COMCAST BUSINESS | MASERGY

WHAT YOU'LL LEARN

- ✓ The benefits of a co-managed service
- ✓ Three "gotchas" to watch out for
- ✓ Who does what: roles and responsibilities

WHITE PAPER

Co-managed SD-WAN: Getting the best out of a shared responsibility model

The need for a virtual workforce is forcing many leaders to rethink their IT operations, and for SD-WAN adopters this has many considering more managed and co-managed services. But why does the work-from-anywhere strategy require more support, and what's the difference between a fully managed SD-WAN service and a co-managed service? This white paper explores SD-WAN management in response to the pandemic, showing you how to use co-managed models to get the best of both worlds.

IT is being restructured under the pressures of remote work

The COVID-19 pandemic is having a significant impact on IT departments. An increased number of help requests coming from employees at home must be addressed. Secure remote access and VPNs now need to be cost effective and reliable for the long term. Security is a bigger and more urgent issue with remote employees connecting at-home devices.

Ultimately, today's work-from-anywhere model is stimulating a restructuring of IT operations that is changing the way business gets done. This is particularly the case as IT leaders implement SD-WAN to assist with their work-from-home strategy.

SD-WAN offers advantages such as applying SD-branch approaches to the virtual workforce and easing the IT burdens of remote connectivity, security, and performance for bandwidth-hungry video conferencing applications. But SD-WAN isn't a plug-and-play technology—it requires ongoing updates and management. Under the new pressures of remote work, IT leaders are thinking long and hard about who should take on the responsibilities required with any deployment. That's because SD-WAN can entail:

- Broadband service procurement, link procurement and installation
- 24/7 service monitoring and optimization with ongoing policy management
- Hardware updates and upgrades
- Service troubleshooting and training for the IT team
- Security, which requires more resources and specialized knowledge

Companies are leaning more heavily on SD-WAN services

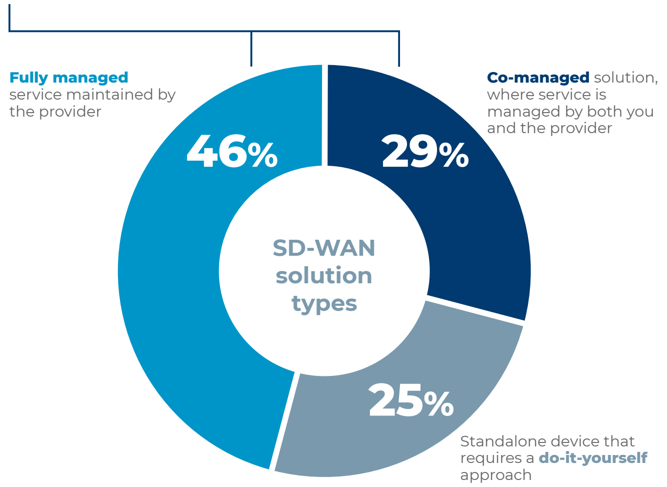
Leaders are more cognizant of the fact that SD-WAN benefits shouldn't outstrip the experts needed to administer it. Cost savings can be eroded when complexity and ongoing management adds too heavily to the ROI equation.

Those that have in-house expertise are naturally immune, as they are more likely to have the required resources available. These companies were largely the early adopters of the do-it-yourself (DIY) solutions, where devices were installed without regard for service guarantees and SLAs. But this is not the case for everyone. Today, remote workers or even branch offices typically lack the needed knowledge, expertise, and resources for ongoing operational management. This also helps explain why the tables are now turning.

Two dynamics are coming together. SD-WAN is reaching mainstream adoption where enterprises are more dependent on providers for assistance. Meanwhile, IT teams are busy serving the new needs of the enterprise—COVID-19. All of this makes IT leaders opt for more service packages. Survey data from major analyst firms demonstrate this recent tipping of the scales.

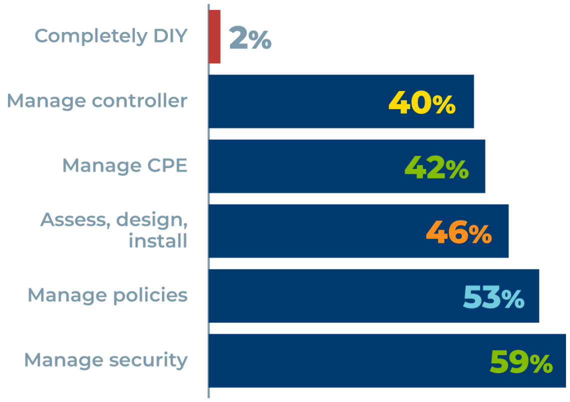
IT leaders prefer managed and co-managed services

75% of those with SD-WAN in use are opting for a co-managed or fully managed solution



- **Nemertes Research** shows adoption of managed services rose from 8% in 2017 to 49.5% in 2020. [Check out the infographic]
- Other results from a [2020 IDG SD-WAN Market Trends survey] show that 75% of SD-WAN users are using a managed or co-managed model.
- Research from Omdia shows 98% of SD-WAN adopters are using external parties at least somewhere along their journey, with 59% of them asking providers to help manage security, 53% asking for help managing network policies, and 46% asking for help with solution access, design, and installation. [Watch the Omdia webinar "Digital Transformation Outlook"]

How do service partners help?



Source: Omdia 2020 Enterprise Networking Insights Survey

OMDIA

- In making the choice to adopt a managed service, most IT leaders are reluctant to outsource SD-WAN completely—only desiring selective service, according to Omdia. Providers have responded, adding co-managed services to their portfolios. Here's what this "middle" option means for IT leaders, and how to get the best of this hybrid model.

