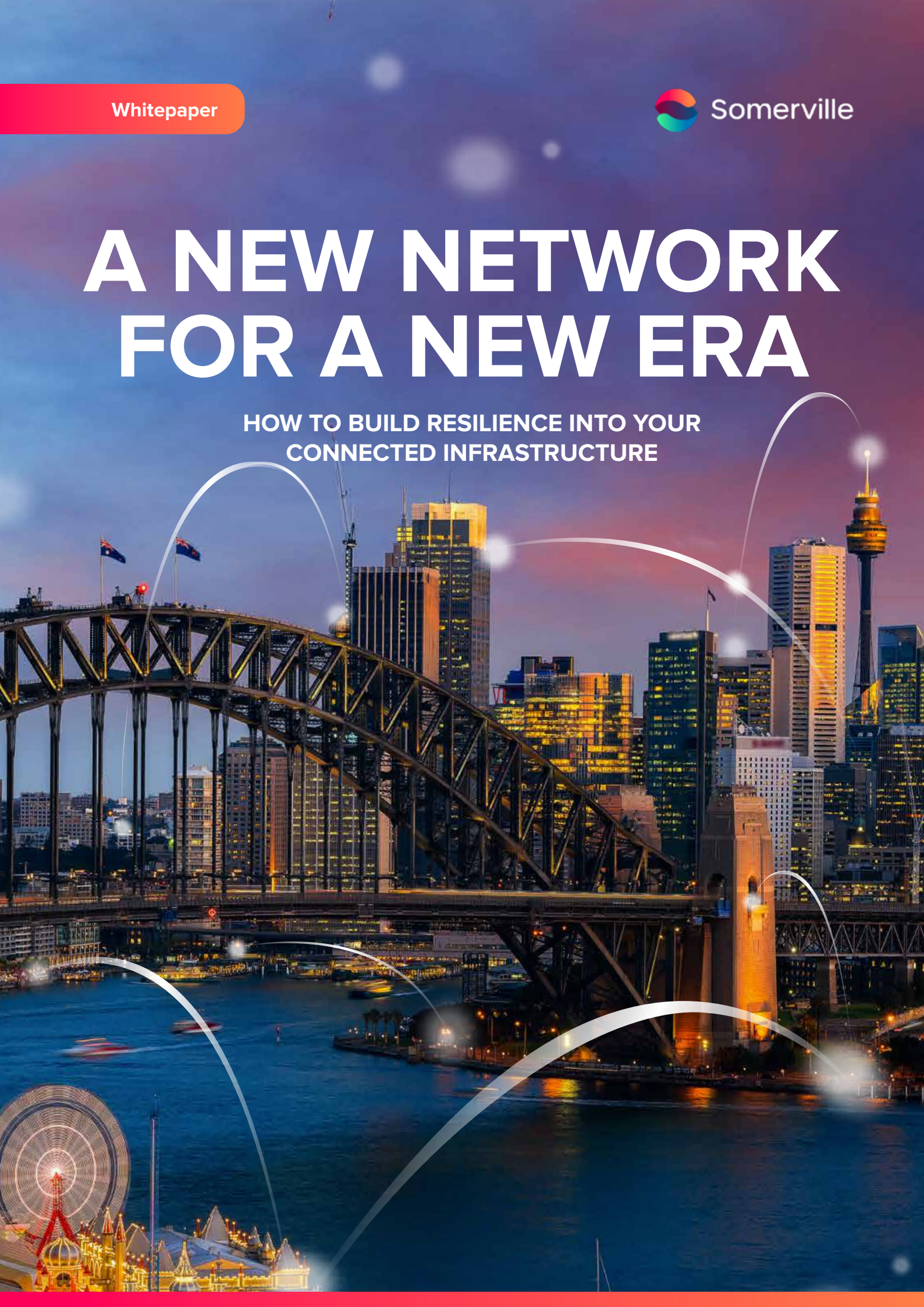
Whitepaper

Somerville

A NEW NETWORK FOR A NEW ERA

HOW TO BUILD RESILIENCE INTO YOUR CONNECTED INFRASTRUCTURE



NEW CHALLENGES IN A NEW ERA

The disruption of the pandemic has forever changed the way people work. Workforces are now distributed across cities and beyond, putting new pressures on long-established network architectures designed for a time when most users were clustered in the head office.

With staff working online from home at least some of the time, continuous access to a reliable, robust network has become critical to maintaining business continuity. The challenge is to give remote workers the same levels of performance, reliability and usability from best-effort home broadband services that were never designed for this kind of usage.

