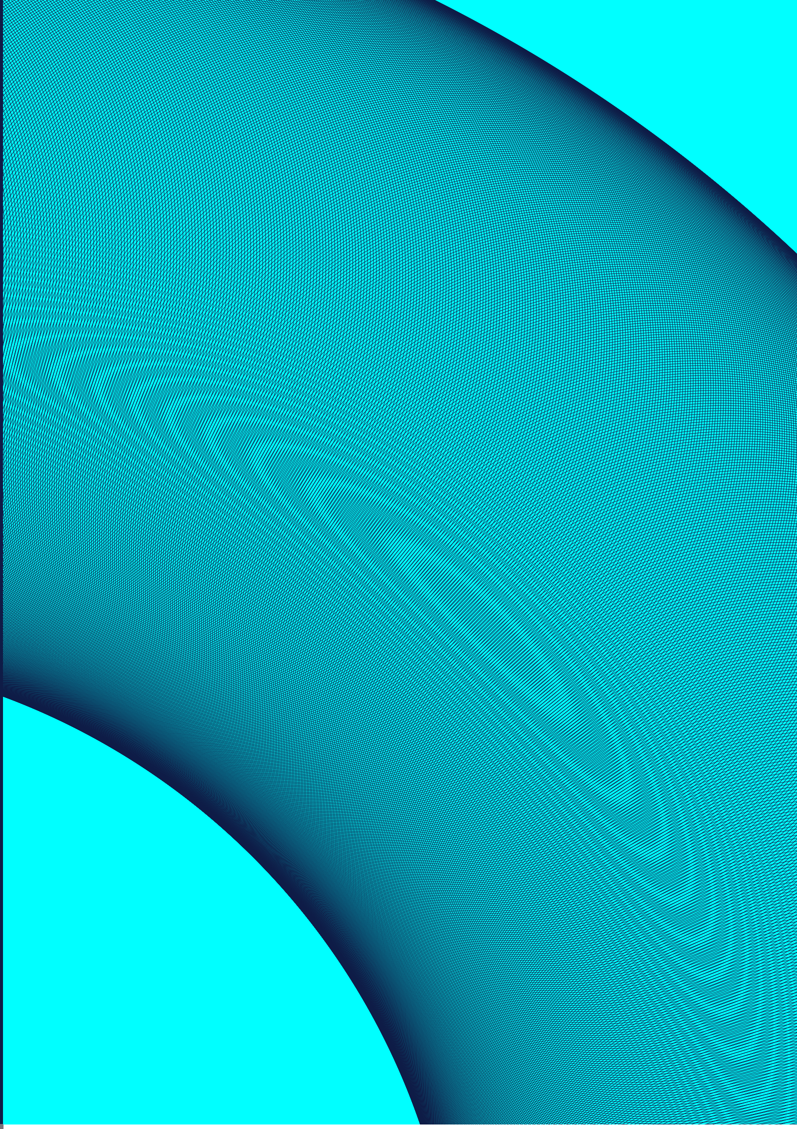
VOCUS

How to leverage your infrastructure for future-proof progress

Introduction: Organisations across public and private sectors are now realising the urgent need for digital acceleration.



However, many continue to overlook the importance of infrastructure in times of rapid transformation. Failing to lay down the right foundations before transitioning to new technology, processes and systems can create a nexus of critical issues down the track. In other words, well-intended plans are good, but infrastructure is everything.

Of course, COVID-19 has been blamed for many rapid and unprecedented changes to the status quo or 'business as usual'. But a few key areas were already beginning to see exponential change long before the coronavirus pandemic.

Some of the most notable areas are security, the world of work, and connectivity. From network security, to cloud computing, to permanent work-from-anywhere (WFA) setups, the need for low-latency, high-performance infrastructure is more pressing and pervasive than ever before.

In this e-book, we'll explore each of these in further detail, summarising the emerging trends, exciting opportunities, and ever-growing demands for businesses across these critical areas.

Chapter 1: Safeguard your business with smart, secure infrastructure

The cyber world represents perhaps the single most revolutionary advent of the 21st century, allowing us to work, play, learn, and connect in ways we couldn't have imagined years ago. However, our growing reliance on the internet and digital technology exposes us to a whole new range of security threats and challenges. As leading Australian national security expert David Irvine put it, 'the wars of the 21st century will be fought and won in cyberspace.'

