

Understanding the power of a **managed software - defined WAN solution**

February 2024 EMA White Paper
By Shamus McGillicuddy, Vice President of Research
Network Infrastructure and Operations



OPTUS


cisco
Partner


EMA™

Foreword

At Optus, we understand the many reasons behind the growing adoption of SD-WAN and have seen first-hand the significant advantages many of our enterprise and government customers are now enjoying through its adoption.

The question now is: what forces are shaping the future and how best can organisations navigate an increasingly complex new digital reality, where security risks are proliferating daily and the user experience is everything?

Robust security is a must-have, given the use of internet, hybrid working and Wi-Fi connectivity as well as the fast-changing threat landscape. Zero Trust Networking needs to be baked in when considering SD-WAN.

Observability, via Digital Experience Monitoring, will also be key – providing organisations with clear insight into the experience of the end user, whether it be an employee at the branch, working from home or an IoT sensor connected to the network.

Here, we see AI increasingly coming to the fore, helping sift through the huge amounts of data generated, identify trends and enable predictive changes to optimise performance.

Redundancy options are also important, and Optus is unique in Australia with our own terrestrial, 5G, and satellite assets as well as our partnerships with LEO satellite providers, which gives us ubiquitous connectivity from the sky to the most remote of locations.

Finally, with sustainability now firmly on the agenda of most boards, the ability of SD-WAN to consolidate functions of advanced networking, Next Generation Firewall, WAN Optimisation and other security features reduce the need for multitude of equipment reducing footprint and energy needs.

Yet SD-WAN is not a simple architecture, nor is it simple to manage or cheap to refresh when new enhancements are released. This can present a challenge for both CapEx budgets and overstretched IT teams. Accordingly, this paper also explores the new imperative for managed SD-WAN services – or SD-WAN-as-a-Service (SD-WANaaS). Available on a per month basis, SD-WANaaS simplifies IT management: no need to manage hardware, software, purchases, renewals or depreciation of capital. In fact, there's no capital required, with the added advantage of a lower total cost of ownership over a 36-month period.

This thought-provoking white paper, commissioned from Enterprise Management Associates (EMA), presents a clear outline of the key drivers for change and how SD-WAN helps organisations to gain greater visibility, flexibility and control over their network infrastructure and applications.

We hope you find this discussion paper both educational and inspiring.

Tom Chan
Director Networking Solutions and Security,
Optus Enterprise and Business



Table of contents

Foreword	2
Digital Disruption Requires a New Secure Network Architecture with SD-WAN	4
Drivers of Change	
Hybrid WAN Architecture Goes Mainstream	4
Hybrid, Multi-Cloud Architecture is Expanding	5
Hybrid and Remote Work is the New Normal	5
How SD-WAN Helps	6
Managed SD-WAN Services Ensure Success	7
SD-WAN is Not Simple	7
Managed SD-WAN Services Offer a Path Forward	8
How to Select the Right Managed SD-WAN Offering	9
Adopt a Unified Platform from a Proven Network Vendor	9
Look for a Cloud-Native, MSP-Friendly Platform	10
Ensure Total Network Observability	10
Setting Expectations for Return on Investment (ROI)	11
EMA Perspective	12
About EMA	12
Why Partner with Optus and Cisco	13

Digital Disruption Requires a New Secure Network Architecture with SD-WAN

Today's businesses are struggling with a new digital reality. Their employees work from anywhere and need to access applications and data that are deployed in a multi-cloud environment. The mission for IT organizations remains the same: securely connect users anytime, anywhere. However, the architecture required to enable these secure connections needs to evolve. Companies must rethink their approach to network infrastructure and security. Managed Software-Defined Wide-Area Networking (SD-WAN) solutions offer a path forward.

Drivers of Change

Enterprise Management Associates (EMA) has identified three significant disruptors that drive businesses to reevaluate the performance, resiliency, and security of their network architectures.

