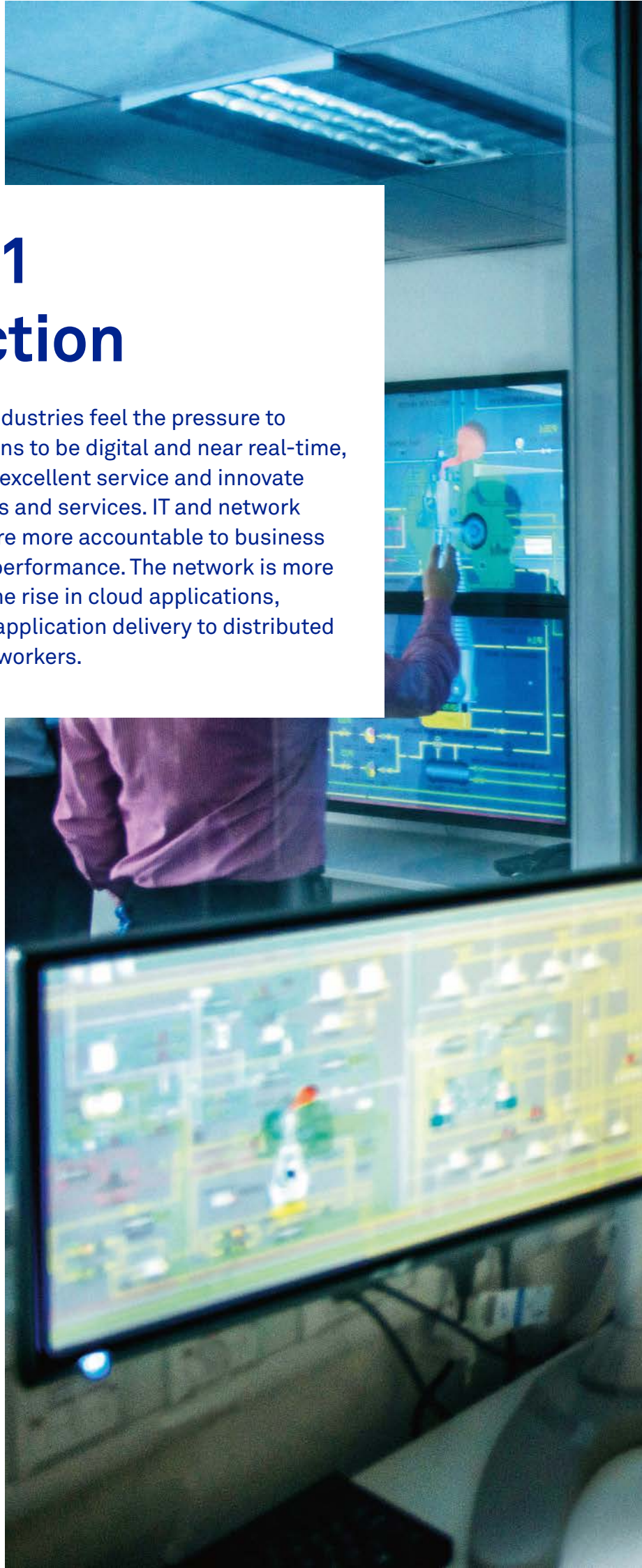
The connectivity guide to successful SD-WAN

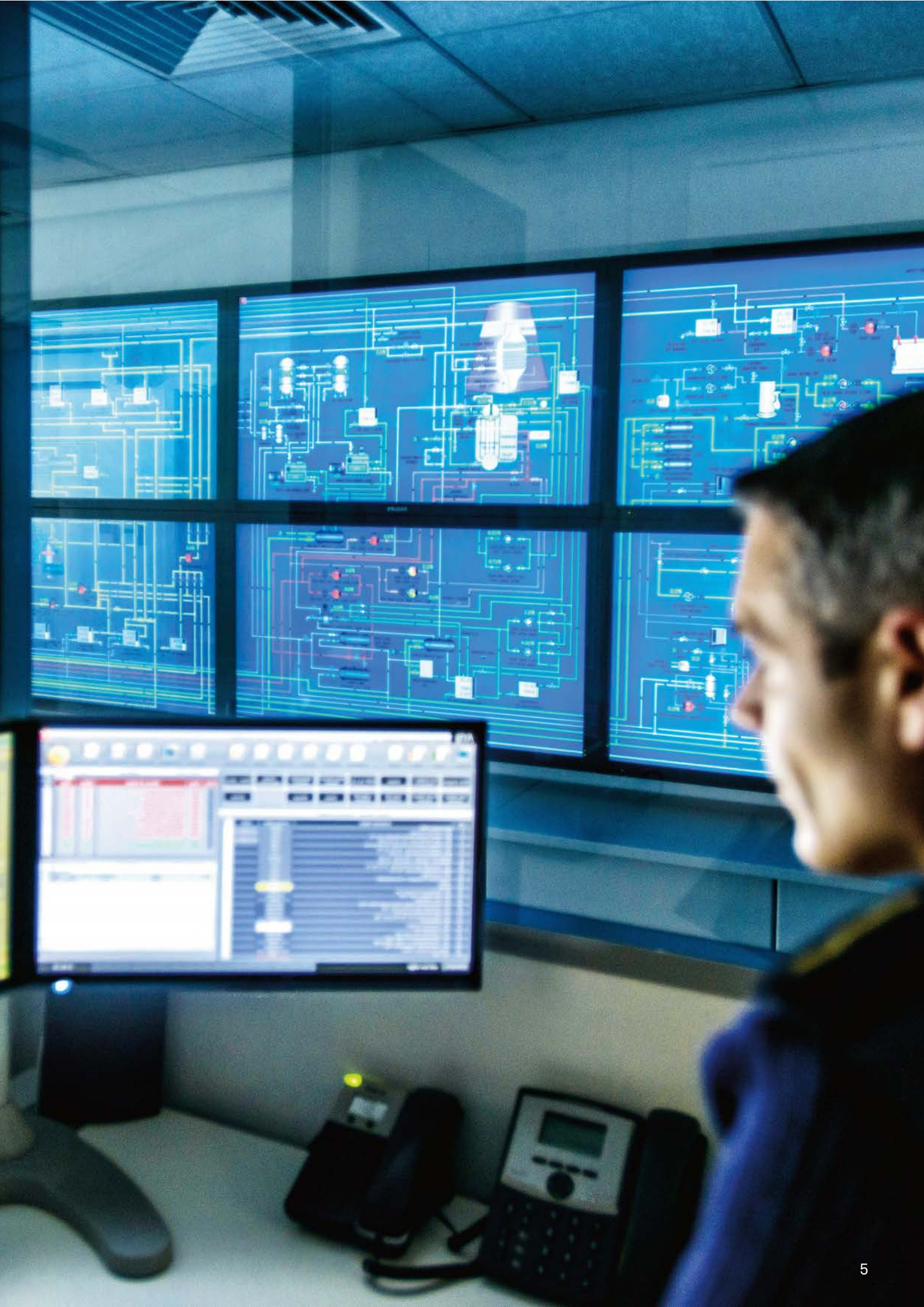
Key buying considerations for WAN transformation

What's inside

Section 1
Introduction

Enterprises across all industries feel the pressure to transform their operations to be digital and near real-time, provide customers with excellent service and innovate faster with new products and services. IT and network infrastructure leaders are more accountable to business leaders for application performance. The network is more business-critical with the rise in cloud applications, and the need to secure application delivery to distributed enterprises and mobile workers.