Indeed, being caught 'off-guard' in today's world comes with more consequences than ever before. As cyber threats continue to become more sophisticated and pervasive, organisations must prioritise the security of their networks, processes, data, and teams, around the clock.

Network security now non-negotiable

Though we may not see it, behind the scenes of everything we do online every day is a vast, powerful, always-on network. As such, protecting your business's most important work, processes, and customer and employee data means protecting your network first and foremost—and ensuring that it is fit for purpose.

In Australia alone, about 74 per cent of companies surveyed said they've suffered a successful cyber attack. Globally, the cost of cyber crime is predicted to reach $10.5 trillion by 2025. The Australian Government regularly publicises major breaches and has made some great headway with the rollout of the national Cyber Security Strategy, but there is still much to be done by both the public and private sectors to address persisting vulnerabilities.

Building a future-proof network allows you to ensure security in a way that is holistic. Leading telecommunications providers will include security either as an embedded component or as a 'bolt-on' to existing networks. This ensures the networks and operational infrastructure that house all of your organisation's mission-critical data, files, workflows, and functions are kept safe.

Connecting and protecting your environment at head office, branch offices and across your remote workforce is more important than ever. As businesses implement and manage multi-cloud platforms, they will need to maximise connectivity between both core and edge elements of their operating environment. This includes support for overlaid services such as IP transit, IP WAN, SIP, SD-WAN, IP telephony, and cloud connect for dedicated data centre connections.

With constant phishing, DDoS, and malware attacks on the rise, your employees will inevitably be exposed to new risks every day. Because of this, it is equally important to reinforce security hygiene at the employee level. Measures such as multi-factor authentication for passwords, secure VPNs, and phishing filters on emails should be carefully understood, implemented, and followed by your teams.

Preparing for the worst

Crisis management is just as important for your systems as it is for your workforce. Prevention is always better than damage control, and when it comes to cyber security, that means a range of sophisticated measures to mitigate the risk of all kinds of cyber threats, including malware, distributed denial-of-service (DDoS) attacks, and phishing scams.

Advancements in quantum computing also pose new ways for hackers to decrypt valuable information. One highly practical measure against this is categorisation.

Categorising each of your existing assets by sensitivity ensures you account for everything across all of your mission-critical data and workloads, and enables you to implement the right level of encryption according to each asset's vulnerability.

Moreover, cyber resilience has become crucial for any business. This is where infrastructure again plays a vital role in any organisation's security efforts. One such example is having a business continuity plan, or disaster recovery plan (DRP). A DRP provides instructions to follow when responding to various disasters, including both cyber and environmental incidents. No business wants to imagine their operational infrastructure and sensitive data being compromised, but preparing for the worst is an essential part of cyber resilience.

To protect your business from ransomware or similar attacks from cyber criminals, your company's DRP should have a clear owner, involve many partners from across the business, be simple to execute, and be continually tested and updated. Your data backup solution should also run automatically in the background and enable easy recovery through a specified point-in-time restore.