Remote work isn't the only disruptive force affecting the resilience of company networks. Long before the pandemic had even begun, the increasing momentum of digital transformation was pushing companies to increase their investment in cloud applications and services.

More than two thirds (69%) of Australian and New Zealand organisations accelerated their digital transformation last year, according to an IDC survey. Businesses increased their transformation expenditure accordingly, from 45% of information and communications technology (ICT) spending at the beginning of 2020, to 55% in 2021.

Large businesses, in particular, have been targeting investment to fix gaps in their digital resilience that were laid bare during the pandemic. Cisco's ThousandEyes internet monitoring platform, for example, identified a 61% increase in the number of network disruptions across internet service provider (ISP) networks, and a 44% increase on cloud provider networks, during the first months of the pandemic.

In working to stabilise their businesses and embrace the 'next normal', IDC found, 80% of Australian and New Zealand organisations are investing aggressively – the highest level of any countries across the Asia-Pacific region.

Much of this investment is being targeted at cloud platforms, which have become a primary tool for delivering a new breed of applications designed to be more customer-focused, easily accessible and rapidly upgradeable.

Yet cloud, like remote working, requires a different way of thinking about network resilience. Today's networks are structured less like the hub-and-spoke configurations of yesteryear, and more like mesh, with remote and office workers connected to data centres, cloud platforms hosting key applications and each other.

"A lot of pressure is put on traditional network architectures and enterprise networks that were predominantly private," explains Andrew Milroy, founder of digital risk advisory firm Veqtor8, who has increasingly seen clients stepping away from the mechanics of networks to focus on higher-level concepts built around business value and resilience.

"These networks are basically no longer fit for purpose, as we do more and more in the cloud, so organisations are bolting on little bits to try and make it work. But that's not enough."

Just as the pandemic has required a new way of working, supporting that new way of working requires a new kind of network.

To support network transformation most effectively, businesses must build network resilience into a range of network topographies and technologies, each with its own total cost of ownership (TCO) equation and operational requirements. These technologies then need to be manageable in a consistent, effective way.

To build a resilient network, IT leaders need to look beyond the traditional factors, such as bandwidth, contention ratios and integrated office and wide-area network (WAN) topologies. More importantly, they need to focus on providing robust, always-on connectivity between the many distributed parts of the modern enterprise.

This paper explores the changing requirements in this 'next normal', examining the drivers for change and the way new network technologies and topologies are giving businesses the resilience to meet the challenges of the coming years.

ADDRESSING LEGACY CHALLENGES

The operational requirements of new enterprise application architectures have exposed the inadequacies of existing legacy networks, which were generally designed in a different time and place, for different needs.

Enterprises might have fast connections between their head office and hosted data centres, for example, but when it comes to remote sites, many companies still depend on a hodgepodge of bandwidth-constrained WAN technologies.

For remote workers, that often means Australia's 'best-effort' National Broadband Network (NBN) and 4G/5G mobile broadband services. Schools, branch offices, small businesses and other satellite operations also often struggle with network performance.

Organisational inertia has made it hard for many companies to justify the expenditure to change long-established network technologies. However, as Jason Bordujenko, Global Head of Channel Solution Architecture at Megaport, explains, this is creating problems as companies lean heavily on web apps – where latency and security are even more important than bandwidth.

"Organisations using traditional hub and spoke network architecture often run into performance challenges," he says. "They treat your infrastructure as the centre-point of your data universe, forcing cloud traffic to traverse paths that may not be optimised to achieve the required performance and availability for a given cloud service workload.

"As services stretch across different clouds and disparate geographies, not only does network traffic greatly expand, but service quality increasingly depends on the quality of connections between components of the service."

Thinking about networks in terms of service quality, rather than hard metrics like bandwidth or latency, is critical to making next-generation enterprise networks as resilient as possible. But it's a big step for companies that have long been forced to develop network infrastructure expertise to link their many sites.

To ensure ongoing suitability for business application requirements and the ever-changing distribution of devices, it's best to think of connectivity in terms of services. These services are developed, delivered and managed by third parties that worry about building the end-to-end connectivity the end customer requires, and managing the technologies necessary to achieve appropriate performance.

"For most companies, there's a limit to what you can do when you have to manage a lot of legacy infrastructure," says Milroy. "Network modernisation addresses a lot of the complexity organisations have to deal with, and service providers are helping by moving towards software-defined networks that have a software layer above the network architecture."

