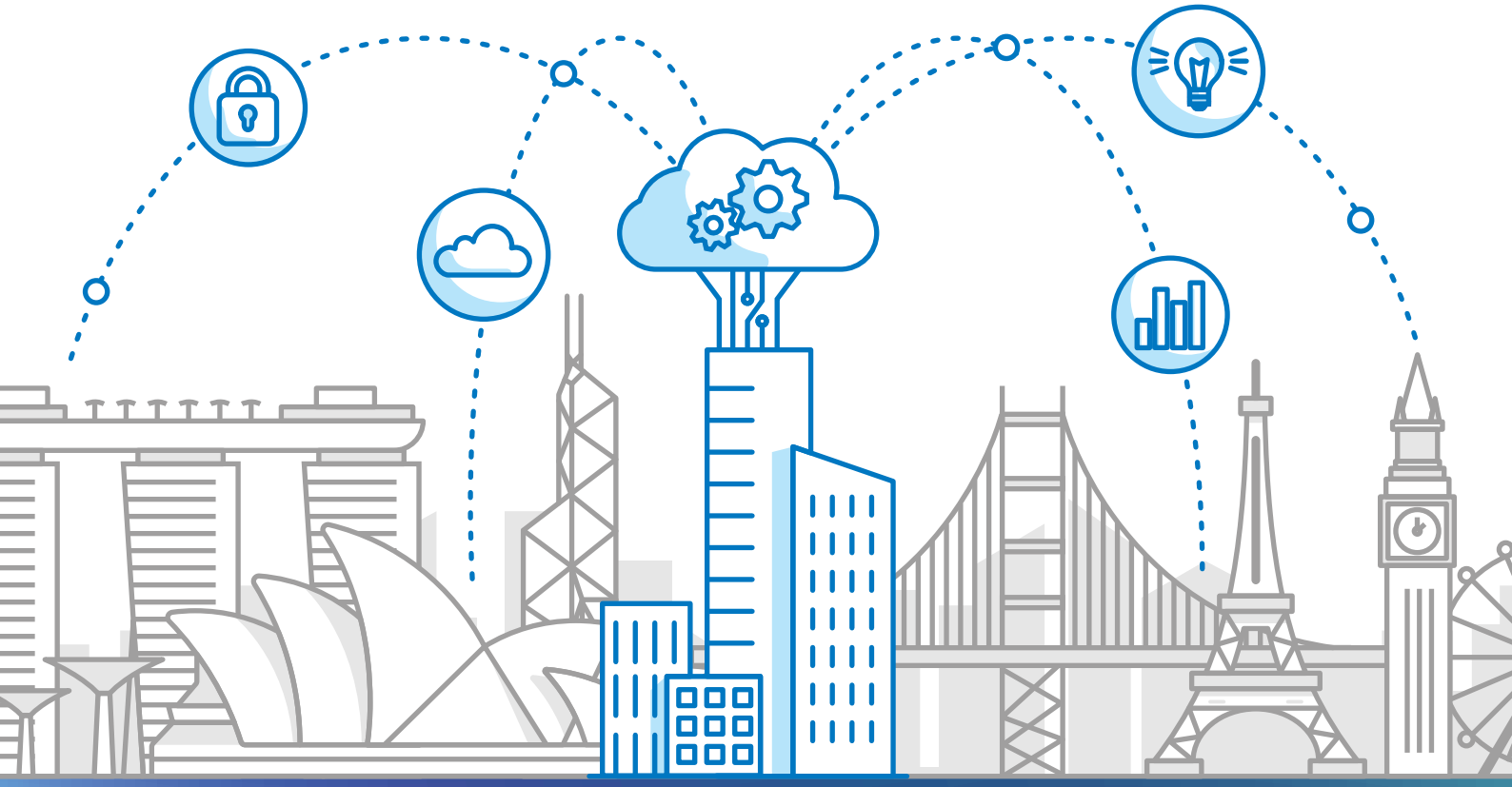
Telstra | GlobalData. | vmware

Whitepaper

SD-WAN Clarified: A Survival Guide for Network Managers



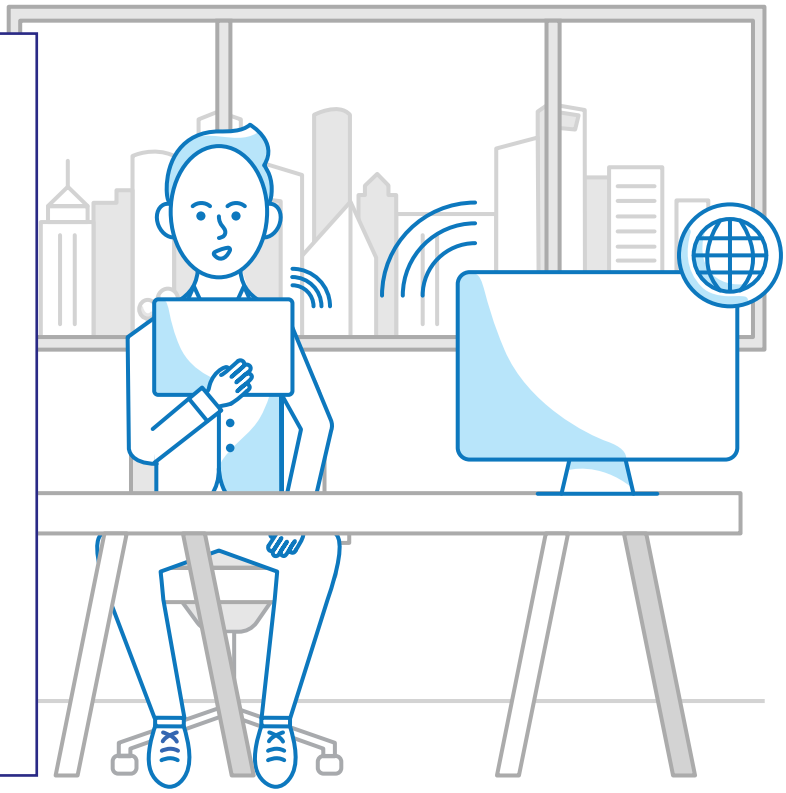
Contents

Executive Summary

Unlike any previous time in recent history, the network has arguably become the single most important ICT investment to meet the new priorities and challenges businesses face in 2020. Digital transformation priorities have accelerated. This is due especially to the unique challenges posed by COVID-19, which reflect on different and future ways of working.

Cloud and mobile-first strategies require agile and future-proofed networks.

These are networks that can be configured dynamically, and which add capacity and throughput on the fly to deliver secure, high-quality and consistent services to an even more distributed workforce. The new workplace arrangements mean employees will be accessing even more 'mission-critical' data, which is hosted on the cloud and transported to any number of locations, endpoints and/or device types.



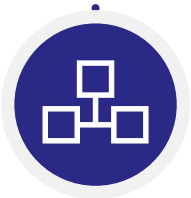
In the past, the focus was on network engineering solutions to interconnect campus and branch environments. There were established Internet breakouts and cloud gateways. Today, businesses are changing. Private networks are no longer the panacea. The public Internet itself is being deployed in more cases as the mainstream technology for corporate networking with SD-WAN. This is changing the role of MPLS and Ethernet in some of the newer solution designs.

The focus now for a digital business is delivering secure, business-grade IT services to the end-user and/or device, not just the physical location of the headquarters or branch office. Users and devices are becoming more mobile and location-agnostic. Nevertheless, they require a secure connection with better application performance to create a high-quality user experience. Some of the benefits include increased employee productivity, network agility and lower IT costs.

With all the dependencies, like access in the last mile, this is easier said than done, especially if the network connects employees, partners and suppliers across multiple borders.

SD-WAN Overlay

An over-the-top capability to a WAN where a virtual network is typically created to run across the top of the physical infrastructure, has helped businesses gain ground with quick tactical wins, with little risk. SD-WAN overlays have advanced networking by improving the management, orchestration and performance of the corporate WAN.