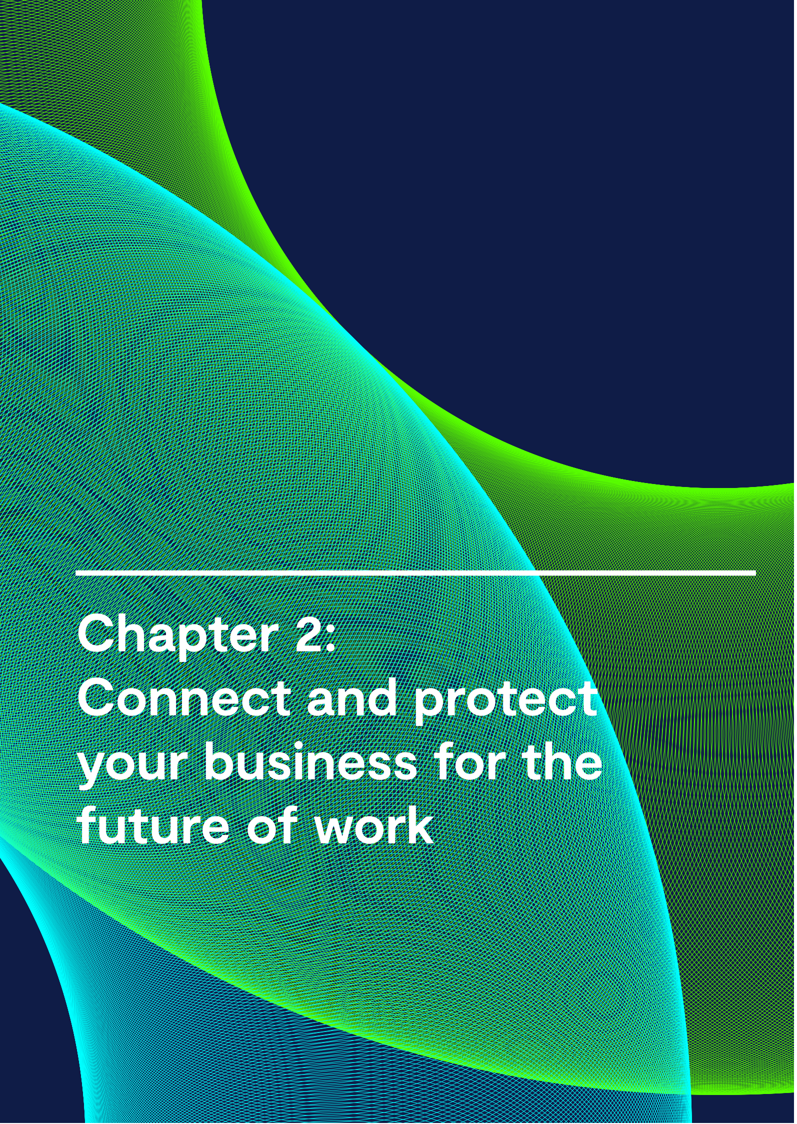
Additionally, key preventative strategies now need to be in place at the top of every organisation. According to a Deloitte study on cyber risk, less than 50 per cent of US executives said they have mature cybersecurity programs in place to address risks posed by emerging technologies, such as 'store of the future', digital identity, connected products, artificial intelligence (AI), and wearables.

For David Irvine, board members should also be better prepared for future cyber threats by understanding the risks and consequences of cyber security, making security hygiene common practice within the organisation, and seeking appropriate security expertise and support on the board or outside your organisation.

Building customer trust

As more Australian consumers and citizens become aware of the prevalence of data leaks and breaches, they look to businesses and government agencies to ensure their data is obtained transparently, sufficiently protected, and stored securely. In the words of Harvard Business Review writer Andrew Burt, "If you're selling a product, you're now selling trust." With this added responsibility comes an opportunity to lead by example for your customers through robust, risk-proof infrastructure, strategic customer-facing communications, and by delivering an experience that demonstrates you put their data security first.

In today's world, prioritising security should be a no-brainer. That being said, the ever-increasing sophistication and prevalence of threats and risks makes it harder than ever to keep up. In order to stay one or more steps ahead, adequate infrastructure is essential. Solid network security and architectures allow you to better monitor your systems, data, applications, and people, as well as be prepared for whatever tomorrow may bring.



Chapter 2: Connect and protect your business for the future of work

It’s safe to say that the world of work has undergone an extremely fast, drastic, and irrevocable transformation in the past year. Gone are the days of physically, geographically, and technologically confined workplaces—and workforces.

This abrupt and complete overhaul has been challenging for businesses and employees alike, as everything from operations, work stations, data management, leadership strategies, internal communications, to employee wellbeing and more, have succumbed to what is now deemed the ‘new normal’.

Say hello to hybrid

It’s important to note that emerging technologies have been influencing and revolutionising our ways of working for a long time now. But the COVID-19 pandemic has served as the final nail in the coffin for ‘business as usual’.

Whether it’s flexible work, work from anywhere (WFA), or remote work, the undeniable truth is that the new world of work is hybrid. As regions around the world enter and exit periods of temporary lockdown, many employees grapple with an ever-changing work setup split between home and the office. Remote-first companies, on the other hand, have their employees work from home permanently, rendering the need for a physical office space completely obsolete.