TOWARDS A BETTER APPROACH

WITHIN THE CONTEXT OF TODAY'S DIGITAL TRANSFORMATION EXPLOSION, MANY COMPANIES ARE LOOKING FOR A DIFFERENT WAY OUT OF THEIR LEGACY TRAP

...and software-defined WAN (SD-WAN) technology has emerged as the best alternative.

IDC, for one, has called SD-WAN a 'game changer' and a key enabler of network transformation. It notes that "the goal of any enterprise should be to improve the application experience for stakeholders irrespective of the application location and device accessed without compromising security".

By enabling network infrastructure to be monitored and managed in software, SD-WAN allows service providers to dynamically change characteristics. It can alter the allocation of bandwidth and the routing of particular types of traffic – reducing latency, for example, by allowing cloud traffic to bypass the network core.

The software-enabled nature of SD-WAN has also made it a driver for better network security and access control – crucial in managing today's tsunami of cybersecurity attacks. It allows for tight integration with cloud security solutions. These can include secure access secure edge (SASE) frameworks, which can simplify network security by integrating a number of cloud services with SD-WAN.

"The objective of network resilience is to ensure reliable connections that are always up and always fast," says Simon King, Director of Systems Engineering at Cisco ANZ. "SD-WAN and software-defined access have evolved traditional connectivity methods to introduce new functionality aimed at ensuring high-quality connections for all.

"The underlying network is similar, but there has been real advancement in the overlay features. The intelligent central control, programmability and use of cloud-based services offer a big leap forward."

These features include the use of real-time broad performance measures to make better path decisions; automated rollout, policy and profiles, and application programming interfaces (APIs) to reduce errors while moving more quickly than traditional rollouts; and greater awareness of user and application intelligence to enhance security.

According to Milroy, service providers "really have an opportunity to orchestrate these services and bring together all of these different pieces of equipment, infrastructure, and legacy within the cloud. It's a very clean, attractive offering – but for it to work optimally, you have to become cloud-native."

With SD-WAN rapidly becoming the default network architecture for increasingly cloud-reliant businesses, the market is rapidly moving to embrace it.

Australia's SD-WAN infrastructure market is expected to grow at 29.6% annually through to 2024, according to IDC. It sees adoption accelerating as SD-WAN technology "becomes the primary means of connectivity within an enterprise".

SD-WAN "addresses the need for improved application performance and increased network security as the number of remote users increases and as enterprises continue to migrate applications to the cloud," says Nicholas Harders, APJ Solutions Director with Aruba, a Hewlett Packard Enterprise company.

"Modern network automation and orchestration approaches deployed in cloud architectures dynamically adapt to changing network conditions and workload transitions, providing a level of network resilience far superior to what is possible with more traditional network management and operational tools."

"The business impact here is an improved level of network resilience, security and, most importantly, application availability with SD-WAN and SASE architecture."

BUILDING A BETTER NETWORK

THE IT LEADER'S CHECKLIST

Designing and implementing a modern network architecture is a significant step, and one that you should undertake carefully and deliberately. To build a better network, you should:

- ✓ Weigh the limitations and technical challenges posed by legacy networks
- ✓ Evaluate the ability of potential service providers to address the pain points revealed during the pandemic
- ✓ Decide whether you're aiming to consolidate your systems in a single cloud, or will pursue a multi-cloud strategy, mixing architectures and capabilities
- ✓ Develop strategies for monitoring and analysing network performance
- ✓ Evaluate current security exposure and ensure that proposed modern network architectures address this
- ✓ Consider how SD-WAN capabilities can standardise your network interfaces and integrate with broad security frameworks like SASE
- ✓ Ensure you have an incident response plan in place, and test it regularly
- ✓ Remember that business resilience isn't just a consequence of cyber attacks, and relies on a whole range of business capabilities functioning robustly through disruption
- ✓ Consider who is accountable for which parts of the revamped business and network, and do it early on so there are no questions later
- ✓ Define SLAs that will help you meet your resilience requirements, and ensure they are clearly communicated to your managed service providers.

CREATING EFFECTIVE IP NETWORKS

Recognising that the reality of new digital businesses requires a completely different approach to connectivity, CSPs are increasingly selling communications services as completely managed internet protocol (IP) networks. They provide an IP 'dial tone' at every connected site, then use SD-WAN to coordinate the range of equipment and communications services working to maintain it in the back end.