Software-defined wide area networking (SD-WAN) is a hot topic in enterprise network decision-making. Besides the obvious cost appeal of switching to cheaper broadband and combining bandwidth, the ability to help control applications running across the WAN is even more attractive given the growth of multiple clouds and applications. But the enterprise route to SD-WAN is not necessarily straightforward or easy.

SD-WAN is an overlay network that still depends on a high-quality physical underlay network, and low-cost broadband is not a 'one size fits all' connectivity option that suits every application, user and location. This can lead to congestion and application performance issues at the branch for end users. Heavy users of Voice over Internet Protocol (VoIP) and video conferencing and latency-sensitive applications need a high-quality uncontended business connection not just the lowest-cost internet connection.

Accessing cloud-based Office 365 and other Software as a Service (SaaS) applications becomes a problem if there is bandwidth degradation, congestion and delay. The biggest risk is hard downtime. Downtime means lost revenue, lost productivity, frustrated workers, and a poor experience for customers and partners.

This buyer guide is designed to help:

- Raise the issues and considerations to assist enterprises in deciding on a strategic connectivity plan or a more successful network transition
- Highlight the practical network choices of enterprises across different sectors
- Identify the factors to consider when choosing suitable connectivity

1.1 Key Considerations

Low-cost broadband is not a 'one size fits all' connectivity option: Low-cost broadband has gained availability and popularity for WAN connections, but it is not always a straight-swap or predictable alternative for private WAN and high-performance connectivity to business critical-applications. Getting it wrong can lead to degradation in application performance, a slow user experience and downtime which impacts overall business productivity and support teams with stretched resources. Business-critical applications being used at a branch site need to be considered and also whether private WAN connections may be needed or dual private and business-grade Internet connections.

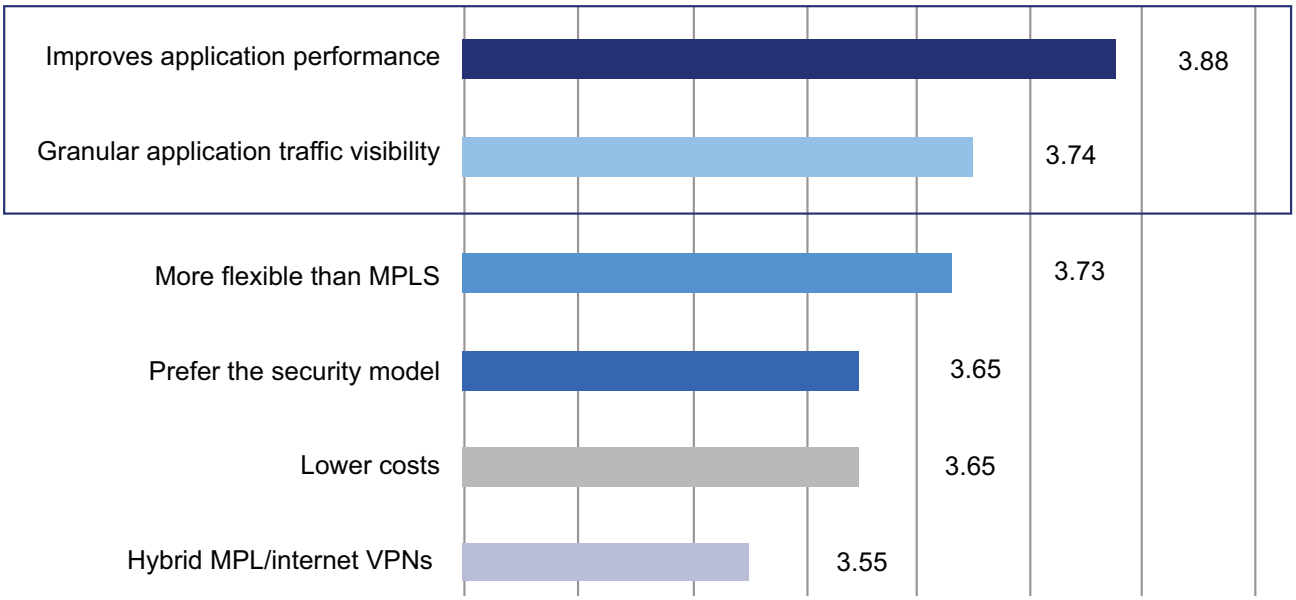
Enterprises are moving workloads to multiple clouds: A connectivity strategy needs to support a growing mix of private and public cloud services, and assert control over the type of flexible network infrastructure needed to support these. For many enterprises, cloud services snuck up on the company over time. Network managers should consider the range of cloud applications being used now and in the future, including

Infrastructure as a Service (IaaS) from public cloud providers, SaaS applications and other private cloud environments.

Network managers should not just focus on cost savings or replacing a private network service (e.g., MPLS) for its own sake: Early SD-WAN customers were driven by lower network costs or the opportunity to replace MPLS but neither is a good long-term motivator for deploying an SD-WAN service. Any network transition or connectivity change requires a complete review of applications, provider agreements, and network design before deploying any new network services at scale.

Many customers expect to realize some cost savings, but SD-WAN's other benefits outweigh them: Ovum's survey research finds that after gaining some deployment experience, customers have come to realise that application performance, flexibility, and agility of their WANs are the major benefits of SD-WAN. In Ovum's enterprise surveys, cost generally falls around fifth place.

Perceived enterprise value of SD-WAN features



Source: Ovum Enterprise Network Services Survey

Section 2
Connectivity checklist

2.1 Application and Cloud Architecture

While the enterprise network has long been a critical platform, its primary focus has changed. The primary goal was once site-to-site connectivity. Now the enterprise network helps provide connectivity from sites, from remote employees and from external partners to applications running across a mix of public and private clouds.

An enterprise migrating network architectures takes a risk that their changes may fail to deliver. This is true for enterprises of all sizes, but especially for those with a network of distributed sites, some in remote areas with limited connectivity; and if there is a need to connect out-of-network, whether its mobile and remote workers, off-net Internet of Things (IoT) connectivity, third-party suppliers, clients or partners.

An enterprise network change requires a complete review of applications and cloud architecture, both the current state and future plans. Enterprises need to make sure that any proposed connectivity solution helps with improving access to applications and overall performance.