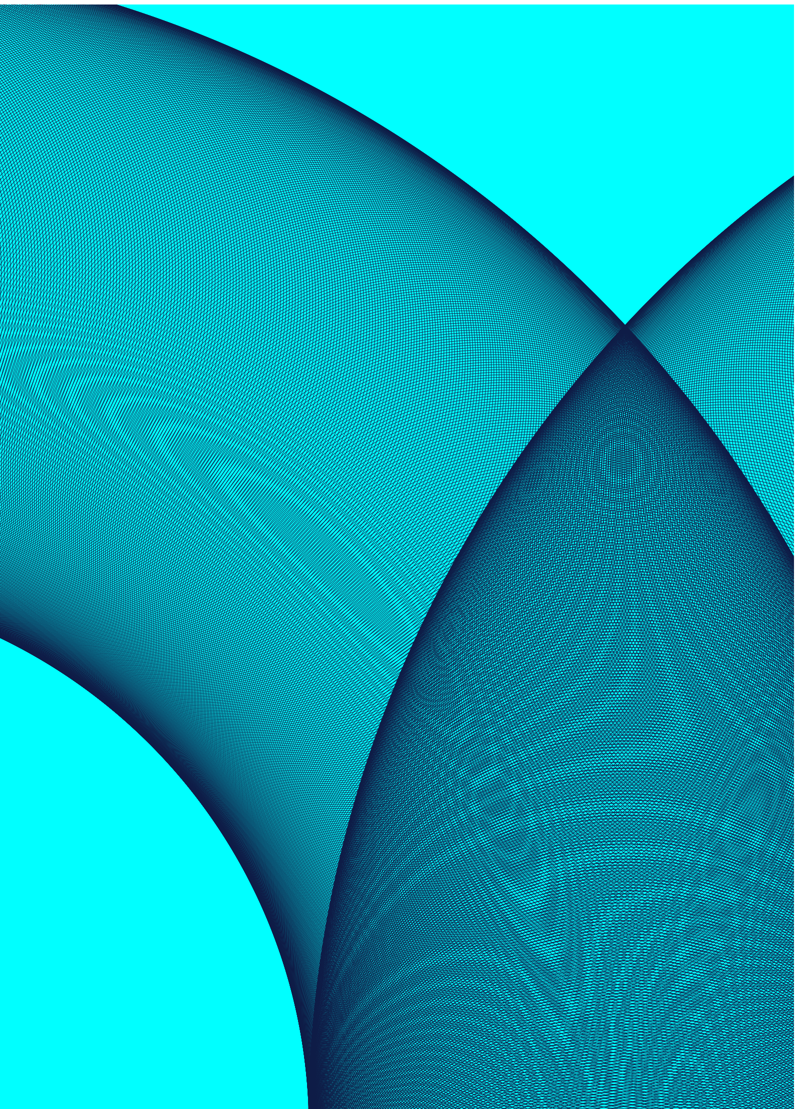
Renowned futurist Dr Bruce McCabe sees the way forward as a delicate balance. People are ultimately social creatures, and temporarily removing the four walls of the office cannot change that. Whether bustling city centres will rise once again is yet to be seen, but flexible work, and the need for team interaction and collaboration, remains a sure thing for the foreseeable future.

More and more workers are also seeing flexible working arrangements as a priority, not a privilege. According to a 2020 study by Growmotely, 97 per cent of workers do not want to return to the office full-time post-pandemic. Similarly, a 2021 Gallup report found that 55 per cent of workers would look for work elsewhere if the remote work option was taken from them. Engagement levels were also found to be higher among remote workers, at 32 per cent, compared to only 28 per cent among office workers. For businesses, supporting and responding to the demands of their teams will be non-negotiable in order to maintain positive levels of employee productivity, engagement, and retention.

However, the impacts of remote work are not limited to work culture and morale. Having your employees work from anywhere also comes with critical security implications. Prioritising cyber security is a must, as you streamline and secure information across your head office, branch offices, and remote workforce.

More businesses across the country are working to implement and manage cloud platforms for their data and processes. Australian government agencies are also doing the same, with the added obligations of maintaining data sovereignty and residency through in-country data centres.

