issues
#7	Network performance, reliability, or resilience were not delivered as expected
#8	Expected cost savings were not realized
#9	Security expectations were not met

Note: n=308 (companies that currently use SD-WAN)

Source: IDC/GTT, 2022

The good news is that while security and cost are top business and WAN priorities, overall, they are the least of the challenges faced when implementing SD-WAN. However, the story differs markedly between groups of SD-WAN users, as the following section explores.

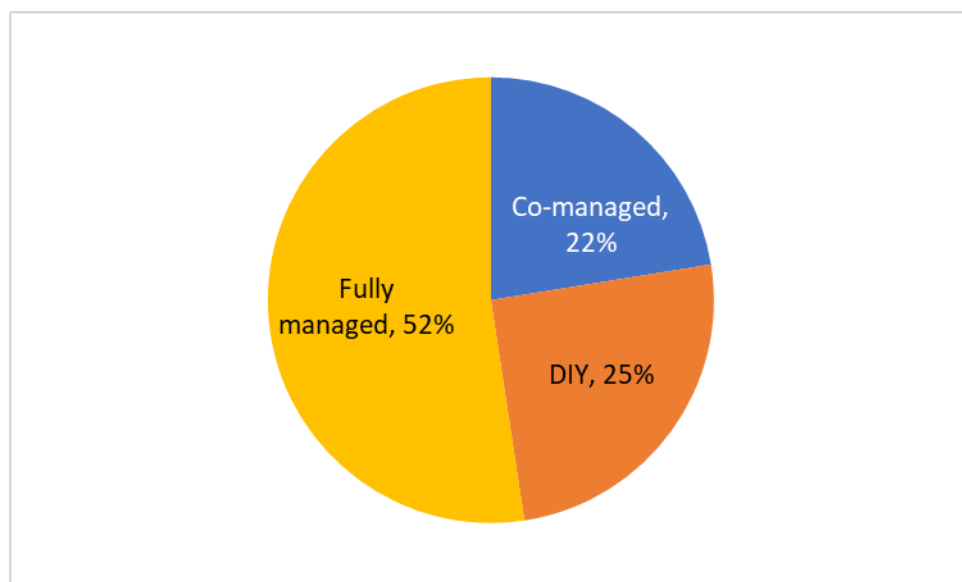
Managed Services Address Key Challenges

Possibly the most significant choice an enterprise will make regarding its SD-WAN is whether to self-manage it in a DIY model or to use a fully or co-managed service.

Choice of deployment model matters. It affects nearly every aspect of the solution: network management, connectivity sourcing, cost model, buying power, security, skills requirements, and many others. Companies considering SD-WAN, and those with current deployments that they need to scale or that are not meeting expectations, should assess very carefully which deployment model is right for them.

FIGURE 3
SD-WAN is Primarily Delivered as a Managed Service

Q. How does (or will) your organization manage the SD-WAN solution?



Note: n=624 (companies that currently use SD-WAN or plan to within 2 years); numbers may not sum to 100% due to rounding
Source: IDC/GTT, 2022

SD-WAN solutions are typically managed in one of the following ways:

- **Fully managed** — The most popular form, whereby a service provider (which may or may not own a network) takes responsibility for operating and managing the solution, sourcing equipment and connectivity, and meeting SLAs.
- **Co-managed** — The enterprise manages certain aspects of the solution via self-service tools, such as routing or security policies, but daily operations are supported by a managed service provider.
- **DIY** — The enterprise takes on the work a managed service provider would do, as well as procuring the skills needed to do so.

Which model a company chooses depends on that careful assessment of their needs as well as their overarching IT strategy, availability of skills, the specific requirements of the network, and their historical practice and preferences.

Note that a quarter of enterprises are, or expect to be, DIY, but there's a significant difference between current and future users: 30% of organizations that plan to implement SD-WAN expect to manage it themselves. For those already running SD-WAN solutions today, the figure is 20%. We'll come back to that after looking at some of the details of both deployment models.

DIY: a valid option but not to be undertaken lightly

A significant minority of SD-WAN users operate in DIY mode, contracting with network providers primarily or only for connectivity. For small or simple networks involving a small number of access and underlay providers, or for environments that can tolerate a level of downtime or brownouts, it isn't too difficult to make this support strategy work well: the company controls the network itself and can tailor it precisely to its needs.