Business-Critical Applications

Consideration: What are the key business applications being used at each site and how are they accessed by on-site, remote or mobile workers?

The key challenge for network managers is how to get the best possible access, performance, cost and security for all of these employees.

- How is the user experience for employees?
- How often does the network response time interfere with their daily productivity?
- Is there near real-time visibility into local application performance?

Business transformation is happening across all industries, from content and media, to banking and finance, manufacturing and retail. Enterprises are becoming more applications-driven, and they rely on their networks to help deliver those applications, content and business transactions.

Software, media and content companies require huge bandwidth for software and content distribution. Manufacturers have invested heavily in ERP applications to closely integrate their supply chains to support just-in-time production and have also invested in networks to support these enterprise applications. Retailers that have been devastated by the rise of e-commerce are using near real-time analytics to drive better foot traffic into their stores and deliver personalised marketing.

The way of working for enterprises, large and small, has changed, with increasing reliance on VoIP and collaborative audio and video conferencing and file sharing for critical communications. Remote users require significantly more bandwidth especially when using video, but they also need to securely access cloud applications.

The sheer number of enterprise applications being used has increased dramatically together with the number of applications hosted in a mix of public and private clouds: SaaS applications such as Microsoft Office 365, Googlesuite, Salesforce, Infrastructure as a Service (IaaS) from Microsoft Azure or Amazon Web Services and ERP systems, Business Intelligence (BI) databases and big data systems in private clouds.

An important and growing share of the traffic between enterprise VPN sites is now internet traffic. Latency, but also packet loss, can be negatively impacted if the traffic from local sites goes to the central site first before reaching the cloud data centres. This causes suboptimal performance for end users. As a result, many businesses are now increasingly looking at having a more distributed ICT architecture with more local internet breakouts, which however still need to be secure.

For SaaS applications in the public cloud, policy control and class of service can be used to prioritize these applications over Internet traffic combined with using a private connectivity gateway to the public cloud provider. A cloud gateway can be integrated with a IP VPN as endpoints on a private network and are useful not only for security and performance but also ease of managing multiple cloud connections, and changing bandwidth as needed.

What applications are being used, QoS and latency requirements?

	Branch	Head office	Business-critical	Latency- sensitive
VoIP	✓	✓	✓	High
Virtual meeting/HD audio/video conferencing	✓	✓	✓	High
Streaming events/webinars	✓	✓	✓	High
SaaS public cloud applications	✓	✓	✓	Moderate
Private cloud – POS, ERP	✓	✓	✓	Moderate
Sales Wi-Fi	✓	✓	✓	Low
Guest Wi-Fi	✓	✓	✓	Low
Send/receive large file transfers	✓	✓	✓	High

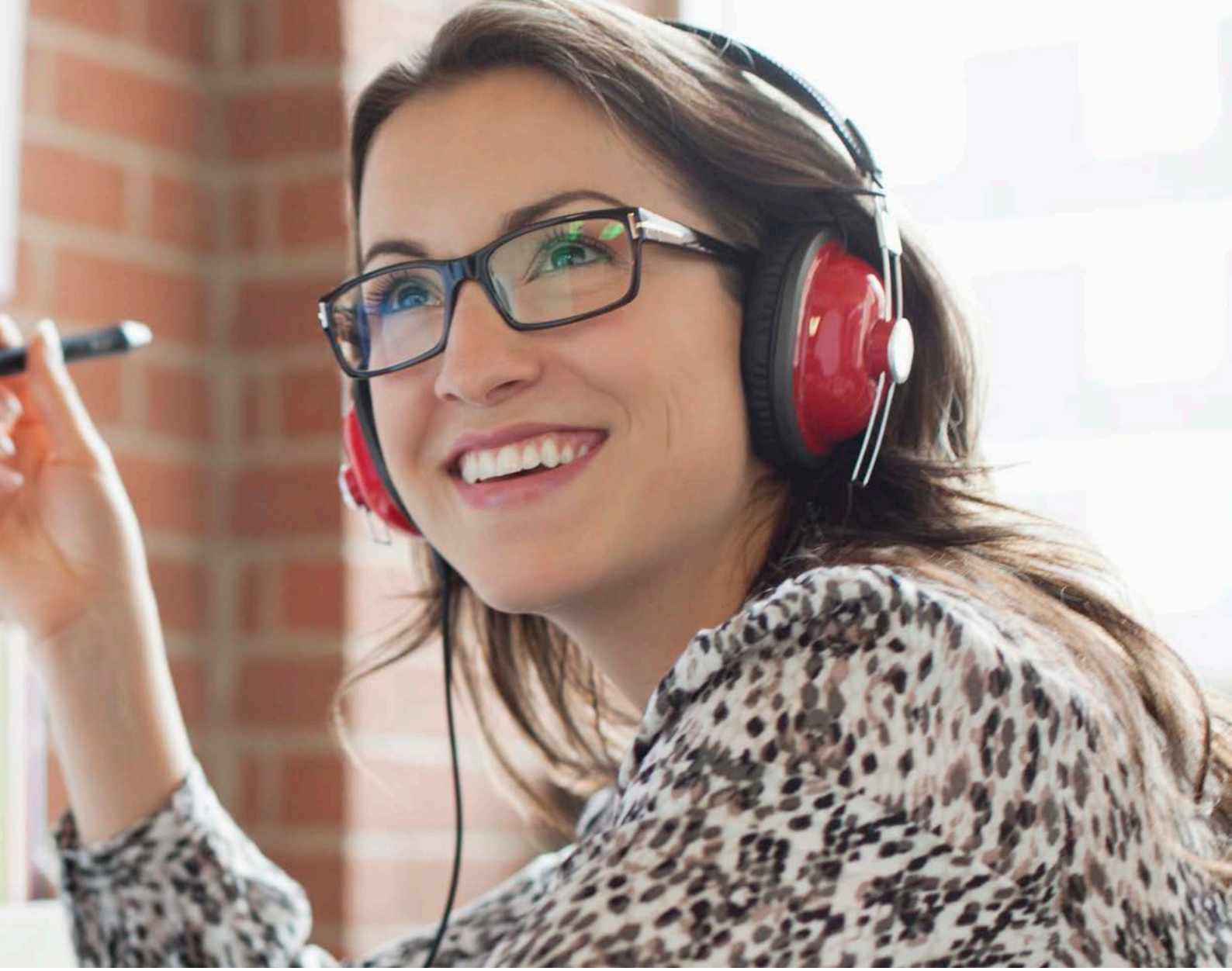
2.2 IT Strategy for Branch sites

Consideration: How many branches do you have or expect to have in the future? What are the key applications used at the branch? How will you manage QoS, latency and security?