As you transition to modern systems, it becomes clear that adapting to the demands of hybrid work means understanding that security and connectivity go hand in hand. For example, a vast number of public and private sector organisations now look to network solution providers for support with their network infrastructure, such as IP transit, IP WAN, SIP, SD-WAN, IP telephony and cloud on-ramps for dedicated data centre connections. Ultimately, ensuring high levels of user security, data protection, and availability will become critical to businesses well into the future.



Digitisation: the big disruptor

Digital disruption is certainly a hot topic of the moment, but the true ramifications of this technology-led phenomenon have yet to take full effect in the world of work. Some of the biggest consequences will include increased demand for digital skills, which will affect organisations' talent planning efforts and workers' employability.

No industry is immune to the impacts of digitisation, and the need to upskill will be felt across every economy. According to the Swinburne Research Report, the most in-demand digital skills around the world will cover:

- software programming and engineering
- data analytics
- visualisation
- IoT (Internet of Things)
- IT architecture
- security

Upskilling the global workforce to bridge the digital divide has become more challenging amidst the COVID-19 pandemic. Organisations are noticing a widespread skills shortage in IT and cybersecurity, due in large part to migration and travel restrictions that are limiting available talent pools.

Businesses who haven't done so already will need to ramp up their hiring for these advanced digital skills, and where possible, offer internal learning and development (L&D) programs to allow existing employees to upskill in these areas. Until now, many organisations have instead turned to outsourcing to meet their company's digital needs. In the future, relying too heavily on offshore workers may slow them down when compared to competitors who have made these capabilities a priority in-house.

Similarly, delivering a positive employee experience is a key differentiator for businesses in the battle for top talent. Investing in technologies that support smarter ways of working, such as agile collaboration and internal communication tools, helps keep employees feeling engaged, productive, and supported in their roles and teams. With the inevitable physical divide that comes with remote working, these digital platforms and channels, together with incentives such as regular employee recognition and rewards, are a must in order to support both employee wellbeing and employee experience as a whole.

Operating further and faster

Artificial intelligence (AI) has come leaps and bounds in the past few years. New generations of more capable autonomous systems have emerged, from autonomous vehicles to automated check-out registers in supermarkets. Driven by improved mechanics, sensors, and software, AI and machine learning are predicted to account for trillions of dollars through improved labour productivity. Currently, the finance, automotive, and telecommunications sectors lead AI adoption.

Meanwhile, for businesses, about half of the activities carried out by workers could be automated. In fact, automation software and robotics are already replacing various human tasks, including data entry, reporting, CRM, payments and invoicing, marketing, shipping and inventory management, customer support, hiring processes, and much more. This means that most workers—from builders, to bankers, to CEOs—will work alongside rapidly evolving machines. The nature of these occupations will likely change as a result.