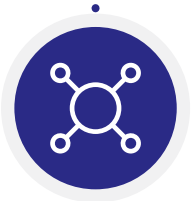


Network Engineering vs. Peering

The way carriers design networks will reflect directly on performance. While private networks supported campus and branch environments well, the shift is also on how public networks are peered and managed, even to third-parties to deliver a business-grade service. The architecture of circuits in a peering construct has a major impact on the quality of the network. Not all Internet services are created equal and a best-effort Internet service may not deliver the performance required for business applications.

Network Evolution

Corporate WANs will continue to use multi-service technologies (e.g., MPLS, Internet), topologies (e.g., star, meshed) and incorporate even more wireless solutions (e.g., cellular, Wi-Fi). SD-WAN will also drive integration between WAN/WLAN, campus, branch and cloud networks. The goal is to have one over-arching control plane to drive better visibility, simplicity and operational efficiencies.



Carrier Underlay Evolution

In the longer-term as SD-WAN matures, carriers' investments in the underlay – relating to the physical infrastructure such as automation – will support the overlay capabilities of SD-WAN such as orchestration. Having both sets of capabilities integrated into a common fabric will create a longer-term competitive advantage for network operators.

Current Perspective

In the current environment, network service has never been more important. As businesses transition from the initial shock of COVID-19, to the realism of moving away from the office-centric workplace to a more remote and distributed environment, the underlying infrastructure needs to be highly adaptable to deliver user-centric ICT service. Data and applications need to be transported securely to and from any location, any device and at any time of day for a consistent user experience. Not only are employees working remotely, so are their partners, suppliers and customers. This creates a force multiplier and raises the value and importance of networking and communications at the current time.

Telstra commissioned a GlobalData study which surveyed 121 IT leaders operating in APAC, Europe and the US regions. It found businesses are investing in the following technologies to enable remote working as a result of COVID-19.

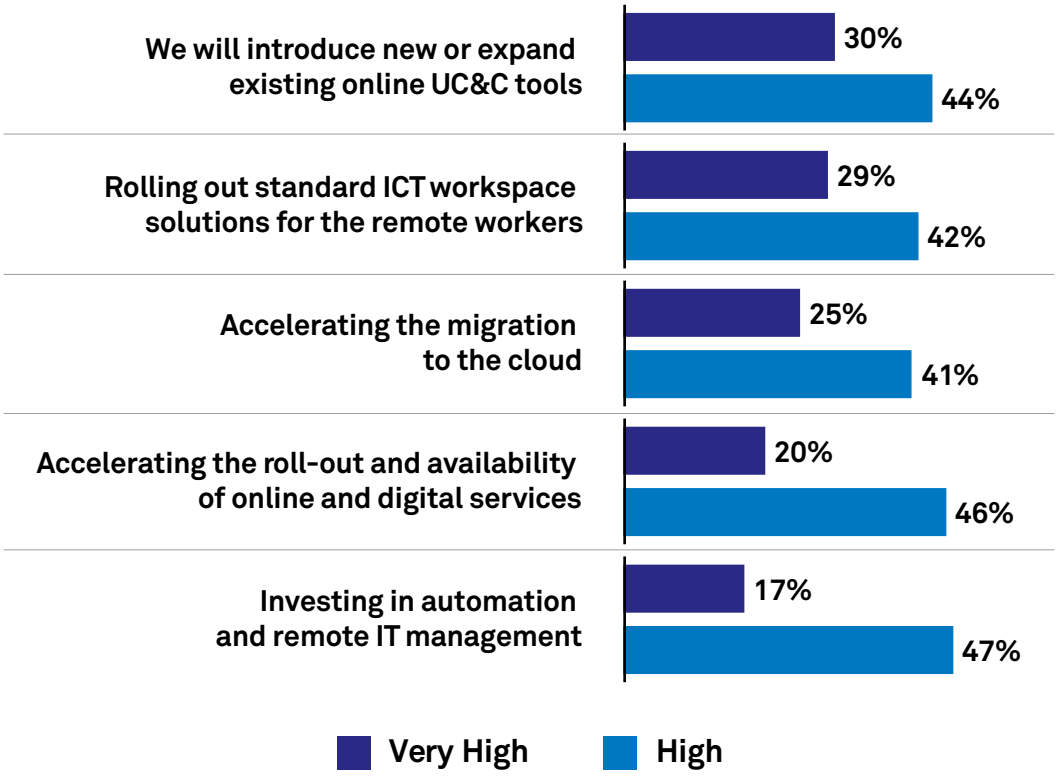
Is your company investing or considering an investment in any of the following to enable more employees to work remotely?