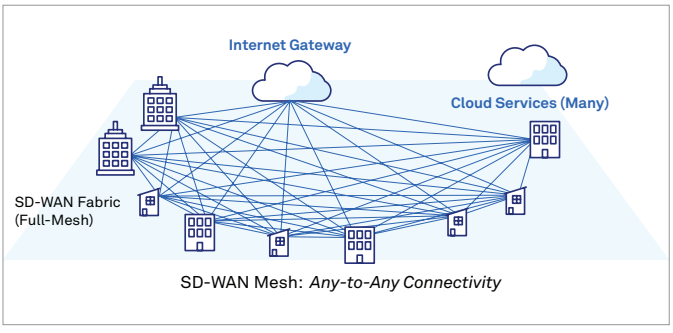
Local branches rely heavily on the network for critical communications, collaboration with headquarters, and access to enterprise applications. Ensuring a more secure network availability and a positive end user experience are top of the list for network managers.

Distributed enterprises with multiple branches, for example, a restaurant chain or retailer that operate on tight margins, are looking for ways they can help reduce operating costs, yet maintain reliable and secure connectivity from branch sites to applications in the cloud.

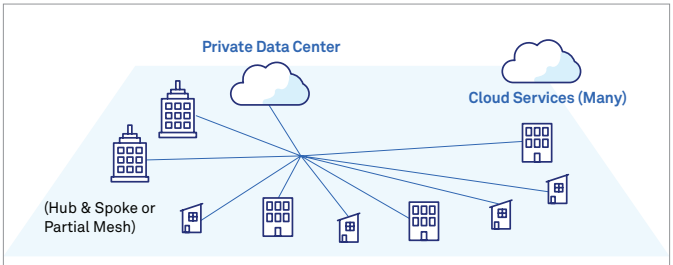
Network architects and managers are being challenged to adapt to increased local demands on WAN bandwidth with the constraints of a flat budget. Low-cost Internet links appear attractive, but quality, bandwidth, resiliency and availability need to be carefully considered, as well as security and business continuity requirements.



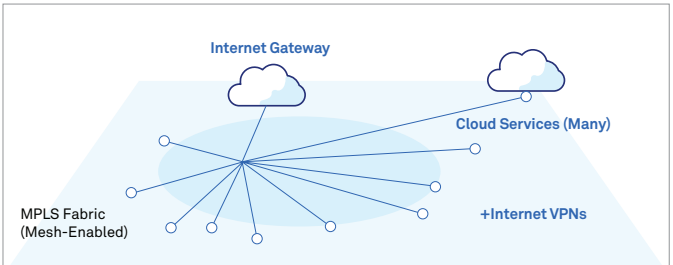
Typical customer network layout



SD-WAN Mesh: *Any-to-Any Connectivity*



SD-WAN Hub & Spoke: *Assigned to Select Applications*



Multi-Network Managed Underlay: *Hybrid Network Flexibility*

Resiliency

Downtime can mean lost revenue, lost productivity, frustrated workers, and a poor experience for customers and partners. Having at least two WAN connections, based on different access technologies for each branch is recommended. For example, using mobile access as a backup for a small site – if the physical link goes down it will fail over to the 4G network. For larger branches, a private dedicated line as the primary with an Internet broadband connection or 4G as a backup.

Branch security

Network security is only as strong as its weakest link. Security at the branch needs to be part of a holistic security strategy including user identity management, firewalls to protect Internet traffic, data encryption, intrusion detection/prevention and updated patches on router software.

Comprehensive security requires IPsec transport encryption, next-generation firewalls (NGFWs) with unified threat management (UTM). Most NGFWs also incorporate a variety of UTM functions, including intrusion detection and prevention (IDS/IPS), quarantining or otherwise deflecting detected malware, and web filtering, which helps detect risky Internet sites and prevents users from visiting them.

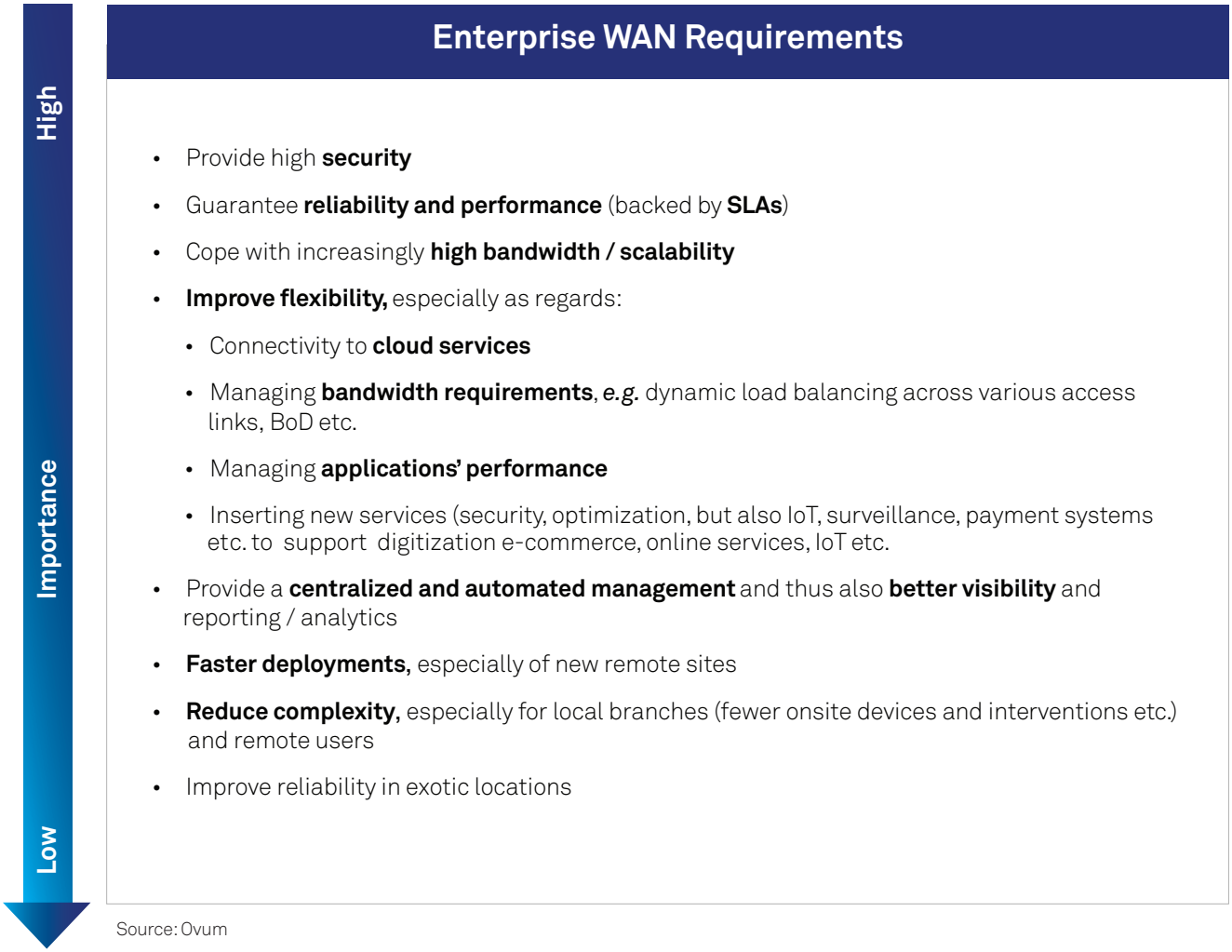
Internet broadband connections to the public Internet present greater levels of exposure to malware and hackers than a single-carrier MPLS network. Direct branch-to-cloud and branch-to-Internet connectivity traffic no longer passes through a centralized data center for security filtering and policy enforcement. Traffic is protected only if a holistic unified threat management security solution is in place at each SD-WAN location. Local internet breakout has become prevalent, so the proposed security solution has to help protect this architectural change. That requires filling in any security gaps to help protect against network intrusions, man-in-the-middle attacks, and malware that can cause denial of service or data theft.