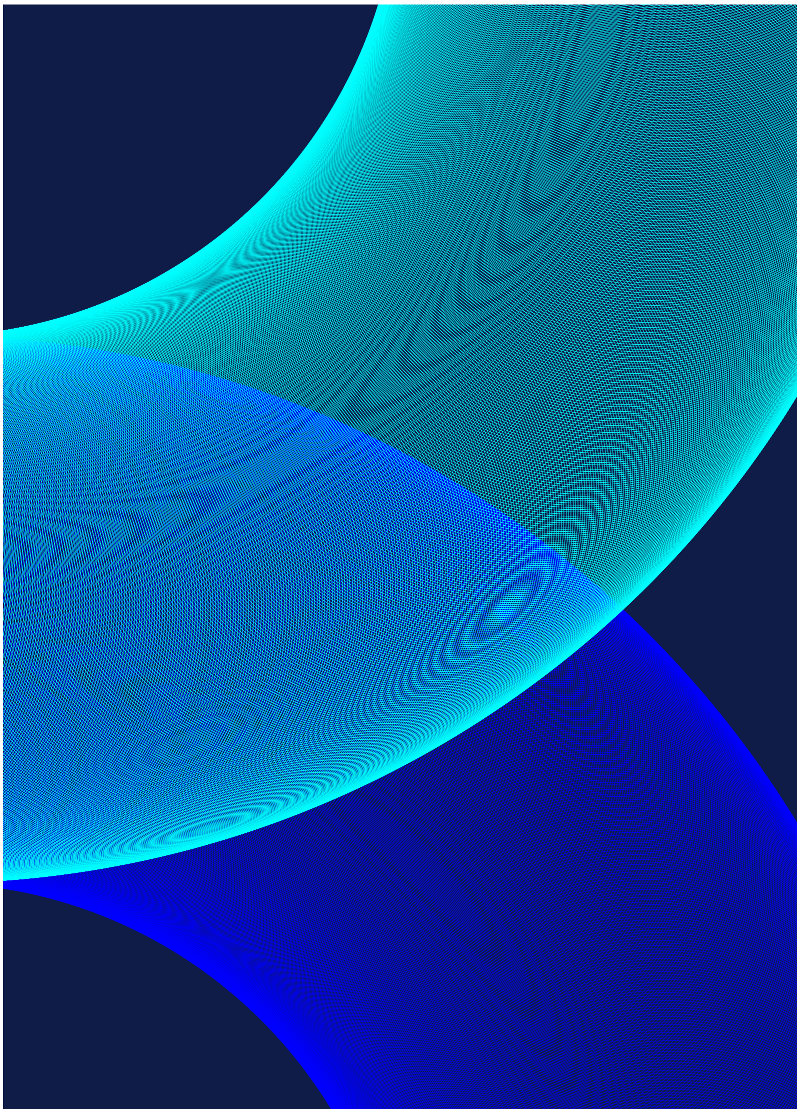
Elevating the experience

Digitisation also presents a unique opportunity to reinvent your customer experience (CX). The e-commerce industry, for example, has seen remarkable growth in the last few years, even amidst the economic challenges of the pandemic. Australian retail ecommerce revenue is forecast to grow by a compound annual rate of 4.22%, reaching $45.7 billion by 2025. This is in large part due to the enhanced shopping experiences that online retailers can offer customers, using technologies such as live 24x7 support chatbots, augmented reality (AR), voice search, personalisation, AI-powered predictive marketing, and API-driven features.

E-commerce businesses have been particularly fast on the uptake of these technologies, but government agencies and businesses across all industries can, and must look to deploy similar optimisation strategies.

This may include optimising all consumer-facing platforms for mobile devices for improved user experience (UX), mobilising teams to boost productivity via speed to market and faster customer response times, or leveraging automation and DevOps tools to debug and streamline your processes. As customers continue to expect more from brands, investing in innovation and CX to design truly customer-centric solutions will give your business a significant advantage over competitors.

The COVID-19 pandemic may well be the biggest disruptor that most of us will see in our working lives. The good news is that disruption is a catalyst for innovation. Out of such drastic change comes a willingness to try new things, and to re-examine the way things have always been done. For businesses and governments, right now is an excellent time to try new ideas, and embrace new technologies for the benefit of your employees, citizens, and customers.



Chapter 3: Unlock connectivity and imagination with future-proof infrastructure

Racing to take advantage of rapidly emerging and evolving technologies can seem like an overwhelming task for governments and organisations.

But this very shift has created a myriad of opportunities that were previously unimaginable. Unlocking imagination through smarter connectivity means opening your organisation to a new frontier of technological advancement, globalisation, and exponential change.

Next, we'll explore some of the drivers at play, as well as the outcomes of emerging technologies, and how to leverage them to gain a competitive advantage for your business.

The case for cloud

The combination of COVID-era disruption, a newfound urgency around digital transformation, and a need to extract more value from every ICT dollar spent has created a perfect storm for businesses, particularly as they turn to cloud solutions to drive their transformation efforts.

Cloud promises a range of benefits, from improved business resilience and disaster recovery, to increased agility, better surge management, lower costs, and more capability to support business applications.

Implementing cloud properly, however, is no easy feat. It requires careful planning, ongoing consideration, and highly sophisticated hybrid cloud architectures. Organisations who fail to build strategies focused on business outcomes may find that new technologies cause more problems than they fix.

A study by global software provider IFS in 2020 found that, despite widespread economic pressures, 58 per cent of Australian businesses planned to increase their spending on digital transformation initiatives to help them get through the pandemic.

This was ahead of the world average of 52 per cent, suggesting that Australian businesses remain more optimistic about cloud's promise than those in many other countries.

"The proactive use of technology may determine who emerges with a competitive advantage and positions themselves as a market leader in the post-pandemic era," the firm noted.