Where these constraints are not acceptable, a company that wants to run its own enterprise-scale, enterprise-grade network must invest in substantial resources and skills. However, skills are in short supply, an economic downturn impedes new investment, and focused, well-funded service providers are likely to remain one step ahead. The days of banks, for example, employing large IT teams that essentially duplicate standard service provider offerings for little additional benefit are over. Unless a company needs an unusually high degree of customization or control, possibly due to the specialized nature of its business or operations, it is generally better off buying standard infrastructure services and using its own resources to create value on top.

TABLE 3
DIY SD-WAN Creates Challenges Around Skills and Scale

Q. What are the main challenges of managing the SD-WAN and related security solutions in-house?

Rank	Challenge
#1	Finding and securing IT/network staff with the necessary skills
#2	Not being able to negotiate as well as an MSP can with vendors and connectivity providers
#3	Keeping up with technical or market developments
#4	Converting from capex to opex
#5	Retaining IT/network staff
#6	Speed of resolving faults or making changes to the solution
#7	Having to pay a premium for skilled IT/network staff
#8	Operating a helpdesk with 24x7 support and local language
#9	Staying up to date on evolving cybersecurity threats and tools

Note: n=157 (companies that use or plan to use SD-WAN and manage or expect to manage it themselves)
Source: IDC/GTT, 2022

The challenges that DIY users report bear this out. In particular:

- **Skills** — This is a major issue in terms of finding and hiring, paying for, training, and retaining. In modern networking as in other tech areas like AI/data, cloud, and cybersecurity, there simply aren't enough experts to go round. Inevitably, they become concentrated in technology and service firms, building platforms and services that are sold and consumed as-a-service.
- **Scale** — Very few enterprises can match the negotiating and buying power that major service providers have with vendors, local access providers, and other network operators. This is a particular issue with SD-WAN as it tends to lead to a greater number and diversity of underlay networks from different providers. As a result, companies can easily struggle to keep costs on track and to manage a growing set of suppliers.

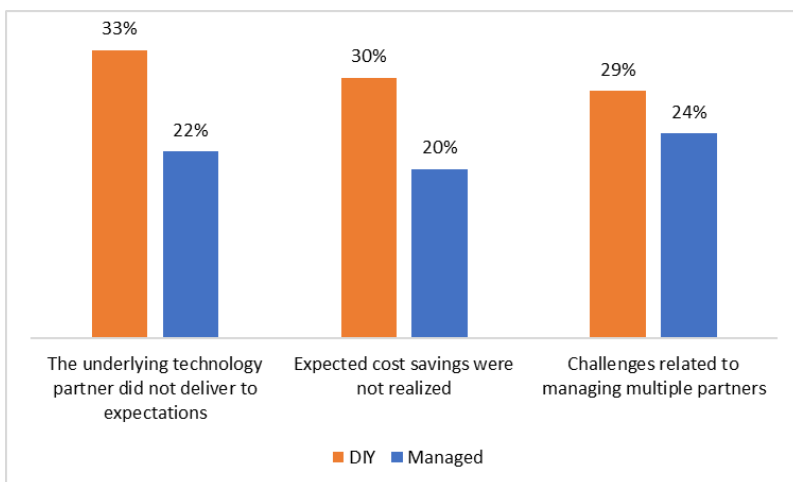
In addition, many of these DIY challenges clash directly with companies' top WAN-related priorities outlined earlier, including improving network security, diversifying the network with hybrid architectures and more access technologies, and reducing cost.

We can now pick up on the point above that SD-WAN challenges differ between groups of users. Figure 4 shows that companies that self-manage their SD-WAN experience significantly greater problems than managed service users in their ability to manage partners and get satisfactory performance from them, and in achieving the level of cost reduction they anticipated would result from the SD-WAN solution.

In fact, more DIY than managed service users identified with all but one of the challenges we asked about. The exception was problems relating to integrating the SD-WAN with existing systems. However, as SIs are a common managed service partner, it is possible that they deepen the average level of integration effort across managed service engagements compared with DIY, creating more opportunities for integration-related problems to occur.

