Driving innovation and mitigating risk

Navigating global megatrends in a cost-effective manner

verizon business

Introduction

In today's fast-paced and interconnected world, organisations across the globe face an unprecedented need for innovation to remain competitive and relevant. However, the challenges and rising costs associated with the pursuit of innovation can become significant roadblocks. This whitepaper aims to address this concern and explore how organisations can foster innovation while effectively managing risk at a low cost.

The first global megatrend to consider in the landscape of innovation and risk is the rapidly changing face of cybersecurity. With the increasing complexity and sophistication of cyber threats, organisations are compelled to continuously adapt and fortify their security measures to safeguard their assets, intellectual property, and customer data.

The push for digital transformation is another powerful force impacting businesses. Organisations must embrace technology-driven solutions to streamline processes, enhance efficiency, and deliver superior customer experiences. However, digital transformation initiatives bring their own set of risks, including data privacy concerns, infrastructure vulnerabilities, and the need for skilled talent to navigate the evolving digital landscape.

Geopolitical pressures also have a profound impact on organisations' innovation strategies. Global shifts in trade policies, regional conflicts, and changing regulatory frameworks introduce complexities that require agility and responsiveness within businesses. Navigating through these geopolitical challenges while maintaining a focus on innovation demands a careful balance of risk mitigation and strategic decision-making.

Beyond these primary megatrends, other aspects further affect innovation in organisations worldwide – including shifting consumer expectations, rising environmental consciousness, and the need for sustainability-driven innovation. Organisations must be mindful of societal changes and leverage them to develop products and services that meet evolving demands, while minimising their environmental impact.

The relationship between innovation and risk is an intricate one, and this whitepaper delves into practical strategies and best practices for organisations to strike the right balance while keeping costs under control. By adopting a holistic approach that incorporates agile methodologies, strategic partnerships, cost-effective technological solutions, and proactive risk assessment, organisations can unlock their potential for sustainable growth and success.

Cost-savings are hitting tech budgets

Australian CIOs are facing shrinking budgets but increasing threats. That's unlikely to change soon, with many of the key drivers of this challenge – including the war in Ukraine and fears over global recessions – persisting. So now is the time to be looking for cost-effective solutions to ensure a company's network is as innovative and secure as possible. CIOs are on the hunt for low-cost, effective ways to simplify networks and improve cybersecurity – and that's where SASE (Secure Access Service Edge), which delivers WAN and security controls as a cloud service at the connection source, comes into the picture.

"No-one is allocating a budget for digital transformation - they are expecting it to happen organically. There's a need for these budgets to go further," says Andrew Lamrock, Verizon APAC Director, Partner Solutions.

While tech budgets may be reducing, this hasn't stopped the pressure piling on companies around cybersecurity and ESG, particularly from a governance and reporting perspective. There are also increasing cybersecurity risks, and a huge focus on what companies are doing to protect the sensitive data they hold. The high-profile cyber-attacks on trusted Australian businesses during 2022 shone a spotlight on cybersecurity and made data breaches a mainstream issue, heaping more pressure on CIOs to adapt and innovate to combat these malicious actors.

There is now an expectation that digital transformation will happen organically within an organisation and will not be a major cost item. This has created the need for smaller operational budgets to go further and for CIOs to do more with less. According to KPMG research in late 2022, well over half of Australian respondents said that less than 10 percent of their company's overall annual budget is dedicated to technology[1]. SASE can help solve this problem, providing a cost-effective solution that can ensure a company's networks are modern and fit-for-purpose in the new ESG world.

"Against a backdrop of geopolitical issues and supply chain reliability problems, there is a need for agility in addressing digital transformation," notes Verizon Senior Client Partner, Stephen Brown.

1. https://kpmg.com/au/en/home/insights/2022/11/global-technology-report-2022.html

Modernising and simplifying a company's network – the SASE way

SASE - secure access service edge - first emerged in 2019, but truly came into its own during the COVID-19 pandemic and is now a viable option for a company's networking needs. It merges software-defined WAN capabilities with network security services, allowing for the creation of a unified, cloud-enabled service model. The pandemic led to unprecedented numbers of employees working from home, and this has not slowed despite the lifting of most restrictions around the world.

Employees now need to access a company's resources and networks from anywhere on a range of devices, and this poses significant security concerns. SASE provides a solution that makes it much easier to connect resources and workers wherever they may be operating, thanks to more flexible networking and better application performance.

"With the rise of the SASE framework we can now rationalise security landscapes for organisations, and with standardisation comes better postures and the cost savings needed to make new thing possible," adds Verizon Senior Client Partner, Mathew Welles.

SASE is a way to modernise and simplify a network on a budget, and to reduce costs and improve efficiency in the long run, helping set a company up for a sustainable future. SASE adopts a simplified and secure-by-design architecture that takes out much of the redundant middleware layers. Instead of piling new security apps and systems on top of the stack – such as tokens, cloud-access secure brokerage and digital leak protection – to combat growing security risks, SASE takes these unnecessary layers out, achieving significant cost-savings.