Telstra/GlobalData April, 2020 'COVID-19: Impact on IT Budget, Strategy and Priorities.' APAC, European and US respondents, n=121.

As businesses move to remote locations, they often mirror office-based environments with home locations. This includes the provisioning of new hardware that is compliant with company policy, security and compliance guidelines. This hardware provisioning also enables collaboration and services to more locations, and requires procuring or increasing the capacity of existing VPN services for secure networking. Virtual desktop applications are also being used for remote access to business-critical applications, especially when the location of physical data is important.

In terms of strategic priorities, the research also shows that **businesses are looking to accelerate the migration of workloads to the cloud, possibly having no data residing in some branch locations**. Businesses are also introducing standard ICT services to employees depending on their roles. As omni-channel is the only channel for customer engagement, businesses are accelerating the rollout of online and digital services to create multiple touch points between businesses and their customers and prospects.

Have immediate ICT priorities changed as a result of COVID-19?



Telstra/ GlobalData April, 2020 'COVID-19: Impact on IT Budget, Strategy and Priorities.' APAC, European and US respondents, n=121.

Nearly all of these emerging workloads will be deployed from cloud environments, which in turn are located in numerous places. On the one hand, networks will continue to interconnect campus and branch environments as they have been doing for years, and now extend this to remote workers. On the other hand, they will need to connect to cloud environments securely at very low latency and high reliability thresholds.

There are many challenges in the network that are not always immediately visible. If configured incorrectly, they become congested. When clouds are provisioned over long distances, users will experience a high level of latency, possibly services being timed out. Cloud providers vary in terms of availability zones and even specifications on how the cloud and networks are to interconnect. On the customer side, even the location of the VPN gateway is important. They need to support the right level of tunneling sessions to meet internal stakeholders' needs, ideally hosted in-region or some cases in-country, and be flexible enough to deliver a higher and consistent performance level. There also needs to be provisions for network failover to deliver continuity of operations in the event of an outage. Business-grade communications will tend to have multiple places of in-built redundancy from the cloud through to the user desktop and device.

Underpinning the technology investments to support the changes to the workplace is network technology. **For this reason, nearly two-thirds of respondents are also re-evaluating their current WAN solutions.** There are many WAN topologies (e.g., bus, ring, star, mesh, tiered) and technologies (e.g., MPLS, Internet, Ethernet, wireless) to consider. Directionally, the interplay between mobile workers and cloud means networks will continue to evolve, as multi-service environments take the best-of-breed approach factoring in areas such as cost, availability and redundancy. WAN, which extends from cloud to branch environments, plays an important role in connecting more users, devices and applications across large distances.

Why is SD-WAN Important in the Modern WAN?

GlobalData/Telstra research shows that nearly half of businesses, on average, have between 50% and 100% of its workforce operating remotely as a result of COVID-19. This is the highest in the UK, Europe, Southeast Asia and ANZ which report two-thirds of employees, on average, working remotely; the lowest figures are in North Asia with only one-third of the employee base working remotely. [1]

Networks are ever more important as businesses tend to be hyper-connected. And with their importance, there is a lot of complexity invisible to average users. Research conducted by Telstra and GlobalData found that over **90% of businesses are now accelerating workloads to the cloud**. This is happening at a time when businesses are supporting a large influx of remote workers.

With businesses moving more workloads to various cloud platforms and supporting the ICT needs of a larger proportion of remote employees, network strategies are starting to change. Some customers are starting to question the role and relevancy of on-premise server rooms in the branch environments, perhaps in emptier offices.