FIGURE 4
DIY Users Report More Challenges Across the Board

Q. What were the main challenges encountered by your organization when the SD-WAN was implemented?



Note: n=308 (companies that currently use SD-WAN)
Source: IDC/GTT, 2022

Managed services pick up where DIY leaves off

In principle, a managed services engagement and a DIY implementation may differ little in terms of technology. The benefit of managed services comes from how the technology is managed and supported, the skills and resources applied, and the additional services available. It isn't a stretch to say that every challenge faced by DIY users in Table 3 is addressed by managed services. Most of them are integral service provider capabilities:

- **Skills** — finding, hiring, and retaining scarce network and security skills
- **Negotiating power** — dealing with vendors and access/backbone providers
- **Support** — operating 24x7 support in local language

The 75% of SD-WAN users that employ a managed service identified their main reasons for doing so as opposed to managing the network themselves (Table 4).

TABLE 4
Managed Services Deliver Compelling Benefits

Q. What are the main reasons for using a managed SD-WAN service as opposed to managing it in-house?

Rank	Reason for Managed Service
#1	Helpdesk support (e.g., 24 x 7, local language)
#2	Visibility, insights, and control without the need for technology certification
#3	Ease of configuration management
#4	Manage, maintain, and facilitate technology upgrades
#5	Better protection against security threats
#6	The SD-WAN is continuously optimized for network performance
#7	Reduce operational costs
#8	Transfer technology risk or capital investment to an external party

Note: n=467 (companies that use or plan to use an SD-WAN managed service)

Source: IDC/GTT, 2022

Some of these reasons are the inverse of DIY-related challenges, but some are unique, such as providing better protection against security threats. Security is such a critical issue that companies can't afford to make do or rely on best effort. And the companies that rate security as a reason for using managed services most highly are the most advanced. Within the survey they are the technology leaders, the largest enterprises, those with the largest networks, and those with the closest integration between networking and IT security teams. These are the organizations most capable of running security themselves, yet they are the ones most drawn to managed services because of the security capabilities that service providers can offer.

Aside from security, enterprises turn to managed services for day-to-day operations that would otherwise tie up staff better employed in more valuable work, and to tap into the platforms and expertise that service providers have built up over time that are costly and difficult to implement in-house. Monitoring and upgrading a large estate of devices, maintaining relationships with a large number of vendors, and providing a global 24x7 helpdesk supporting all languages needed, for example, are simply not practical for most companies and, consequently, simply not done.

One last comparison between managed services and DIY solutions adds a further insight into the outcomes of both approaches. Within both country and industry samples in the survey, companies' use of managed services correlates with how well their networks support their overarching business priorities. Conversely, the use of DIY solutions is negatively correlated. For example:

- **Nordic organizations** report the highest level of managed services and lowest level of DIY. At the same time, their networks provide the highest level of support for their business priorities.
- **Austrian companies** are lowest for managed services, highest for DIY, and their networks achieve the lowest level of support for their top business priorities.

This should not come as a big surprise. Delivering a technological foundation that aims to support CEO-level business outcomes such as agility, innovation, and digital transformation is far from easy, and it is about far more than just the technology, as described above.

Finally, returning to the earlier point that 30% of SD-WAN planners expect to be DIY but only 20% of actual users are. This indicates a sizeable proportion of companies that intend to manage the network themselves switch to some form of managed service during or after implementation. This is plausible given the finding that DIY users in practice face significant challenges relating to cost, manageability, and partner management.

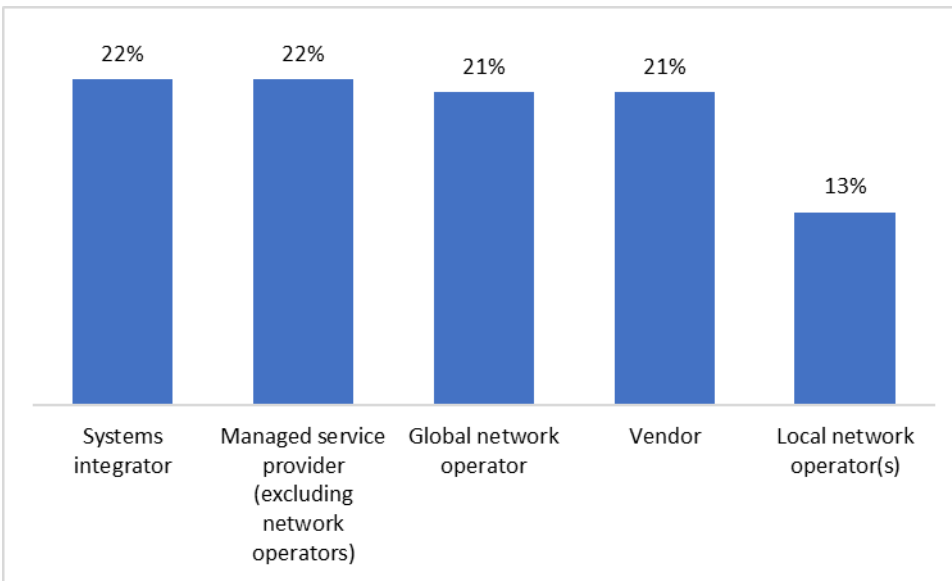
DIY can certainly work for some companies, but equally certainly not for all that attempt it.