Hybrid WAN Architecture Goes Mainstream

The Internet is an essential WAN connectivity option for enterprises. In 2023, EMA research found that 99% of companies will increase their use of the public internet for connecting sites to their WANs. Meanwhile, 67% are maintaining their use of enterprise-grade, managed WAN services like MPLS (Multi-Protocol Label Switching).¹ The result is a

hybrid WAN solution that leverages two or more connection types to accommodate their changing network requirements

Internet connectivity offers low-cost bandwidth at a time when companies are finding MPLS services to be bandwidth-constrained and expensive. However, the internet is inherently insecure and a shared resource, so service level agreements (SLAs) aren't available. Given these baseline conditions, companies must adopt networking solutions that can apply leading security technologies and traffic steering policies to ensure critical application traffic is protected and prioritized. Managed SD-WAN solutions can improve resiliency and use different connection types to enable a secure and reliable hybrid WAN that allows businesses to grow.

¹ Unless otherwise noted, all research insights and data cited in this paper were originally published by EMA in the April 2023 report, "WAN Transformation with SD-WAN: Establishing a Mature Foundation for SASE Success."

Hybrid, Multi-Cloud Architecture is Expanding

By the end of 2024, 88% of IT organizations will support multi-cloud networks with at least two different Infrastructure-as-a-Service (IaaS) cloud providers in their overall digital architecture.² In EMA's experience, most large businesses also maintain on-premises data centers. These hybrid, multi-cloud architectures introduce network complexity increasing the network's overall vulnerability.

IT organizations are rapidly adopting network solutions that mitigate these risks. They are prioritizing connectivity solutions that span across multi-cloud environments and provide enterprise-grade security regardless of how and where applications and data are accessed. Software-defined solutions are uniquely positioned to help IT organizations adapt to changing network conditions while ensuring consistent policy enforcement, access controls, and user experiences.

Hybrid and Remote Work is the New Normal

In the wake of the COVID-19 pandemic, 94% of companies saw a permanent increase in the number of remote employees. Furthermore, 96% of those who have remote employees report that many of them are hybrid workers who work from home and at the office.³ IT organizations need to provide hybrid workers with reliable and secure network experiences regardless of where they are working.

As the workforce extends beyond the physical office, businesses struggle to extend security measures to every user and every device regardless of location. Legacy remote secure access solutions like Virtual Private Networks (VPNs) were not designed to accommodate today's hybrid workforce. Users now expect seamless, secure connectivity regardless of where they work. Businesses are adopting solutions that provide good user experiences without sacrificing security.

² EMA, "Network Management Megatrends 2022," April 2022.

³ EMA, "Modernizing Network Engineering and Operations in the Era of Hybrid and Remote Work," August 2023.

94%

of companies saw a permanent increase in the number of remote employees

96%

of those who have remote employees report that many of them are hybrid workers

How SD-WAN Helps

SD-WAN is a Software-Defined Networking (SDN) technology that establishes a management overlay across disparate WAN connections. SD-WAN edge gateways establish secure tunnels between corporate sites, data centers, and the public cloud. SD-WAN gateways typically offer routing, traffic steering, and network security (e.g., an edge firewall) across multiple network connections. A cloud-delivered SD-WAN controller can simplify some—but not all—operations by centralizing configuration, monitoring, and management.

A successful SD-WAN solution simplifies hybrid networks and multi-cloud architectures by providing centralized control over network design. The technology optimizes connectivity and manages traffic with intelligent routing. Furthermore, SD-WAN technology secures hybrid WAN connectivity, multi-cloud connectivity, and hybrid worker connectivity with standard security implementation across all types of network access.

SD-WAN can help businesses reduce network complexity and improve security. However, SD-WAN implementation and ongoing operations often challenge IT organizations. EMA research indicates that IT organizations now rarely implement this technology on their own. Most companies now adopt managed SD-WAN services. Managed Services Providers (MSPs) can eliminate the complexity of SD-WAN implementation while delivering a secure, cost-effective solution with enforceable SLAs.