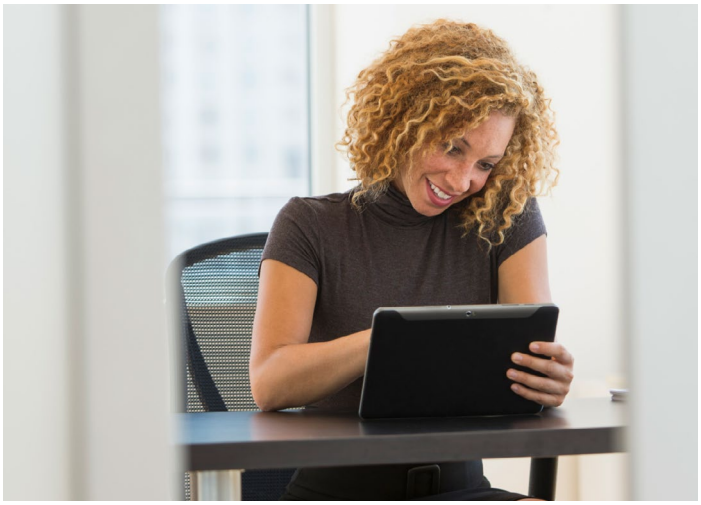
This secure architecture provides a strong foundation on which to build a network, and eliminates the need for a company to invest time and money making its tech stack more complicated, in a futile effort to make itself more secure. Budgets today just aren't big enough to be doing this anymore.

Andrew Lamrock continues, "The modernisation of networks always creates a cost-out scenario. The current depressed economic conditions and slim availability of budgets create a challenge to innovate.

"We need to unify security, IT, network, infrastructure, apps and end-user support, so when a secure network is deployed, it generates benefit across all domains. Before COVID this all worked in silos, but that's starting to change."

According to research by Forrester[2], adopting a SASE framework can offer a return on investment of up to 270 percent for a large organisation. The research also found that a company that implements a SASE network starts to see a profit within six months.

Andrew notes, of his Verizon solutions team, "Secure network is the foundation to build from. We are part of your entire ecosystem – every dollar we help an organisation save on a network, they'll spend on the cloud. So we can watch it evolve. There is a huge middleware market opening up around zero-trust access. But we can now take out the middleware and create a full desktop publishing ecosystem."



The next generation of SASE is coming

The SASE revolution is coming, and the next generation of the networking solution is already emerging. SASE represents the convergence of information technology and operation technology, with network and security united into the one solution, helping to simplify and streamline a company's network. It enables a full ecosystem to be created and for unnecessary baggage in the form of middleware to be removed, for the benefit of both cybersecurity and a company's bottom line. This new form of secure network helps to implement detect and respond principles by design, and does this in an interactive and automatic way.

SASE is now reaching maturity and is already approaching a new wave, next generation of the architecture. The SASE stack is constantly evolving without the need for VPNs or tokens, with new features added in an easy and cost-effective manner.

Now is the time to get on board with SASE. According to Gartner research, IT spending in Australia is forecast to grow 7.8% in 2024[3], with local CIOs planning to invest in SASE more than any other technology to simplify the delivery of critical network and security services via the cloud "SASE is now very mature and we're moving into advanced SASE solutions. The stack itself is constantly evolving with extra features. It's about taking out the middleware, and that leads to tens of millions of dollars in savings. It's significant," notes Andrew.

2. https://www.paloaltonetworks.com/blog/sase/what-is-the-roi-of-sase/
3. https://www.gartner.com/en/newsroom/press-releases/2023-09-12-gartner-forecasts-it-spending-in-australia-to-grow-in-2024

According to the SASE & SD-WAN report by Dell'Oro Group, the SASE market around the world reached $US6 billion in 2022[4], up more than 30 percent year-on-year.

Adapting to hybrid work

It is now commonplace for employees to work from anywhere, at any time. Once the realm of freelancers and contractors, hybrid or fully remote work is now common for most companies, regardless of size. While this has brought with it a wealth of benefits, it has also increased the cybersecurity threat for these companies, with workers using different devices from a range of locations outside of a company's network. No longer is the castle and moat-style approach to network security adequate - a company's network and cybersecurity practices must meet their employees where they are.

According to Finder's Consumer Sentiment Tracker, which is a monthly survey of about 1,000 adults, just under 30 percent of Australians worked remotely in 2022[5]. Of these, more than 25 percent worked remotely from within Australia, while 7 percent worked overseas. A further 14 percent plan to work overseas this year at some point.

This presents a new challenge for CIOs in shoring up the cybersecurity of a network and ensuring these employees can access everything they need to in a secure manner.

SASE can help organisations shore up cybersecurity to combat the immense risks associated with the rapid rise in remote work, which is clearly here to stay. SASE can enable employees to continue to work from home or remotely in a safe and secure way.