What to look for in a managed service provider

Enterprises that use a managed service partner with a range of service provider types. Again, many options are equally popular, and none stands out particularly. Figure 5 shows that SIs, MSPs, vendors, and global network operators claim approximately equal shares. Local network operators are lower, possibly reflecting the fact that all companies in the survey were multinational (operating in at least two countries).

FIGURE 5
Enterprises Use a Variety of SD-WAN Managed Service Providers

Q. What type of service provider manages your organization's SD-WAN and related security today?



Note: n=245 (companies that use an SD-WAN managed service); numbers may not sum to 100% due to rounding
 Source: IDC/GTT, 2022

Companies choose a provider for a variety of reasons: existing relationships, influence from other partners, the nature of the broader engagement, and so on. Each type has its strengths and weaknesses, but for SD-WAN and network security implementations, a provider that owns and operates an IP network has some clear advantages. They own at least part of the underlay and can integrate it with the SD-WAN solution at a fine level. And they can draw on long-standing, peer-level relationships with network vendors, local access providers, and other carriers.

Europe-headquartered global machine parts supplier: “Cost is always a factor, but not the most important. GTT, our managed SD-WAN provider, had the best technical solution, good account team and project management, global footprint, and the ability to execute.”

Table 5 shows the main criteria that enterprises use to select an SD-WAN managed service provider. While the list includes some strengths of each type of provider, the most important to enterprises is that the provider owns, or at least operates, the underlay network. And on a global scale. Multinational network operators that can meet other criteria in the list as well, such as consulting and professional services, industry solutions, and a strong security proposition, are potentially strong candidates for an SD-WAN engagement.

TABLE 5
Network Ownership and Global Reach are Key in Choosing a Managed Service Provider

Q. What are the most important criteria for your organization when selecting a managed SD-WAN provider?

Rank	Criterion
#1	They are responsible for operating the underlying network
#2	Ability to provide a global service with a single point of contact
#3	Deep industry expertise
#4	They can provide consulting and professional services
#5	Support for a wide range of SD-WAN and security vendors
#6	Flexible commercial/billing options
#7	A full range of other network services (e.g., MPLS, internet, private line)
#8	Depth and quality of security offerings
#9	Close partnerships with cloud providers

Note: n=467 (companies that use or plan to use an SD-WAN managed service)

Source: IDC/GTT, 2022

Like any potential provider, though, they need to demonstrate a wider set of capabilities and characteristics: continuous optimization of the solution, technical support, account management, customer-centricity, agility and flexibility, ability to hire and retain skills, a good digital experience, and many more.

France-headquartered global retail services company (on choosing an SD-WAN managed service provider): "Cost was low but not the most important factor. More important was the very good existing relationship, good support, geographical reach, and technical approach."

At the simplest, an enterprise needs to agree with the service provider on the balance of control. For example, for a managed service if the customer can make changes directly or change transport networks if needed. And if so, where the demarcation lies between customer and provider and how flexible it is.

Ultimately, a good service provider will recognize the need to support the diversity of approaches companies will continue to take, including supporting companies that want to take a primarily D I Y approach to their SD-WAN.

For example, an enterprise may be unwilling to take a full managed service but may consider a co-managed arrangement whereby they retain control over key decisions affecting the network but delegate day-to-day management and support to the service provider. Or a lighter touch engagement whereby the company runs the network itself and draws on the service provider for advice and guidance in certain areas. Or a service provider that owns the underlay could integrate it with the DIY environment the enterprise built itself.