Branch appliances

Enterprises are interested in helping with consolidating and reducing the amount of equipment at each branch that needs to be configured, setup, and remotely managed and supported. VoIP is replacing PBX systems but branches can still have Ethernet switches, branch routers, wireless LAN, WAN optimisation and security firewalls. Each network device has its own complex interface.

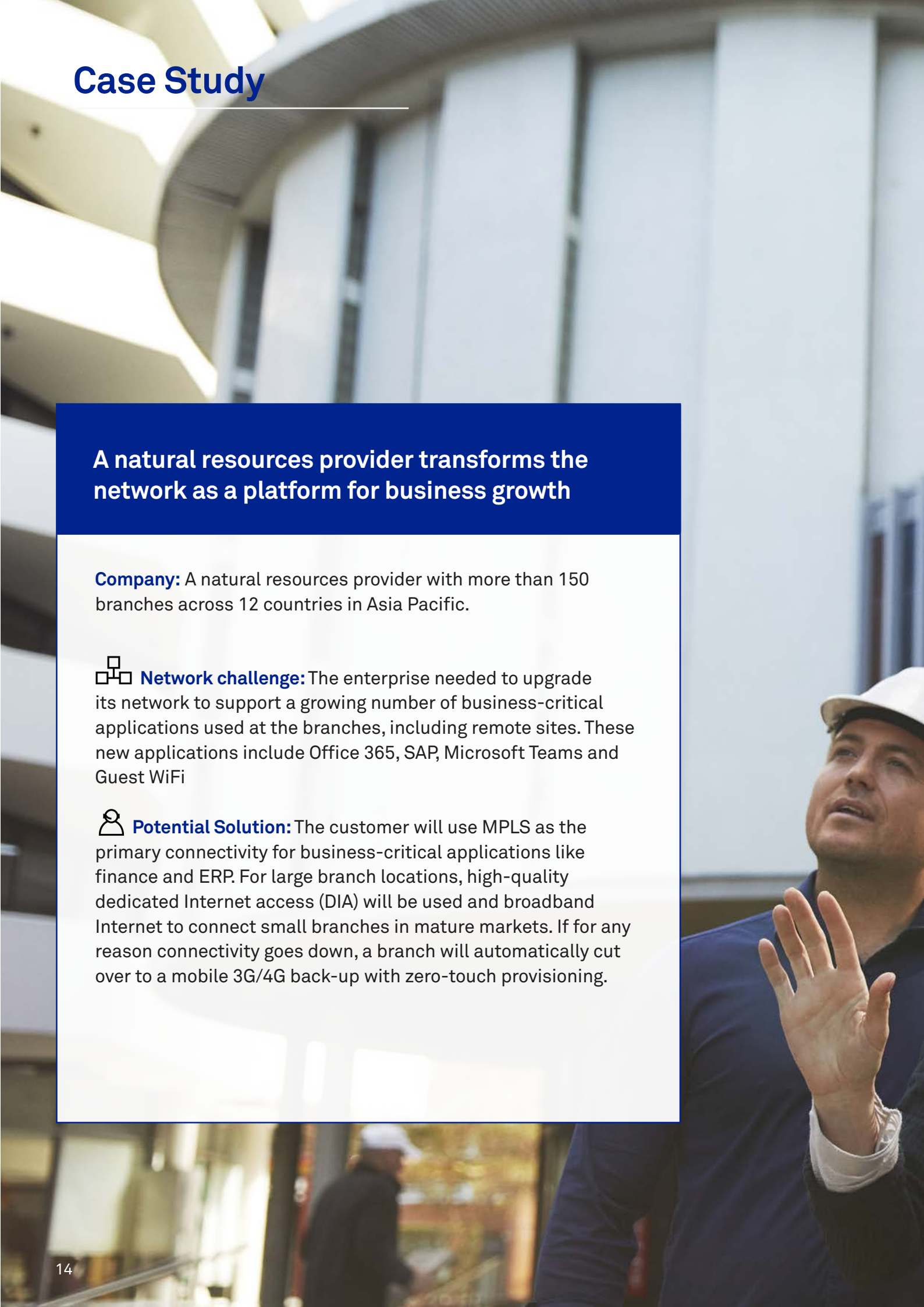
Local branches tend to rely on remote skilled IT personnel to monitor equipment, and to troubleshoot networking issues, such as downtime or slow application performance. For this reason, network managers want to have more control and visibility and near

real-time business intelligence regarding the state of the network and the performance of individual applications. This includes the ability to set application policies not just for performance but also for better security visibility, and to block data and applications. Demand is still in the early stages, but some enterprises are considering consolidating the number of physical appliances and relying instead on virtualized firewalls, remote access, WAN optimisation that can be provisioned on grey boxes. The software-defined branch (SD-Branch) leverages the concepts of SDN and network virtualisation to package the most popular network requirements into a software-based solution running on a unified platform. The virtual network functions (VNFs) can be downloaded and run either directly onto onsite customers' uCPE, including at local branches, but also in the customer's own data center or in the providers' data center (as cloud VNFs).



Source: Ovum

Case Study



A natural resources provider transforms the network as a platform for business growth

Company: A natural resources provider with more than 150 branches across 12 countries in Asia Pacific.

Network challenge: The enterprise needed to upgrade its network to support a growing number of business-critical applications used at the branches, including remote sites. These new applications include Office 365, SAP, Microsoft Teams and Guest WiFi

Potential Solution: The customer will use MPLS as the primary connectivity for business-critical applications like finance and ERP. For large branch locations, high-quality dedicated Internet access (DIA) will be used and broadband Internet to connect small branches in mature markets. If for any reason connectivity goes down, a branch will automatically cut over to a mobile 3G/4G back-up with zero-touch provisioning.

A logistics company builds a robust SD-WAN to deliver great application performance

Company: A logistics and transport provider with more than 50 sites in Asia Pacific, Europe and the Americas.