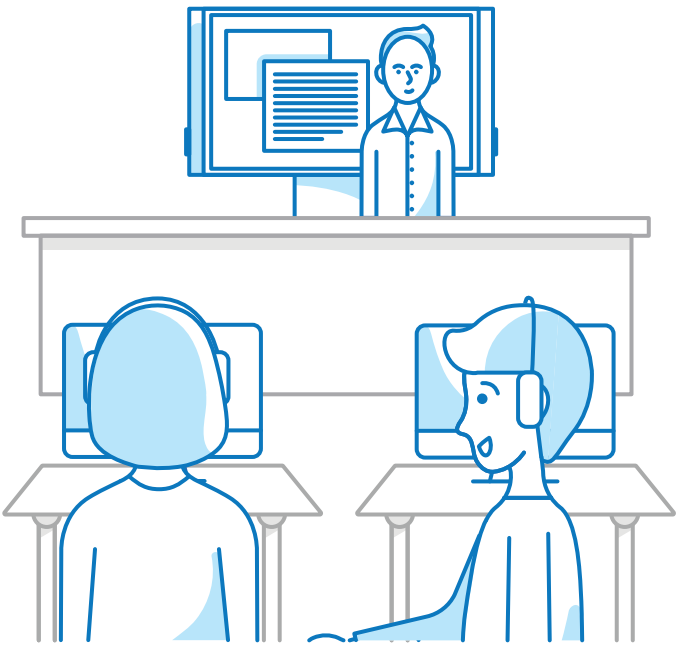
Others are re-evaluating the need for dedicated data center space for co-location, if the priority is to move potentially all workloads to the cloud. This, in turn, starts to change network strategy and the way networks should be designed.

SD-WAN allows IT managers to regain the upper hand. Nearly 90 per cent of global businesses are trialing or deploying SD-WAN technology. The top use cases are having greater ability to provision and manage networks, especially in accommodating the many moves, adds, and changes for new workloads. SD-WAN is also an important enabler for the new distributed workforce. [1]

1 Telstra/GlobalData April, 2020 'COVID-19: Impact on IT Budget, Strategy and Priorities.' APAC, European and US respondents, n=121.

Nearly two-thirds of businesses today are re-assessing their current WAN strategy. [1]

SD-WAN allows businesses to move as fast as their workloads. As companies introduce new workloads, such as containers and virtual machines (VMs), they are better able to automate the associated policies. This includes, for example, the configuration of switches, firewalls, and routers to align network and security. While businesses are looking for speed, agility and ability to deliver a consistent user experience across networks, it also needs to be **secure and compliant with many current regulations such as data sovereignty.** [2]



Better Management

Many solutions will use centralised orchestrators to configure and apply policies across the network through graphic user interfaces (GUIs), drag and drop functionality managed from the cloud and enabled through an edge device. **The orchestration solutions use AI/ML to drive recommendations and operational efficiencies.** This provides a better way to manage heterogeneous estates in a repeatable and automated way. Branches and endpoints can turn 'on and off,' incorporated into the WAN topology and policy with no specialist IT support required on-site at each branch, corporate office or home location.

Business-Grade over Public Internet

As businesses have embraced multi-service networks, public Internet has become more prominent in the mix of technologies. The quality of connections is also improving due to the way many telecom providers are managing, peering and interconnecting their networks. There are also newer protocols. Some are programmable enabling networks to become adaptive. As the public Internet is conditioned to deliver business-grade performance, SD-WAN becomes a strong option in addition to other established technologies, such as private MPLS. **GlobalData research shows that SD-WAN is becoming mainstream and increasingly used for mission-critical applications such as voice, collaboration, contact centers and CRM/ERP.** [1]

1 Telstra/GlobalData April, 2020 'COVID-19: Impact on IT Budget, Strategy and Priorities.' APAC, European and US respondents, n=121.
2 Noteworthy, the number one cause of outages is human error. The number one source of human error is the configuration and management of networks.

Cloud-Readiness

With more workloads moving to the cloud, SD-WAN solutions are also providing other advantages such as direct, but secure connections to cloud and SaaS applications using tunneling and encryption. Internet links are optimised with traffic flows to improve WAN and application performance through cloud gateways. Link correction and remediation features allow for links to failover without losing the session. Some providers are building up the cloud gateway infrastructure to optimise the Internet for the delivery of SaaS.