Security: Most Critical and Changing Fast

Security is critical regardless of the technological or economic cycle. But the move to cloud-first and internet-first, the explosion in remote working, and the growing uncertainty of the economic and geopolitical outlook are creating some extreme security challenges. No wonder that companies say that improving network security is their top WAN priority.

Just as the approaches to SD-WAN itself are many and varied, so too are the ways that organizations are implementing SD-WAN-related security. Overall, there is no clear consensus on best practice, no necessarily right or wrong answer. As Figure 6 shows, almost equal numbers of companies take a multi-vendor, best-of-breed approach as do a single vendor/service provider approach, and even no particular approach at all. The advantages of a looser approach (including breadth of choice and relative ease of switching out vendors) are offset by the advantages of a more tightly integrated approach (such as more assurance of interoperability and less manual configuration).

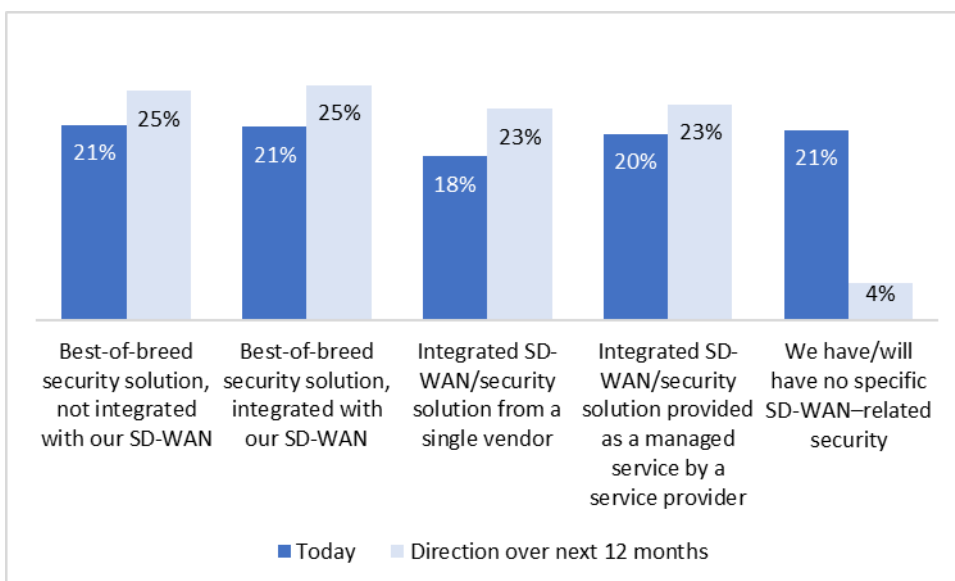
Respondents told us which direction their organization is heading toward over the coming year. The main change will be companies moving away from having no particular position on SD-WAN-specific security, to adopting one of the options shown (with a slight bias toward integrated security, particularly among the largest companies and retail organizations).

There is an overall trend toward network and security convergence, but that doesn't mean every enterprise will take the same journey at the same speed. SD-WAN security solutions will remain diverse and, once again, good service providers will support a wide range of models.

FIGURE 6
SD-WAN Security Remains Diverse

Q. Currently, what is (or will be) your main source of security solutions related to your organization's SD-WAN?

Q. What direction do you expect that will move toward over the next 12 months?



Note: n=624 (companies that currently use SD-WAN or plan to within 2 years)