Can you really have the best of both worlds? Co-managed "gotchas"

In shared models, companies no longer face the binary choice between a fully managed service and DIY, where cost and control have traditionally been pitted against each other. Thus, the co-managed decision may feel like a no-brainer. However, truly getting the best of both worlds takes careful consideration in the areas of agility, flexibility, and security. Buyer beware.

Your network freedom depends on their solution flexibility

Beware of SD-WAN providers that simply add a high price tag for their service--when in fact--that service only limits your IT freedom. These services might lock you into specific networks, connectivity types, and internet service providers. In today's fast-paced, fast-changing world, IT leaders favor more flexibility and choice. Ask these questions:

- **Transport agnostic:** Can you mix and match network connectivity types, including public internet (broadband), direct internet access, wireless or 5G, and private SD-network service?
- **ISP agnostic:** Which last mile internet services providers (ISPs) can you work with? Are you limited to only the SD-WAN provider's list or can you bring your own broadband?
- **Network agnostic:** Can you work with your own existing private/MPLS network, overlaying SD-WAN and public internet services on top, in an "over the top" strategy? Some "in-net" solutions require the client to tie the SD-WAN functionality to the provider's own network backbone or service cloud, which potentially limits your design options. With in-net solutions, the provider's network acts as the foundational platform for your capabilities, so you should explore the underlying architecture. Platforms standardized on software-defined infrastructures will allow for more agility and flexibility.

What is co-managed SD-WAN?

A co-managed model is a shared responsibility arrangement, creating balance where businesses benefit from distancing themselves from the administration and complexity while still retaining control over the network service.

Advances in SD-WAN specifically allow for this balance, namely centralized management capabilities, cloud-based SDWaaS (SD-WAN as a Service), and online consoles. As a turnkey alternative to the DIY approach, this model decreases the burdens of SD-WAN setup and network performance management without eradicating the client's loss of control—all at an extra cost of course.

Your speed-of-change rides on their responsiveness

Understand specifically what service controls you have and which tasks require a service ticket. Tickets can take days or weeks, slowing your speed-to-change. Your provider's mean time to responsiveness is critical, as are on-demand service controls and real-time performance visibility for each individual application. Ensure you have direct control over the services you change the most, and understand who will serve requirements that fall outside your control and how fast they can execute.

- Does the provider own and operate their own NOC 24/7 or do they outsource?
- How will you be able to track and view the progress of any tickets?
- Are the controls your IT team will use all the same controls the provider's NOC uses?
- Do you have access to all those controls or only a portion of them?
- Do you have visibility of elements you can't directly control?
- How does the provider measure customer service and what is their customer experience reputation?

Your security simplicity also depends on their capabilities

Security is now part of the SD-WAN infrastructure with firewalls as embedded features and a variety of ancillary security functions built into today's solutions. This can be extremely valuable for companies seeking to reduce IT complexity, outsource, and reduce the security "noise" of firewall alert management. When every organization wants to leverage the cost benefits of the public internet, firewalls are must--which in turn make unified threat management and SOC response teams a requirement as well. Evaluate your provider's security maturity and how they will help you expand your coverage. Take into consideration these security functions:

- Next-gen firewalls, cloud firewalls (Firewall as a service FWaaS) and your options when it comes to putting firewalls on-premise or in the cloud
- Cloud security, cloud workload protection, and Cloud access security broker (CASB)
- Network visibility including identity-based WAN analytics and shadow IT discovery
- Secure web gateways
- SOC services for unified threat management and incident response
- Security analytics available inside the SD-WAN management portal

At the end of the day, a co-managed model is a great way to modernize legacy IT infrastructure, gaining the advantages while still freeing your IT resources. A detailed, pragmatic approach is required when it comes to understanding who does what and how your partner is set up to execute on your needs. Masergy's co-managed SD-WAN service model helps explain how to succeed with shared responsibilities.

Fully Managed vs. Co-Managed: Who does what?

While specifics may vary across providers, here's the approach Masergy takes.

	Fully Managed Solution: Provider does it all, but you still get some control	Co-managed Solution: Shared responsibilities
Design	Provider	Provider
Implementation/Install	Provider	Provider
Configuration	Provider	Client: You customize standard firewall rules and other security policy configurations using the portal
Network management and monitoring	Provider	Provider: End-to-end management and monitoring is provided, but the service may vary when public internet connectivity is deployed ■ When clients bring their own ISPs for connectivity (using an "over the top" solution), then Masergy manages and monitors the SD-WAN equipment only ■ When clients use Masergy-provided ISPs for connectivity, Masergy provides end-to-end management and monitoring
Policy management: Business policy, firewall policy, security profiles	Provider and/or Client: Portal allows client to make on-demand modifications, alternatively client can call Masergy NOC	Client: You customize standard configurations using the portal and manage them on an ongoing basis
Incident resolution	Provider: All break-fix performed by Masergy NOC	Shared: Clients are responsible for any break/fix related to Layers 4-7 of the OSI network model while Masergy is responsible for Layers 1-3
Moves, adds, changes, deletes (MACDs)	Provider and/or Client: Portal allows client to make on-demand modifications, alternatively client can call Masergy NOC	Shared: Client is responsible for all MACDs pertaining to Layers 4-7 of the OSI network model while Masergy is responsible for Layers 1-3

About Masergy

Masergy is the software-defined network and cloud platform for the digital enterprise. Recognized as the pioneer in software-defined networking, Masergy enables unrivaled, secure application performance across the network and the cloud with Managed SD-WAN, UCaaS, CCaaS and Managed Security solutions. Industry leading SLAs coupled with an unparalleled customer experience enable global enterprises to achieve business outcomes with certainty.