Managed SD-WAN Services Ensure Success

SD-WAN is Not Simple

Only 38% of SD-WAN implementations are completely successful. Skills gaps, implementation complexity, and security integration challenges often undermine SD-WAN projects. Nearly 41% of IT organizations told EMA that their network teams lack the engineering talent to design, implement and operate an SD-WAN-based network.

More than 28% told EMA that an SD-WAN implementation is simply too complex, even when they have sufficient engineering talent. For example, network teams must configure hundreds of tunnels in an SD-WAN overlay and tune Quality of Service (QoS) settings for various applications. Rolling out SD-WAN across dozens or hundreds of sites can take more than a year and pulls valuable resources from other strategic initiatives.

Additionally, 24% of organizations are struggling significantly to integrate SD-WAN with their existing security architecture. SD-WAN often replaces legacy network security devices such as Unified Threat Management (UTM) appliances or firewalls in branch offices. The network team often struggles to translate existing security policies into the SD-WAN solution. Furthermore, they must integrate SD-WAN security with any additional third-party security solutions that remain in place. SD-WAN solutions that seamlessly integrate with existing security architectures will lead to more success.

Only

38%

of SD-WAN implementations are completely successful

24%

of organizations are struggling significantly to integrate SD-WAN with their existing security architecture

Managed SD-WAN Services Offer a Path Forward

When SD-WAN emerged more than a decade ago, many IT organizations adopted a Do-It-Yourself (DIY) approach for implementing the technology, but today companies increasingly look to MSPs to navigate digital transformation through a rapidly evolving network landscape. IT organizations are shifting toward a managed approach because they have found SD-WAN to be more complex to implement and manage than they initially expected. EMA research recently found that 66% of IT organizations prefer to consume SD-WAN as a managed service rather than follow a DIY approach. Smaller companies are even more likely to prefer a managed SD-WAN service, given they are more likely to face skills and knowledge gaps within their IT organizations.

Organizations that consume SD-WAN as a managed service told EMA that there are four primary drivers of this decision.

The Vice President of Architecture at a large energy company addresses these concerns when describing to EMA why he chose a managed SD-WAN solution: "I said [to upper management], we don't have the right headcount, we don't have the resources, and we don't have enough CapEx to buy the hardware. Otherwise, I would have had to ask for 10 new employees and \$3 million for hardware."

Given these dynamics, it's no surprise that managed services are a best-practice approach to SD-WAN. EMA research found that successful consumers of SD-WAN technology are three times as likely to prefer a managed service over a DIY implementation.



Integration with other managed services:

Many MSPs offer managed services that they can seamlessly integrate with SD-WAN, relieving concerns around integration with existing security architectures. This integration can also offer a smooth path forward to Secure Access Service Edge (SASE), a solution architecture that unifies SD-WAN with cloud-delivered security services.



Network assurance: MSPs can offer SLAs on performance and uptime that standard internet service providers cannot. These SLAs are essential as companies adopt hybrid WAN solutions.



Cost savings: A subscription-based managed service eliminates the need for large capital outlays for new SD-WAN hardware. An organization can also avoid the expense of hiring SD-WAN experts to implement and manage the solution. This approach allows IT organizations to redeploy internal resources for maximized productivity and cost savings.



Reduced deployment complexity: Although SD-WAN is a software-defined technology, it is not easy to implement. Secure and resilient SD-WAN solutions don't happen overnight. They take careful planning and implementation. MSPs offer the experience and resources to make this process as efficient as possible without sacrificing the quality of implementation.



How to Select the Right Managed SD-WAN Offering

There are dozens of SD-WAN solutions on the market today and hundreds of MSPs offering SD-WAN services. So how do you find the right managed offering? EMA recommends that IT organizations consider the following guiding principles.