Source: IDC/GTT, 2022

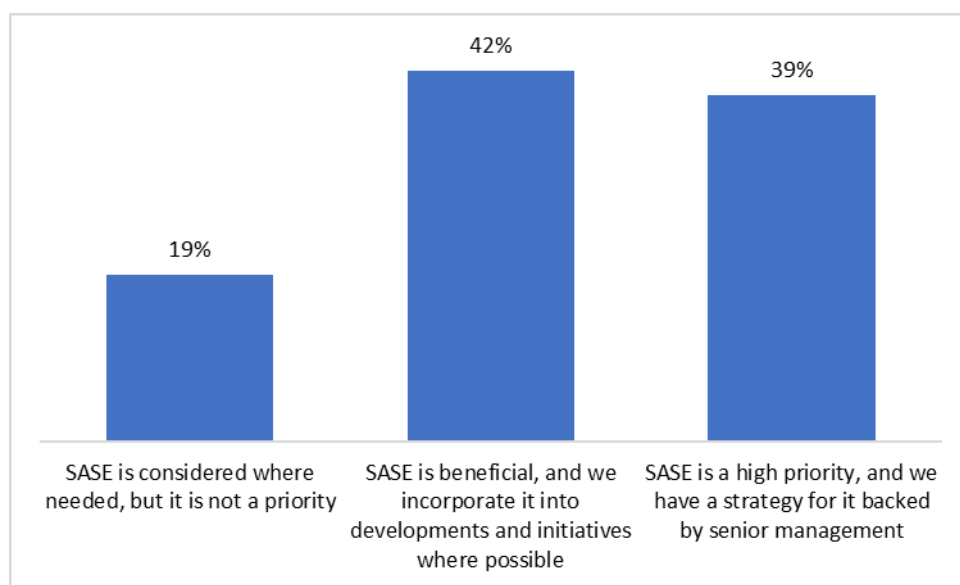
Reflecting the trend towards network/security convergence, interest in SASE is high and growing (Figure 7). Most organizations have plans to deploy it to some extent.

As we saw earlier, companies that lag in their adoption of SD-WAN tend to be behind the technology curve in general, and the same association applies to SASE. Where SASE does score particularly highly is with companies that use a global network operator as their managed service provider for SD-WAN. These businesses are in the sweet spot for SASE. With sites and remote workers spread across multiple geographies and access providers, they can benefit immediately from bringing together access and multiple security functions into a cloud-based managed service.

FIGURE 7

SASE Momentum is Strong

Q. Which of the following best describes your organization's position on SASE?



Note: n=650 (all companies); numbers may not sum to 100% due to rounding

Source: IDC/GTT, 2022

Security architecture is important, but so too are simple, fundamental principles. For example, taking careful account of security when selecting an SD-WAN solution or service pays off. The survey found a clear correlation within both country and industry samples between how much companies prioritize security when making an SD-WAN decision and how well their security expectations were met after implementation. For example:

- **Italian companies** score lowest in terms of prioritizing security and subsequently highest in terms of their security expectations not being met.
- **Spanish organizations** conversely are a close second in terms of prioritizing security and report by far the fewest security-related unmet needs.
- Among industries, **financial services** scores highest on prioritization and lowest on unmet needs.

Given this, organizations looking at SD-WAN need to work with their partners to understand and define their security requirements from the start of the engagement to maximize the likelihood of a successful security outcome. Those that don't are much more likely to need to take post-implementation remedial action or, worse, to potentially be left with inadequate protection.

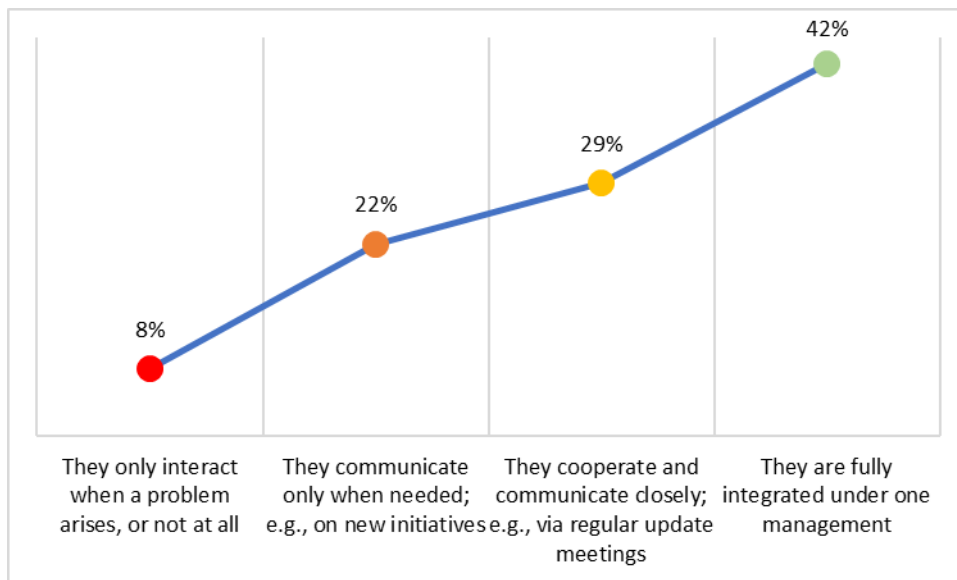
This is another key area where working with a managed service provider can help to ensure that all aspects of a solution are considered and to navigate the options and choices available. If the service provider also operates the network, it will be able to design and optimize security deep in the network and run the combined platform as an end-to-end fully managed service if required.