Network challenge: Employees were experiencing persistent Quality of Service (QoS) issues with voice and video conferencing applications. The team needed to improve network visibility in order to troubleshoot these performance issues and ensure daily executive meetings could take place without QoS problems. As a small IT team, they required a software-based network solution that was low-touch, easy to manage and would be flexible enough to support future business growth.

Potential Solution: The customer implemented a SD-WAN overlay with MPLS and premium Internet access and a secondary Internet backup line for all sites to help ensure that there is a higher level of resilience for core collaboration applications. SD-WAN will use performance-based application routing of business-critical financial, inventory and asset tracking applications. A security vulnerability and threat assessment will be carried out prior to the deployment of local internet breakouts.

2.3 Geodiversity of WAN

Consideration: Enterprises with sites in different regions and countries or remote locations need to consider quality of connectivity options, service levels and local compliance.

For enterprises looking to grow their business, this may involve opening new sites, setting up new data centers, and expanding to new cities. Network teams are expected to enable the business expansion and need to consider locations, whether sites are in less mature markets, the quality of connections and local service providers.

Network service acquisition and installation can be major pain points for customers transforming their networks, and larger deployments require knowledge of local providers and a large variety of network alternatives. Managed service providers have deep managed-services skills that are transferable to provide connectivity, IPVPN, SD-WAN and other network services across many different countries and diverse locations. It's also essential to have a good understanding of the local competitive and regulatory environment. The availability of local support is important to ensure adequate response time and resolution of issues impacting sites and remote user locations.

Managing multiple connectivity types and local providers is a massive challenge in an ever-changing broadband landscape. The large carriers have relationships and contracts with in-country local access partners and can typically offer a choice of access technologies, performance, price etc. from various local partners.

While it is true that MPLS links can be expensive, prices and price difference compared to internet access vary widely depending on countries. Comparing an MPLS link to a low-cost consumer-grade internet connection shows a large price difference. On the other hand, if you compare MPLS to a business-grade dedicated internet access with similar SLAs, the price difference becomes smaller, and indeed can sometimes disappear depending on countries and carriers.

Furthermore, even if there are two different xDSL providers, it is likely that they both rely on the same copper local loop and also possibly on parts of the same equipment in the local exchanges. This could mean that if one service is unavailable, so is the other one. Moreover, laws and regulation can be a limiting factor: tunneling through some countries is difficult and slow or even forbidden (e.g., India, China, Russia). These aspects limit SD-WAN potential in some markets or at least at some sites.

Managed vs. DIY Unmanaged

Enterprises vary widely on the decision whether to outsource WAN connectivity management to a single provider or to work with multiple providers; and on whether to manage networks in-house, or off-load some or all management to

partners. These decisions are driven by many factors including budget, company culture, network complexity, and available in-house skill sets.

Wide area networks are not plug-and-play solutions. Local access connections are typically sourced by the service provider, except sometimes for backup links, e.g. mobile or xDSL backup, but only very rarely for the main MPLS link. The nature of SD-WAN is access-agnostic and this stimulates a bring-your-own-access philosophy. However, early adopter enterprises validate that just because devices are cheap and can be centrally configured does not mean that the network design and the business requirements are less complex. The need for a mature managed-service operating model is as compelling as ever.

The main reason why network operators push for their own local access is the impact on service quality and SLAs in general: if too many sites are based on just any type of customer-provided access, resulting quality may be too low and carriers may struggle to keep up their SLAs. In effect providing the local access helps in order to better combine the underlay (the MPLS network and access technologies) and the overlay (the SD-WAN orchestrating the underlay).

2.4 Performance & SLAs

Consideration: What kind of availability and QoS do you need at your sites? What level of MTTR and support? Do you need near real-time monitoring of network KPIs and application performance?

Important considerations in buying network connectivity are performance and reliability and meeting QoS expectations for end users. An SLA is a good indication of connectivity capability and overall performance, where the provider feels their strengths and weaknesses exist. An SLA is a commercial agreement around average performance levels rather than a per packet performance guarantee. Receiving service credits is small consolation if your connectivity is down for an extended period of time.

MPLS remains very good in terms of traffic separation and prioritisation, and with low latency and packet loss can achieve high SLAs. MPLS definitely still has a role to play for larger sites in general as well as for certain critical, especially near real-time, applications. With best effort consumer-grade internet access, there is no way to achieve really high availability 'five 9s' business SLAs. Some argue that with SD-WAN you can combine two best effort consumer-grade connections to gain higher bandwidth and availability. Yet, this may only improve performance from 'very poor' to 'not quite good enough.' This scenario can also be difficult to achieve for sites in less mature markets, where there may not be two different consumer internet connections to choose from: no LTE (possibly even no UMTS), no coaxial cable, and for instance only one xDSL provider.

Last mile connectivity

Local access or last mile connectivity will have the most impact on applications and network traffic performance for employees and may stop video and voice from performing. Typically, operators will offer a mean time to respond and an availability SLA. Here you need to carefully consider the implications of downtime and the cost of downtime to the business vs. the actual monthly cost of the access line. For example, a 98% availability SLA on a consumer broadband connection is an average over a monthly period, and could mean a site is down up to 10 hours per month – is that acceptable to your business?