Security

As with legacy WAN, security is an important core capability. SD-WAN security solutions are provided from the cloud (e.g., with no local inspection) or through physical hardware. The on-site solutions tend to have multiple virtual services working together within a physical appliance (e.g., hypervisor and SDN controller). Built-in security solutions provide the essentials (e.g., application-layer firewalling, IDS/IPS, anti-bot, anti-malware, web filtering, SSL DPI). Cloud-based solutions can increase latency in certain scenarios. Most providers accommodate both requirements.

Performance Monitoring

Similar to other WAN services, SD-WAN is also offered as a managed service. This is important for the monitoring and management of links (e.g., latency, throughput, packet loss, jitter, utilisation). Using this information, and understanding the applications and workloads, many **SD-WAN solutions make real-time routing decisions to deliver the strongest possible performance picking from a variety of network links and routing paths**.

SD-WAN as a Pure/ OTT Overlay

Many SD-WAN deployments to date have been tactical and provided some quick wins such as better application performance monitoring and steering, ability to save costs using alternatives to MPLS, simplified management with orchestrators, and zero-touch provisioning. SD-WAN technology overall has definitely advanced modern networking.

While SD-WAN brings many benefits from traditional networking, this space is becoming commoditised. There are now over 60 vendors, each vying for a share of the market. Since SD-WAN is a feature on top of traditional network services, security, or WAN optimisation, customers have some level of familiarity with the product and an established connection to a channel partner. Ultimately, SD-WAN varies in the level of competitiveness or solutions that it can solve. There have been some false starts and setbacks along the way. Collectively, **SD-WAN tends to improve traffic engineering, management and visibility within network domains under management, not the WAN and network solutions overall. Ultimately, however, SD-WAN can only function well when the underlying Internet connection is reliable and high performing**. This presents a unique opportunity for the operators to reframe the debate by addressing how SD-WAN can also be addressed through the network as an 'underlay' technology, which we discuss in the next section.

Using SD-WAN with 'Carrier Underlay' Connectivity to Complete the Picture

Telecom providers are developing architectures to address some of the customer limitations with having an overlay, or orchestration, alone. A carrier underlay strategy underpinned by investments in the physical infrastructure, such as AI, ML and automation, can help businesses deliver a sustainable competitive advantage for their WAN service. Adopting both an overlay orchestration with their chosen vendors, as well as underlay strategy, unique to network operators, can bring additional benefits over time.

While an SD-WAN overlay looks at traffic engineering and steering over the top of a physical network, the underlay considers the additional services, as well as what the integration of a physical and virtual network can bring to the market.

In concrete terms, the underlay (as the market evolves) is the implementation of technologies, such as AI/ML, security, automation and orchestration engines, into the physical core network. These deliver more value than an over-the-top overlay service. Customers benefit from a single integrated solution. Carriers use the core network to unveil more value. The service wrap is difficult, or impossible, for non-network operators to replicate. These combined capabilities, the carrier underlay with an SD-WAN overlay, provide some of the following advantages:

Better Ability to Support Multi-Vendor Environments

One of the immediate benefits of a carrier underlay strategy is for the Communication Service Provider (CSP) to understand applications and data running across the network (overlay), before dynamically applying policies and/or resources to improve the performance, security, availability of these workloads (via the underlay). **Having a network that is more application-aware makes it possible to allocate the right level of resources based on the application-service level metrics.** It also gives the carrier a strong position to support multi-vendor environments, especially in L4 (transport) to L7 (application). Networks would have to automate and orchestrate policies to promote interoperability. It is important for telecom providers to offer best-of-breed solutions (especially from the network function virtualisation perspective, allowing customers to deploy network functions from different vendors) and give customers options to avoid vendor lock-in. This can **help businesses strike the right balance between systems** that are open and programmable, and closed system environments that are tightly coupled and integrated.