Finally, enterprises need to understand how networking and security can converge in an organizational sense. As the technology converges, so too do the teams within organizations that are responsible for defining and managing these critical domains. Over 40% of organizations claim that these teams are fully integrated under single management today (Figure 8). This has grown from very low levels only a few years ago and indicates the speed at which these two worlds are coming together.

As that happens, the teams need to align on approaches to buying and integrating security technology. Given that there is no consensus on SD-WAN security architecture, there won't be an obvious way to do that in most companies. The teams need to agree some pragmatic guiding principles that fit with and support the organization's overarching IT strategy.

FIGURE 8
Networking and IT Security Teams Are Closer Than Ever

Q. How well integrated are your organization's IT security and networking teams today?



Note: n=650 (all companies); numbers may not sum to 100% due to rounding
Source: IDC/GTT, 2022

Recommendations

SD-WAN is maturing and taking on a growing proportion of enterprises' critical networks and applications. Its openness and flexibility means that organizations can build and secure networks in more ways than ever, resulting in a wide diversity of approaches being taken. This increases the level of complexity and so increases the need to engage with expert partners to ensure that SD-WAN is implemented and managed optimally and securely to deliver the greatest advantage.

IDC recommends that enterprises take the following actions:

- Assess where SD-WAN is in your organization in terms of its reach, maturity, and support for critical workloads in relation to legacy networks. Most companies are pivoting from legacy to SD-WAN now and need to ensure they have the strategy and partners in place to do it right.
- Account for the benefits, hard and soft, of using a managed service, particularly a network-centric managed service, over a DIY implementation. If you choose the DIY option, make sure you have the resources and capabilities and can face the challenges identified in this White Paper. Don't underestimate the difficulty of implementing and managing an SD-WAN environment at scale in-house.
- Address network/security convergence in terms of technology, services, and organization and consider what partner you need to successfully implement SASE and broader convergence.

There is no single path to success with SD-WAN. Every company has its own set of requirements, preferences, and challenges, and what works for one may not work for another. There are some commonalities among companies that are advanced in their use of SD-WAN, however, and as this White Paper has outlined, their use of managed services is an important factor in realizing the full potential of their SD-WAN.

MESSAGE FROM THE SPONSOR

The survey results discussed in this white paper show that adoption of SD-WAN among enterprises across the globe is widespread. However, ICT teams face multiple challenges that are preventing them from realizing the full benefits of this technology.

GTT is a managed network and security services provider to organizations around the world. We design, deliver, and manage solutions that leverage advanced cloud, SD-WAN, and security technologies to customers in 140 countries across six continents on our global Tier 1 IP backbone.

If you would like to discuss the findings of the white paper or find out more about GTT solutions, please visit [GTT.net](https://www.gtt.net).

About the Analyst



[James Eibisch](#), Research Director, European Infrastructure and Telecoms

James Eibisch is responsible for IDC's research on European enterprise communications services including SD-WAN and cloud/multicloud connectivity. Central to this is understanding how networks are evolving with the growth of software-defined and cloud-centric connectivity services from telcos, hyperscalers, and overlay providers, and what that means for how companies source, build, and manage their networks.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications, and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

IDCUK

5th Floor, Ealing Cross,
85 Uxbridge Road
London
W5 5TH, United Kingdom
44.208.987.7100
Twitter: @IDC
idc-community.com
www.uk.idc.com

Global Headquarters

140 Kendrick Street,
Building B
Needham,
MA 02494
+1.508.872.8200
www.idc.com

Copyright and Restrictions

Any IDC information or reference to IDC that is to be used in advertising, press releases, or promotional materials requires prior written approval from IDC. For permission requests contact the Custom Solutions information line at 508-988-7610 or permissions@idc.com. Translation and/or localization of this document require an additional license from IDC. For more information on IDC visit www.idc.com. For more information on IDC Custom Solutions, visit http://www.idc.com/prodserv/custom_solutions/index.jsp.

Copyright 2022 IDC. Reproduction is forbidden unless authorized. All rights reserved.