Adopt a Unified Platform from a Proven Network Vendor

MSPs build offerings with multiple SD-WAN vendors to ensure they address the needs of all customers, based on price, scalability, feature requirements, and more. Moreover, some MSPs will use multiple technologies to assemble a managed offering. They might enhance the security of an SD-WAN product with a third-party firewall. Or they might combine an SD-WAN solution with a third-party cloud-based security offering to build out a managed Secure Access Service Edge (SASE). However, multi-vendor solutions can result in poorly configured, mismatched technology stacks. This adds complexity that challenges performance and adds security risk. EMA research has found that single-vendor SD-WAN strategies are usually more successful than multi-vendor ones. Unified platforms simplify management and provide stronger security.

For these reasons, it is crucial that IT organizations pay close attention to the SD-WAN products that their MSPs offer. To optimize performance and security, businesses should seek services based on unified SD-WAN platforms. They should also look beyond the MSP at the underlying networking vendors that provide those solutions to ensure that MSPs are working with vendors that have a track record of success. Proven networking vendors can offer scalable, feature-rich solutions with highly security networking technology on a unified platform.

Look for a Cloud-Native, MSP-Friendly Platform

IT organizations are increasingly embracing cloud-managed networking solutions, for their simplicity, reliability, and scalability. When choosing a managed SD-WAN service, organizations should focus on MSPs who work with truly cloud-native management platforms. These MSPs will bring a cloud security skillset along with their cloud management skills.

Many SD-WAN vendors will “cloudify” their solutions by hosting a legacy controller in the cloud. These controllers are not cloud-native. Instead, they are based on monolithic architectures that are difficult for MSPs to work with. For instance, a legacy controller may require downtime during software updates. A true cloud-native platform offers hitless software updates thanks to its multi-tenant, globally distributed, high-resiliency architecture. Cloud-native technology will ensure your network is optimized and secure at all times.

Furthermore, a cloud-native SD-WAN controller is usually easier to use. This allows MSPs to fully operationalize the solution and pass on any associated cost savings to the end customer. It also simplifies management of the SD-WAN solution all around. This is important because 58% of SD-WAN adopters prefer a hybrid operating model for SD-WAN, where the IT organization and the MSP share responsibility for Day 2 operations, such as change management, monitoring, and troubleshooting. This holds MSPs accountable to their SLAs and enables internal network operations teams to collaborate with an MSP on complex problems.

Ensure Total Network Observability

Given that most organizations adopt a hybrid SD-WAN operating model, SD-WAN observability is essential. SD-WAN solutions offer native monitoring and troubleshooting capabilities, but only 40% of IT organizations are fully satisfied with those features. Thus, IT organizations should look closely at the observability capabilities of the SD-WAN solutions available to them. In recent years, many SD-WAN vendors have acquired network observability vendors to enhance their capabilities in this area.

When thinking about SD-WAN observability, IT organizations should look at how solutions provide visibility into both the SD-WAN overlay and the WAN underlay. The SD-WAN overlay consists of the tunnels that an SD-WAN solution establishes across the WAN. SD-WAN solutions should provide visibility into the state of these tunnels and the nature of the applications that are traversing them. The WAN underlay will consist of a variety of connectivity services that the SD-WAN tunnels are built upon. This mix of services can include MPLS, broadband internet, and 4G and 5G fixed-mobile services from multiple regional providers. Establishing an end-to-end view across this diverse WAN underlay environment can be difficult but essential. EMA research found that successful adopters of SD-WAN are more likely to have end-to-end visibility into their entire WAN underlay.

Setting Expectations for Return on Investment (ROI)

IT organizations should start any conversation with a managed SD-WAN service provider with a discussion about potential returns on investment. EMA research has identified four primary ways in which SD-WAN investments ultimately pay back customers.

Reduced security risk: The typical cost of a security breach for an enterprise is \$4.45 million.⁴ Any investment that can reduce security risk should be considered through the lens of that potential cost. An SD-WAN solution typically offers strong integrated security capabilities at the edge. If enhanced to a full SASE solution, it can reduce security risk even further. IT leaders should ask MSPs in-depth questions about the potential for a managed SD-WAN offering to reduce security risk.