Policy-Based Automation

Through the core network, telecom providers can dynamically apply policies across the network environments: LAN, campus, branch, data center and even third-party clouds. These solutions can potentially encompass both fixed and wireless infrastructures. **Having the ability to better automate policy from the core offers a better way to manage 'own' and 'third party' Virtual Network Functions (VNFs) at different layers of the Open Systems Interconnection (OSI) Stack.** Other benefits are in areas such as offering bandwidth on demand to an individual department or providing more resiliencies for mission-critical links. There are also **advantages in providing more end-to-end visibility and control from employee laptops and devices to the servers in third-party clouds**.

Data-Driven Root Cause Analysis

AI/ML technologies, when applied to the core network, can identify hidden relationships between data sets in customer environments. This can set out **recommendations to improve guaranteed uptime and resiliency through reference architecture.** These solutions can use more data from the network (e.g., core and edge) to determine the cause of network degradation, or outage, at any point of time pinpointed to an individual site or demarcation point. The use of data to identify and isolate faults faster provides for better accountability, especially in multi-vendor stacks. Similar solutions can offer preventative or predictive maintenance as well as improvement in network operations. **This benefits businesses by moving from a hypothesis-driven root case analysis to empirical data-driven insights.**

Deterministic Routing

Telecom providers using the latest protocols and routing technology can provide more direct point-to-point routing across the public Internet, to improve security and performance on an end-to-end basis. This is **a managed service which requires working with multiple ISPs and in-region operators, and commitments by all network operators to improve performance.** These efforts are enhanced with in-region private peering, which impacts performance and Round-Trip Delays (RTDs), and improves SLAs over own- and third-party networks.

Security

Through a carrier underlay capability, the core network acts as a threat intelligence platform. This provides better visibility, insight and predictability of potential security vulnerabilities and attacks, such as DDoS. For years, providers have included anti-malware, IDS/IPS, and other security capabilities embedded into the actual access circuits. **The use of AI/ML can help to improve threat detection and prevention, which in turn, improve incident response and remediation.**

Conclusion and Future Outlook

As the growth of cloud adoption continues in parallel with a spike in the number of branch sites and pop-up environments, traditional topologies of WAN solutions will also transform. Networks will continue to be multi-service, multi-technology, multi-protocol and multi-domain, which reflect the dynamic and service-centric environments they need to support.

GlobalData research shows that at least half of large, multi-site enterprises have already deployed SD-WAN and over the next 24 months, this figure will surpass 90 per cent. While there are over 60 SD-WAN mainstream vendors to consider, not all technology partners are equal. **There are capability differences between vendors. The overall SD-WAN capabilities are also limited to the environments that an individual vendor may support.**

The network overlay offers an over-the-top capability to a WAN where a virtual network is typically created to run across the top of the physical infrastructure. This set-up offers immediate improvements in automation, visibility, performance and network management. Traffic engineering can improve application-level performance.

The carrier underlay, however, starts to integrate the physical and logical solution into one platform. This provides the ability to deliver policy orchestration for appliances at the core of the network, which is important for linking different connectivity estates, OSI layers and supporting multi-vendor environments. Carriers can also better apply technologies such as AI/ML to move environments, and better manage 'own' and 'third-party' networks to deliver an end-to-end business class service.

Private and In-Region Peering

SD-WAN is also changing peering. In the past, network capability was determined on the level of engineering, especially in private MPLS environments. Today it is also measured by how well networks are peered with each another as the public Internet moves from 'best effort' to 'business grade.'

Private peering, especially in-region private peering, will be more important for delivering a high-quality service with fewer router hops and the lowest possible latency intervals for the most mission-critical workloads, such as voice and video. Direct, private connections between two carriers also avoid congestion in many intermediate transit links, such as a third-carrier with a slower speeds.

In-region private peering is also important to address challenges associated with the growth of regional traffic and variability in traffic patterns, which will only be exacerbated with the rapid expansion of remote and distributed workforces.

While SD-WAN overlay capabilities can determine the best links and paths to take by matching the attributes of the application to the network (e.g., latency and jitter), carrier underlays provide additional tools to manage the telecom infrastructure of own and third-party networks. In some cases, this can even extend to offering SLAs over public Internet including third-party ISPs.

Carrier underlay also opens the path to other capabilities, such as Inter-Carrier Orchestration. The latter monitors the performance and inventory between own and partner networks, performs functions such as the automated ordering and provisioning of resources, and provides an end-to-end view of network status.