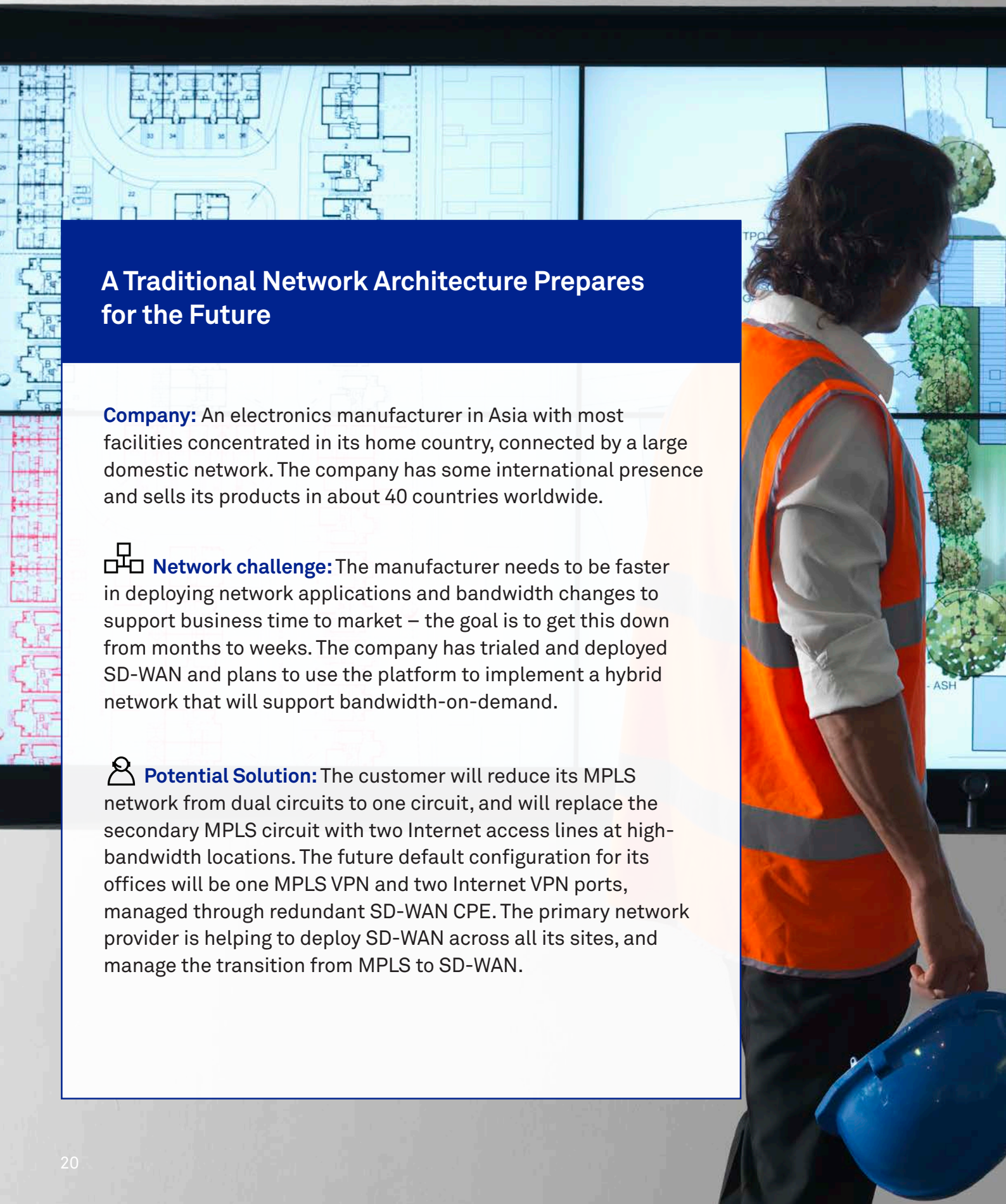
Local support and customer portal

Another consideration is local support availability – is it 24x7 in all time zones or are there limited daily hours? Some response times can be up to 12 hours on connectivity and that is just the time to respond to an issue, it is not a mean time to repair guarantee. With a managed VPN service, a dedicated service manager is usually provided and Level 1 access to field and technical support.

While SLAs are really important, having near real-time control and visibility into network and application performance is a growing requirement. Most service providers now offer online customer portals that report performance metrics in near real-time on class of service, network performance and service level agreements.

The network department can use near real-time visibility into application performance – including the end user experience and 'cost-to-deliver' KPIs – to help satisfy its stakeholders with useful statistics.

Case Study

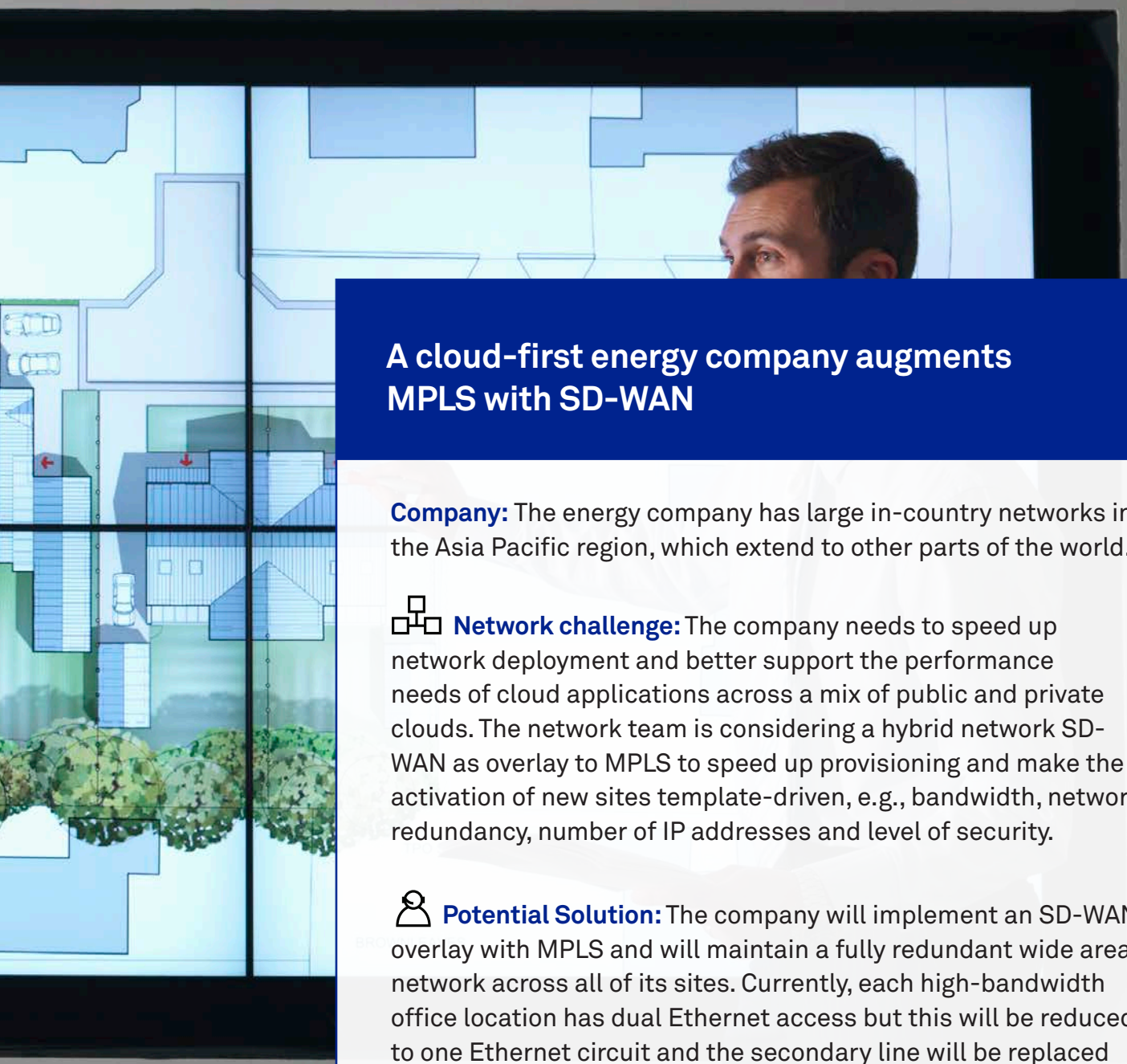


A Traditional Network Architecture Prepares for the Future

Company: An electronics manufacturer in Asia with most facilities concentrated in its home country, connected by a large domestic network. The company has some international presence and sells its products in about 40 countries worldwide.