Reduced costs: SD-WAN consolidates multiple solutions (routers, firewalls, network management tools) into a single platform. IT organizations should compare the costs of a potential refresh of these individual platforms and the ongoing cost of maintaining them with the cost of consolidating onto a single platform packaged as a managed offering. This may involve translating some capital costs to operational costs, given the shift from purchasing hardware and perpetual software licenses to a lower-cost subscription model.

Cloud enablement: IT organizations tell EMA that SD-WAN adoption helps them with their cloud transformation strategies. As they migrate to the cloud and establish hybrid, multi-cloud architectures, connectivity, and security become extremely complex. The software-defined nature of SD-WAN can mitigate the complexity, thus reducing the costs associated with building out cloud connectivity and security.

Improved network and application visibility and performance. SD-WAN observability improves an IT organization's ability to manage problems and plan for the future, ensuring minimal disruptions as network requirements change over time. The efficient architecture and traffic steering features of SD-WAN ensure that network and application performance is maximized. This reduces the chances of a service degradation or outage, which is essential in terms of ROI, given that the average cost of a minute of downtime is \$12,900 per minute.⁵

4 IBM, "Cost of a Data Breach Report 2023" (<https://www.ibm.com/reports/data-breach>)

5 EMA, "The Modern IT Outage: Costs, Causes and 'Cures,'" October 2022.



EMA Perspective

SD-WAN solutions have been on the market for over a decade, but IT organizations are still struggling to find the best path forward. EMA research has identified several best practices that can ensure success.

First and foremost, companies should abandon DIY approaches to the technology. IT organizations simply experience more success when they work with an MSP. However, choosing the right managed SD-WAN service isn't trivial. This paper has offered several tips for how to find the right offering. It starts with making sure that the SD-WAN platform underpinning a managed offering is a unified technology from a proven networking vendor with cloud-native management, strong security, and superior observability. If you are ready for the transition to SD-WAN, talk to your trusted MSP partners about their offerings and use this paper to help you find the right solution for you.

About EMA

Founded in 1996, Enterprise Management Associates (EMA) is a leading IT analyst research firm that specializes in going "beyond the surface" to provide deep insight across the full spectrum of IT management technologies. EMA analysts leverage a unique combination of practical experience, insight into industry best practices, and in-depth knowledge of current and planned vendor solutions to help its clients achieve their goals. Learn more about EMA research, analysis, and consulting services at www.enterprisemanagement.com or follow EMA on [X](#) or [LinkedIn](#).

Why Partner with Optus and Cisco




Optus and Cisco have come together to enable secure managed connectivity and modern working.



Our strategic advantage

 End-to-end Solutions	 Experience & expertise	 Unique offering
<ul style="list-style-type: none">• A one-stop-shop for connectivity, networking, security, observability, collaboration, and managed services.	<ul style="list-style-type: none">• 25+ year partnership• 2,000+ joint customers over the span of the partnership• 500+ Cisco Blackbelt certifications held by Optus employees• Jointly funded dedicated sales specialist and GTM resources.	<ul style="list-style-type: none">• Significant joint investment in a multi-year program to deliver• Secure managed network services.• First to market with innovative managed services solutions

Our customer benefits

 Reduced Business Risk	 Ease of Implementation	 Future Proof
<ul style="list-style-type: none">• Validated architecture & carrier-level integration• End-to-end observability for prevention & faster problem solving• Protect, detect & respond to security events for LAN, WLAN, WAN & Cloud.	<ul style="list-style-type: none">• Seamless Integration of systems, teams, and technology.	<ul style="list-style-type: none">• Track record of first-to-market joint solutions to ensure changing business needs are met.

Talk to us today

Request a call back at
optus.com.au/enterprise/contact-us

Follow us