"This is the power of the SASE model," Andrew continues. "To deploy a full SASE framework, you don't need VPNs or tokens or zero-trust architecture. Country to country, hotel to hotel, public Wi-Fi or home broadband – you simply connect.

It's ubiquitous. That's the beauty of it. There's one rule for every single user, regardless of the connection type."

Critical infrastructure compliance

Australian companies which qualify as critical infrastructure operators have new compliance obligations under the Security of Critical Infrastructure (SOCI) reforms.

SOCI places a range of new obligations on companies operating critical infrastructure across 11 sectors:

- Energy
- Communications
- Data storage and processing
- Financial services and markets
- Water and sewerage
- Healthcare and medical
- Higher education and research
- Food and grocery
- Transport
- Space technology
- Defence industry

Organisations in the sectors that have been 'switched on' now have positive security obligations, which include reporting information to the Register of Critical Infrastructure Assets, mandatory cybersecurity incident notification requirements and the development of a risk management program[6]. This program must identify all risks to the critical infrastructure asset, measures to mitigate these risks and implementation of effective governance and oversight procedures relating to security. Failing to adopt, maintain or comply with one of these programs can result in a fine of more than $44,000.

It is now also often a requirement for companies to comply with the Australian Cyber Security Centre's Essential Eight cyber mitigation strategies[7], which are:

- Application control
- Patch applications
- Configure MS Office Macros
- User application hardening
- Restrict admin privileges
- Patch OS systems
- Multi-factor authentication
- Daily backups

The implementation of a SASE framework provides an easy, cost-effective way for companies to achieve

4. https://www.delloro.com/market-research/security/sase-sdwan/
5. https://www.finder.com.au/remote-working-statistics#how-many-aussie-adults-worked-remotely-in-2022
6. https://www.cisc.gov.au/compliance-and-reporting/overview
7. https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/strategies-mitigate-cyber-security-incidents/strategies-mitigate-cyber-security-incidents

compliance with the risk management program obligations around cybersecurity – while also ensuring companies give themselves the best chance of their systems remain uncompromised.

On the environmental side of ESG, SASE also enables a company to move towards technologies that use less power, helping to mitigate their impact on the environment and be more sustainable going forward.

In addition to reducing costs and shoring up cybersecurity, SASE has the power to greatly assist organisations' compliance with ever-increasing ESG responsibilities, primarily through meeting governance and environmental sustainability requirements.

"It's very powerful. You can pretty much just tick the ASD recommendations. It makes governance reportable and visible. As SASE continues to mature, it ticks governance requirements and will continue to do that when it matters," concludes Andrew.

Riding out the perfect storm with SASE

It's not an easy time to be a CIO. On the one hand, global headwinds, the war in Ukraine, recession fears and rising costs of living have created severe economic conditions and the need to cut back on costs. On the other hand, the cybersecurity threat is now a mainstream, dinner table conversation following a series of major cyber-attacks directly impacting millions of Australians. The cyber threat has never been bigger, but budgets are shrinking across the board in companies across all sectors, and tech divisions are being hit heavily.

This perfect storm has meant that CIOs are being asked to do more activity relating to cybersecurity, networks and digital transformation with less budget. The economic disruptions have had a particular impact on digital transformation, innovation and cybersecurity, and has left CIOs looking for a way to modernise and adapt their companies' networks at a very low cost, and to even find cost-savings while doing so.

The answer lies with SASE. Secure access service edge offers a cost-effective method of simplifying a company's network in a way that can create major cost-savings and assist with ESG reporting concerns.

SASE is the convergence of software-defined WAN capabilities with comprehensive network security services, including secure gateways, cloud-access security brokers, zero-trust network access and firewall-as-a-service. It allows for the creation of a unified, cloud-delivered architecture model that enables secure access for any employee wherever they are. This addresses a significant new cyber risk which has emerged in the post-COVID world, with a significant amount of the workforce now operating from outside the office. SASE allows workers to log in from different devices in different locations, to the same network.

SASE is a way to modernise your network cost-effectively, and ensure there is a system in place which can constantly adapt and evolve to meet new concerns and reporting requirements, without the added cost of manual reporting or extra investments. Reporting obligations through ESG and government regulations, such as the critical infrastructure regime, have ramped up in recent years, and having SASE in place creates immediate compliance with many of these, including the crucial Essential Eight.

SASE is set to ride a new wave of maturity soon, meaning now is the time to get on board. With tech budgets shrinking and the cyber risk ballooning, it offers an effective and efficient way to be on the cutting-edge of networking and security while not breaking the bank.

Verizon's offering

As a leader in SASE core technologies – including network, security and managed services – for more than a decade, Verizon offers the expertise needed to implement a SASE network environment with ease. Implementing an effective SASE solution requires a partner that has expertise in the space, and Verizon has more than 25 years' experience in security, more than 30 years' experience managing customer networks and 15 years as a Magic Quadrant™ Leader for Networked Services globally.

Gartner, Magic Quadrant for Network Services, Global, Danellie Young, Karen Brown, Gaspar Valdivia, 22 February 2023.