Network challenge: The manufacturer needs to be faster in deploying network applications and bandwidth changes to support business time to market – the goal is to get this down from months to weeks. The company has trialed and deployed SD-WAN and plans to use the platform to implement a hybrid network that will support bandwidth-on-demand.

Potential Solution: The customer will reduce its MPLS network from dual circuits to one circuit, and will replace the secondary MPLS circuit with two Internet access lines at high-bandwidth locations. The future default configuration for its offices will be one MPLS VPN and two Internet VPN ports, managed through redundant SD-WAN CPE. The primary network provider is helping to deploy SD-WAN across all its sites, and manage the transition from MPLS to SD-WAN.



A cloud-first energy company augments MPLS with SD-WAN

Company: The energy company has large in-country networks in the Asia Pacific region, which extend to other parts of the world.

Network challenge: The company needs to speed up network deployment and better support the performance needs of cloud applications across a mix of public and private clouds. The network team is considering a hybrid network SD-WAN as overlay to MPLS to speed up provisioning and make the activation of new sites template-driven, e.g., bandwidth, network redundancy, number of IP addresses and level of security.

Potential Solution: The company will implement an SD-WAN overlay with MPLS and will maintain a fully redundant wide area network across all of its sites. Currently, each high-bandwidth office location has dual Ethernet access but this will be reduced to one Ethernet circuit and the secondary line will be replaced with two Internet access lines. The customer believes this will maximize the value of SD-WAN. Internet breakout locations are also completely managed. Remote sites used to require expensive satellite connectivity but the customer will migrate to a SDN-enabled WiFi grid system. The company can now have a new location networked for testing and operations within six weeks. This faster site provisioning has helped improve the IT department's relationship with its business stakeholders.

Section 3

Future Considerations

More of the same, but enterprise network evolution will step up complexity and need for managed services.

Enterprise IT decision-makers believe that the trends they need to help them transform their networks and their business are now known and they are in the process of executing on these key trends:

01

Increased connectivity to clouds, and higher demands for performance. This includes a need for dynamic bandwidth with variable pricing, particularly focused on services that are attached to the cloud.

02

More agile services powered by platforms such as SD-WAN and backed by hybrid networking, including MPLS. These services are faster and more flexible to procure and connect, to make it easier to on-board new sites to the enterprise WAN.

03

Customer surveys tell us that the majority of customers are now looking for managed or co-managed offers from service providers driven by the network sourcing complexity and on-going performance management requirements (see our connectivity guide checklist for successful network transformation).

The Connectivity Buyer Checklist for Successful SD-WAN

Cloud and business-critical applications

Question	What is the maximum uptime required by your most critical applications?	Do you have AWS VPCs or Microsoft Azure to connect to your WAN?	How do you securely connect mobile workers?
Approach	• The size of the site, its level of importance, the location, number of employees and the type of applications used will help determine the quality of access and service level required. Using only internet connections, especially low-quality consumer ones, would not be suitable to provide optimized access to cloud data centres, larger sites and critical applications in general. • Consider using MPLS if you have latency-sensitive applications. Internet broadband has a different latency profile and different oversubscription ratios. • For a business sending and receiving large digital files or using streaming applications, upstream and downstream bandwidth capacity are a real consideration which means that a symmetrical high-speed link would be a better option. • For mobile users and home office workers, ensure you have a secure remote access VPN in place.		

Branch IT

Question	Do you want to offload Internet traffic at the branch?	Do you want to consolidate appliances at the branch?	How will you handle branch office security?	How critical is the time to deploy for new sites?
Approach	• For enterprises with branches that will connect directly to the Internet, an established security model for sending corporate WAN traffic over the public internet is needed since traffic no longer passes through a centralized data center for security filtering and policy enforcement. • Security at the branch needs to be part of a holistic security strategy including user identity management, on-premises firewalls to help protect Internet traffic, data encryption, intrusion detection/prevention and updated patches on router software. • Enterprises sometimes wrongly assume SD-WAN has integrated security. Consider carrying out a security vulnerability and threat assessment prior to deploying SD-WAN and local Internet breakouts.			

Performance and SLAs

Question	How much downtime can the business withstand at the branch office (minutes/hours per year – quantify number of 9s)?	Do you need to upgrade capacity?	What type of upgrade – best effort ADSL/cable or dedicated fiber?	Do you need bandwidth on demand capability?
Approach	• Having at least two WAN connections, based on different access technologies for each branch is recommended. For larger branches, use a private dedicated line as the primary with an Internet broadband connection or 4G as a backup. • If you need to increase bandwidth in your branches to support cloud migration, consider static bandwidth with predictable flat-rate pricing. If you have occasional or event-driven requirements e.g. to support variable events or times of year, SDN-enabled bandwidth-on-demand flexibility may be a better option. • Check the finer details in SLAs: the mean time to respond vs. repair by site and the availability SLA and access line cost vs. cost of downtime. Also ensure the provider is offering you a customer self-serve portal with near real-time performance KPIs and SLA reporting.			

WAN Geodiversity

Question	Do you need to connect sites in remote, hard to reach locations?	Do you currently use global MPLS?
Approach	• For networks across multiple geographies, consider partnering with a global managed service provider that has existing access relationships with local providers is recommended. • Enterprises that rely on managed services for their WAN today can continue to rely on managed services for SD-WAN. • Enterprises accustomed to running their own ICT infrastructure have a better chance of blazing their own path in SD-WAN; but even for experienced IT departments, the transition is not simple. • Customers with complex MPLS configurations built up over years with global routes that need guaranteed performance; and applications with especially tight performance tolerances can consider keeping this in place. • Hybrid MPLS/internet networking or all-internet? An enterprise in doubt should go to hybrid networking first and map a gradual MPLS exit. To leave MPLS, the enterprise needs strong internal IT competence willing to take on the challenge. It also should have strongly trusted partners and budget contingency to grow the SD-WAN project into a bigger network transformation initiative over time.	

Section 4
Appendix

Author

Sandra O'Boyle, Associate Analyst

sandra.oboyle@informa.com

Ovum Consulting

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Ovum's consulting team may be able to help you. For more information about Ovum's consulting capabilities, please contact us directly at **consulting@ovum.com**.

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 services to thousands of business, government, carrier and OTT customers. Telstra Enterprise is a division of Telstra that provides data and IP networks and network application services, such as managed networks, unified communications, cloud, industry solutions and integrated services. These services are underpinned by our subsea cable network, one of the largest in the Asia Pacific region, with licenses in Asia, Europe and the Americas, and access to more than 2,000 Points-of-Presence around the world.

Contact your Telstra account representative for more details.

Australia

1300 835 787

telstra.com.au

International

Asia +852 2983 3388 **Americas** +1 877 835 7872 **EMEA** +44 20 7965 0000 **Australia** +61 2 8202 5134

Sales tg_sales@team.telstra.com **Channel Partners** partners@team.telstra.com telstraglobal.com