COMCAST BUSINESS | MASERGY

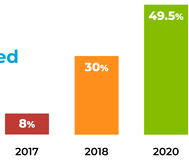
Next-Gen SD-WAN: A framework for decision making

As SD-WAN has evolved, IT leaders have more solution options and therefore more decisions to make. How should the solution be managed and secured? Which features are key for the future? **Nemertes Research offers this framework for making SD-WAN choices.**

Management choices

DIY vs. managed vs. co-managed

Traditionally SD-WAN has come in two basic flavors: do-it-yourself overlay networks (DIY) and fully managed solutions. But a middle path has emerged: co-managed SD-WAN, where the service provider shares management and control with your IT staff.



Adoption of Managed Solutions

Touchpoints for management decisions

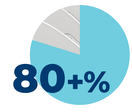
	PROs	CONs
Do It Yourself	▪ Maturity, broader install bases ▪ Complete control ▪ Lower per-site cost	▪ Complete responsibility: deploy manage, troubleshoot, update ▪ Staff knows only this network ▪ Only own staff to lean on
Fully Managed Service	▪ Outsource responsibility: deploy, manage, troubleshoot, update ▪ Deep bench and learnings across networks	▪ Loss of control of platform and management responsiveness ▪ No control of who staffs or for how long
Co-Managed Service	▪ Retain as much responsibility as desired, outsource rest ▪ Deep bench and learnings across networks	▪ Higher cost of managed with reduced staff time savings

Security choices

Branch firewall, monitoring, and response

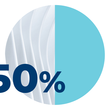
Today's SD-WAN solutions come with optional add-ons for next-generation firewalls, integration tools, and managed security services.

SD-WAN users



want their SD-WAN to replace branch firewalls

intend to enable direct internet access for 75% of their branches, on average



intend, on average, to have 50% of their branches connected via internet links only

Touchpoints for security decisions

The current state of network security: How well is your IT doing at keeping branch routers up-to-date on software and correctly configured? How much effort do configuration changes require?

Firewall architecture and plans: Is your security team ready to collaborate on new approaches for security at the branch? If not, are they ready for a platform with separately manageable firewall endpoints (virtual network functions) sanctioned by the SD-WAN provider?

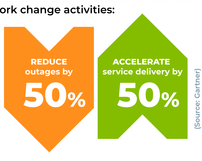
Fitting into the ecosystem: SD-WAN solutions should work with existing security architectures, feeding data into SIEM systems, integrating into CASB and SOAR environments, and managed solutions should offer options for 24/7 threat monitoring and incident response.

Future-proofing choices

AI and autonomous networks

The infusion of AI into SD-WAN can automate network management and optimization by delivering a virtual assistant. Adding new AIOps capabilities enables SD-WAN solutions to track normal traffic behavior and learn how to solve problems automatically.

Organizations that automate 70+% of their network change activities:



[Source: Gartner]

Touchpoints for AIOps

Now or near-term: IT leaders should look for tools that deliver AIOps now, or have a roadmap to deliver AIOps functionality

- AI-powered analysis to identify network patterns and trends
- Virtual network advisor offering proactive advice
- Actionable insights into root cause analysis and security events
- Automation with the ability to integrate cleanly into orchestration controls

Straightforward simplicity: Managed SD-WAN offerings with AIOps should:

- Provide AI-driven analytics and automation for its own underlay networks and infrastructure
- Keep analytics all in one management console with real-time data
- Make AIOps a straightforward addition of functionality rather than require a complete retooling of the infrastructure