This 'one network' approach leverages diverse connectivity options to deliver connectivity across a range of network architectures. It can span fibre and leased lines as well as the hybrid, hyperscaling multi-cloud environments required by today's digitally enabled environments.

The manageability and integration of SD-WAN allows providers to sell communications outcomes based on service level agreements (SLAs) that deliver a certain quality of connectivity, not on bandwidth. They also offer flexibility, allowing companies to easily adapt to changing user and application activity.

Backed by guaranteed resilience capabilities, this new network model means companies no longer have to worry about building networks from point to point. They can instead think only of communications services as providing resilient IP connectivity between all their networked resources.

"People are moving more into talking about network as-a-service today," explains Milroy.

While IP service guarantees simplify the idea of next-generation networking conceptually, he says, they need to be sure they address the other issues it creates – such as maintaining visibility of the user and application traffic traversing the network.

"Companies have put a lot of demands on their network infrastructure and need performance and uptime," Milroy says. "They have nonstop requirements around compliance and other issues all the time. IT teams have been able to get the visibility they need while paying different rates for the performance, capacity requirements, reliability and availability that they're looking for."

For all the benefits that managed IP networks provide, many companies may struggle to embrace them conceptually, given lingering attachments to conventional notions of relatively static networks – where services like multiprotocol label switching (MPLS) were previously the favoured mechanism for improving speed.

Nevertheless, as more enterprises move away from static legacy environments and to managed IP networks, they must think about how to abstract their new services from the architectures they are running on. They need to ensure that the network continues to support the business, even as technology moves on and new use cases continually change the way the network is used.

To realise those benefits as effectively as possible, businesses should deploy applications in a cloud-first architecture that is more distributed, more flexible and more resilient than ever. While legacy applications will inevitably persist for some time, the inexorable migration to modern IP networks will ultimately guide companies into an environment where every application operates like it was built for the cloud.

USING A MANAGED SOLUTION

The transition to new network architectures will continue in stages, with companies targeting a range of new network states in which each has its own network resilience profile – and is delivered by managed network service providers.

Long-term relationships are key to ensuring those architectures continue to meet business requirements, Aruba's Harders says, noting that "companies typically enjoy the greatest benefit from a network investment immediately following the deployment."

"Beyond this, the cost to maintain the infrastructure slowly increases over time, and the focus on the network becomes reactive instead of proactive. A managed network service addresses the ongoing operational aspects of the network, but also delivers proactive services to fully realise the value of the original network investment."

The nature of that investment varies significantly from company to company. While 31% of executives responding to a recent IDC Cloud Pulse survey said they anticipated having a single cloud environment in place by 2022, 29% said they would have multiple cloud environments for migrating workloads and data.

Some 18% said they would have multiple cloud environments with little to no interoperability between them. This would leave each cloud environment to implement its own form of network resilience internally.

By contrast, 15% said they would have multiple cloud environments that run seamlessly across different clouds. This would allow resilience to be built into applications that can dynamically adapt to changes in individual clouds' performance and availability.

Just 7% of the surveyed companies said they would have a fully managed multi-cloud environment, in which common tools and processes supported the seamless operation of applications across different environments.

Each of these end states correlates with a different mix of service provider capabilities and expectations, reflecting the range of relationships that enterprises may have with their network service providers.

Those relationships will be increasingly important as companies look to augment their networks with cutting-edge capabilities from managed network providers. These include correlation of intelligence by using AI predictive analysis; pervasive security that's built into network services to reduce potential damage from a cyber attack; and the emergence of edge computing, where workloads are moved into the network itself.

"Taking the opportunity to transform on- and off-premise technology offers much more than compensation for the traditional network architecture," says Cisco's King.

"Security can increase markedly with rapid adoption of cloud-based security functionality; awareness of performance and true user experience can be measured like never before with modern application and network (full-stack) observability; and modern networking solutions such as cloud-based dashboards and control centres offer consistent and programmable control with simplified operations and reduced error."

Such capabilities will build on the aggregated connectivity services offered by providers that actively manage a broad range of physical network services. These range from dark fibre to leased-line connectivity to managed content delivery network (CDN) services from a variety of providers.

"As a longstanding partner of tier one carriers nationally, we have built a network with almost 100% geographical coverage that lets us offer a range of connectivity services to organisations anywhere in Australia," explains Osh Ranaweera, National Network Manager at Somerville.