Recommendations

Carrier Underlay and Overlay Offer a Holistic Approach

As carriers manage the physical infrastructure, they are best-placed to deliver a holistic capability, which brings together physical and virtual capabilities of SD-WAN into a single integrated platform. Some carriers are further along this journey than others. This approach helps to support multi-vendor environments, expand service domains and deliver consistent services across 'own' and 'third-party' networks. Ultimately, network services need to keep pace with cloud services and become more dynamic and intelligent to meet rapidly changing business requirements.

Look for Better Multi-Vendor Support to Correlate Underlay with Overlay

With over 60 vendors active in the promotion and selling of SD-WAN services, the market is fragmented. Enterprises will want visibility end-to-end, across all networking environments and to safeguard against potential of vendor lock-in for just one. A carrier underlay strategy offers a path that promotes interoperability between hardware and software vendor products and visibility that can extend across the entire network, including third parties. An intelligent network is a foundation for offering many capabilities such as AI/ML to drive continuous value to business.

Plan for SD-WAN Converging with Branch

While most businesses still have a significant number of appliances on-site, SD-Branch offers NFV capabilities in areas such as load balancing, security and WAN optimisation, which can be provisioned as instances, replacing the need for purpose-built hardware. There are also options for universal CPE (uCPE) to provide SD-WAN, plus critical L4-L7 functionality through a single appliance. This will dramatically reduce the hardware on-site and improve business agility in changing the network resources required for the branch instantly and remotely. This is a relatively new area with customers conducting trials and proof-of-concept, but enterprise customers should consider the longer-term implications of such capabilities and ensure that it is in their provider's roadmap.

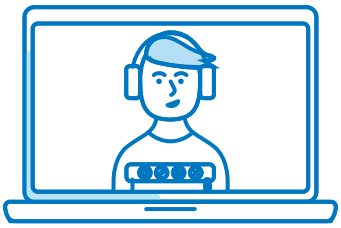
SD-WAN Managed Services

There are many options for managing SD-WAN solutions ranging from a DIY approach, co-managed to the fully managed service. Based on GlobalData's research, enterprises prefer managed service models due to the complexity of network integration, the orchestration of policies, ongoing governance, compliance and security. Particularly in a multi-service environment, a managed service removes the need for enterprises to manage multiple vendor relationships (private networks, public Internet, SD-WAN and various network functions/appliances) and the complexity in trouble-shooting. Given the different traffic requirements in regions, many enterprises have opted for networks that consider local/regional needs over standard single global contracts.

Connecting International businesses to Asia and Asia to the world enabled by our people, innovative technology and partnerships

Adaptive Networks

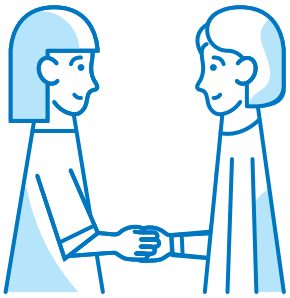
Data Centre &
Cloud Transformation



Modern Workplace

Service Accelerators

Strategic Alliances



Industry Solutions

About Telstra

Telstra is a leading telecommunications and technology company with a proudly Australian heritage and a longstanding, growing international business. Today, we operate in over 20 countries outside of Australia, providing data and IP networks and network application services to thousands of business, government, carrier and OTT customers.

About VMware

VMware SD-WAN by VeloCloud simplifies branch WAN networking by automating deployment and improving performance over private, broadband Internet and LTE links for today's increasingly distributed enterprises, as well as service providers.

Why VMware SD-WAN with Telstra Managed Services

VMware SD-WAN, provided by Telstra, is a pioneer in branch networking with a solution that combines the economics and flexibility of multiple WAN transports with the deployment agility of a cloud-based service. VMware SD-WAN provides a Cloud-ready solution delivered over Telstra's global network as a comprehensive managed WAN service.

Contact your Telstra account representative for more details.

tg_sales@team.telstra.com

telstra.com/international/ManagedSD-WAN

2020.08.20 v120 CCoE