Ranaweera has directed the evolution of the Somerville Gateway, a concept that allows a single, managed secure point of access to the Somerville's national network, private cloud as well as public cloud services such as AWS and Azure – a complete, end-to-end connectivity solution.

Because customers don't have to worry about the underlying complexities in the IP network, they can focus on improving their business application architectures and outcomes – and leave Somerville to manage its Australia-wide and global network through its Australian-based headquarters.

"We want to provide our customers with a seamless experience through an array of connectivity services including SD-WAN solutions that address a wide range of enterprise requirements," Ranaweera explains. Because we own our national network, we maintain control of the complete network stack and everything in the service layer, which is how we provide better value and outcomes to our customers. The more we can control and manage, the better our SLAs can be for our customers."

HOW INTERFLOW MODERNISED AND SECURED ITS NETWORK

As a leading provider of trenchless pipeline solutions, Interflow's 600 employees are carrying on a proud legacy that has spanned more than 85 years. But when its old legacy network and 'scattergun' IT management became a problem, the company embarked on a major upgrade that would give it the modern, manageable, highly secure architecture that a modern business needs.

"We had a lot of manual process, which was cumbersome," IT technical services manager Daniel Bogos explains. "And with Interflow's growth, there was a lot of opportunity to take things forward from an IT perspective. We were looking for a partner that could take us on an IT journey."

By working with Somerville, Interflow was able to lay out a plan for a far more robust, resilient network strategy that would modernise its architecture and suit its needs for the long term.

This included a significant upgrade to its HPE Aruba network infrastructure, installation of an enterprise-grade Sophos XG Firewall in every branch, and a major process overhaul that aligned its security practices around the Australian Cyber Security Centre (ACSC) 'Essential Eight' and its 37 strategies to mitigate cybersecurity incidents.

Supported by Somerville's expertise in connectivity, the modernisation project has driven a major digital transformation across the Interflow business. The company is now enjoying greater visibility, easier IT management, better employee mobility, and improved bandwidth performance and business operations – providing a high level of cyber resiliency and overall peace of mind.

"Somerville ticked all of the boxes and understood the company's business requirements and objectives," Bogos says, "and is now taking us on a massive IT journey."

BUSINESS BENEFITS

OF A BETTER NETWORK

The shift to managed services has simplified one of the three main pillars of the modern enterprise network – the IP network. Along with data and applications, and the people and devices comprising the modern workplace, IP networks had been one of the key management challenges for modern organisations.

Yet as networked enterprises become more complex and the cloud disrupts everyday operations, it has become harder for all but the biggest companies to effectively manage multi-cloud connectivity in-house.

In a multi-cloud era, where reliable and flexible network connectivity has become table stakes, companies are increasingly making the strategic choice to entrust their critical business applications and services to managed services specialists. That's because these specialists can provide the guaranteed performance, availability and resilience that are difficult for companies to maintain on their own.

By moving to an IP network managed by an external provider, enterprises can gain benefits including guaranteed improvements in network performance, cost optimisation and security management, and the simplicity of a single bill – all while reducing the need for scarce and expensive internal networking experts.

Thanks to the evolution of network virtualisation technologies, and the maturation of dynamic management technologies such as SD-WAN, today's network architectures offer levels of manageability, security and resilience that were difficult, if not impossible, for most companies to access in the past.

"SD-WAN has the capability to solve the majority of the network and security challenges that the industry is facing today at a reduced TCO without compromising the network experience," says Dileep Nadimpalli, IDC Research Manager for Enterprise Infrastructure. "With a single SD-WAN fabric, enterprises can do away with multiple point solutions covering networking, security and WAN optimisation requirements.

Data, people and devices can now be located anywhere, with robust IP networks providing secure and resilient connections between them, and CSPs managing the details of the underlying network.

This reduces the complexity of a key element of digital transformation and can deliver cost savings. Cisco, for example, estimates that migrating from MPLS to SD-WAN can cut costs by 60% for an enterprise connecting 50 sites at 2Mbps using SD-WAN, and by 70% at 50Mbps.

This investment will not only reduce ongoing costs, but it also will streamline the management of multi-cloud networks by providing access to modern security, access control and dynamic network capabilities.

Nearly half (48%) of IDC respondents said they would be increasing their reliance on advanced automation platforms to reduce the manual management of their network, while 41% anticipate increasing reliance on software-defined networking technologies.

Such technologies are essential to keep up with changing work and business patterns. For example, the increasing maturity of network automation will help companies stay abreast of change and keep up with ever more complex security, scalability, portability and resilience issues.

“It is a journey of network transformation that evolves over time, with additional functionalities and services getting added as per industry demands,” says IDC’s Nadimpalli. “Hence, it is extremely vital to choose the right partner that is abreast with industry changes and requirements, and has long-standing experience in delivering deep technology expertise.”

THE USER’S PERSPECTIVE

Modern multi-cloud networks raise many issues for technical architects, but for the end user there is only one consideration: does the network allow fast, easy access to any resource that’s needed, from anywhere the user is located?

This access must, of course, be provided securely and efficiently, with automation to ensure applications scale with demand, and analytics to ensure that user experience isn’t being compromised by unexpected changes in performance or network structure.

“The demands on networking have become more critical than ever as workers demand their applications not only work but work well, no matter where they were located,” says Megaport’s Bordujenko. “The ability to deliver optimal application performance at the edge needs to be at the forefront of the minds of network architects.”

By engaging with end users throughout the network modernisation process, network architects can better understand what performance characteristics their networks must provide. They will also be better positioned to receive feedback from users whose productivity is the goal of the modern multi-cloud network.

HOW TO MAKE THE TRANSITION:

6 STEPS TO HELP YOU GET STARTED

It's one thing to talk about the benefits of a modernised corporate network, but another entirely to put it into practice. Here are six steps to help you get started – and to guide your transition to a better way of networking that will continue to grow along with your business.

1. Evaluate the cost and limitations of your current network environment.
Consider the ongoing costs, such as capital maintenance and equipment upgrades, and the skills needed to manage them. Compare these with the potential reduction in business uncertainty, improved reliability and strategic flexibility gained by shifting day-to-day connectivity to a third-party service provider.

2. Identify technical issues with the current network, and envision your ideal end state.
Legacy networks are often riddled with inefficiencies, so it typically won't take long to identify potential areas for improvement. Speak with network managers, end users and technical architects to better understand what you're fixing, and how a modern multi-cloud network architecture can help.

3. Expand your network visibility and analytics.
Building a consistent, scalable and responsive multi-cloud network can dramatically improve network resilience. But it's important to ensure that you also have the tools to monitor and analyse ongoing performance against expectations. Even external providers should offer visibility into the network's operation so you can evaluate adherence to business objectives and SLAs.

4. Address security considerations to protect workloads and data from attack.
Expanding network reach, changing usage models and new application architectures have created new security vulnerabilities that must be proactively and continuously addressed. Ensure your new network incorporates robust, AI-assisted security controls spanning threat detection, authentication, vulnerability scanning and other elements across the multi-cloud environment.

5. Extend policy-based network automation.
Network automation is crucial to building networks that are more responsive and aligned with the changing dynamics of today's businesses. Make sure you leverage automation, where possible, so that you can spend less time thinking about the network and more time on improving the business.

6. Discuss your requirements with a strategic partner.
Ensure your partner understands contemporary multi-cloud environments, and the impact they have on networking architectures – and can provide robust managed network services to support this change.

FURTHER INFORMATION

For further information about how Somerville can help you meet the challenges of network resilience, or to contact our technical specialists to discuss your current requirements, please get in touch on 1300 209 233 or info@somerville.com.au.

THANK YOU TO OUR CONTRIBUTORS

OSHADHA RANAWEERA

Manager – Connectivity Services at Somerville

ANDREW MILROY

Adjunct Professor, Principal Advisor of Ecosystm, and Founder of Veqtor8

SIMON KING

Director of Systems Engineering at Cisco ANZ

JASON BORDUJENKO

Global Head of Channel Solution Architecture at Megaport

NICHOLAS HARDERS

APJ Solutions Director at Aruba

About Somerville

As one of the most experienced end-to-end IT service providers in Australia, Somerville has been delivering exceptional service and value to customers for almost 40 years. Our customers come from a wide range of industries, including finance, education, legal, insurance, superannuation and automotive. We believe in forging genuine partnerships with them. We take the time to understand their business needs and internal IT capabilities so we can develop innovative solutions to their IT challenges that will enable change for tomorrow and beyond. Our services include connectivity, security, cloud, modern workplace solutions, and hardware and software procurement. These services are delivered by our Australian-based team of skilled engineers and are backed by proactive 24/7 support, 365 days a year, so organisations can rest assured their critical systems are up and running around the clock.

Somerville Technology Pillars

somerville.com.au 1300 209 233 info@somerville.com.au