Increased spending on transformation will happen regardless of widespread revenue hits that force decision-makers to trim budgets and reallocate increasingly scarce resources, according to findings from a 2020 GlobalData report.

Enabled by flexible software and scalable hardware, a multi-cloud solution boosts organisational agility. But to work most effectively, it must be supported by purpose-built network infrastructure that closely supports the vision for cloud in the organisation.

Connecting to multi-cloud

Low-latency connectivity is truly the key to successful cloud application and management. Cloud strategies are about much more than simply transferring existing infrastructure to a service provider. In the multi-cloud world, business services must flow smoothly between different solutions that are physically housed hundreds or thousands of kilometres apart.

Loading a webpage, for example, may involve API calls to a broad range of cloud services—so if even one of these is slowed down, the whole user experience may be affected.

This is particularly problematic given users' increased reliance on devices that may be located anywhere, and connected using networks with a broad spectrum of performance and features.

While the agile design of a cloud solution can be a lifesaver in uncertain times, it can also introduce new challenges if it's not managed carefully. In particular, public cloud has introduced new security dynamics, such as shared security models. These dynamics inevitably require new thinking for organisations in order to avoid a significant drop in their security posture. A 2020 survey by Sophos found that 74 per cent of companies using cloud had been hit by a public cloud security incident, with stolen credentials exploited in 29 per cent of cases.

Just 72 per cent of Australian businesses were even aware of all their cloud infrastructure—well behind the 85 per cent in the United States—and 69 per cent of attacks exploited misconfiguration in cloud environments, compared with 59 per cent in the United Kingdom.

To attain reliability, businesses need to design their multi-cloud environments with the same or better level of resilience and disaster recovery as they had in their legacy environment.

Organisations will need to start by addressing latency issues and implementing strategic thinking to ensure smart, seamless end-to-end experiences. When moving towards cloud adoption, for example, you will need to understand how your new services will be consumed, by whom, and how they will scale. Future networks will be populated with internet of things (IoT) equipment that is often wirelessly connected and has its own performance characteristics, which is a critical consideration when designing for the future. As such, network infrastructure will need to be adequately built for purpose to process the ever-increasing amounts of data either inside or outside of the cloud.

Aided by artificial intelligence (AI) algorithms that will decentralise data analysis and management of enterprise systems, multi-cloud environments must be able to apply the same levels of rigour and agility to data and applications no matter where they are located.

The multi-cloud will, in effect, be the steam engine of the digital-transformation revolution. Customers' transformed business environments will be linked by 'tracks' connecting a range of public and private-cloud service providers around the country and the world.

Agility must be a core feature of your migration to a multi-cloud environment. It enables you to adapt and adjust as you move through the discrete stages of your migration, such as rationalising and migrating data into the cloud, building the new application environment, and addressing security issues by establishing clear procedures and auditing standards.

Your choice of infrastructure for the transformation will be crucial to ensuring your multi-cloud environment ultimately meets your business requirements. And while there are extensive data centres available for hosting your private cloud or Infrastructure-as-a-Service (Iaas) solution, it's important to consider the range of characteristics that each offers, as well as your goals in adopting them.

The effectiveness of your multi-cloud environment will also depend on the type and configuration of connectivity services between your business and the data centre (or centres) the new architecture is built upon.

Connecting and protecting your environment at head office, branch offices and across your remote workforce is more important than ever. As businesses implement and manage multi-cloud platforms, they will need to maximise connectivity between both core and edge elements of their operating environment. This includes support for overlaid services such as IP transit, IP WAN, SIP, SD-WAN, IP telephony, and cloud connect for dedicated data centre connections.

Beyond the clouds

Far-reaching connectivity is becoming more accessible, reliable and affordable, making the world feel a whole lot smaller. Significant advancements in space technology have made low-latency connectivity possible within and between urban, regional, and even remote environments.

Satellite technology, for example, makes use of a range of orbits for telecommunications, satellite imaging, aviation, and navigation purposes. These include geostationary orbit (GEO), low earth orbit (LEO), medium earth orbit (MEO), polar orbit, sun-synchronous orbit (SSO), transfer orbit and geostationary transfer orbit (GTO), and Lagrange points (L-points). Of particular interest among these are LEO satellites, which are currently helping to bridge connectivity gaps right across the country, enabling Australians to work, play, and connect further and faster.

On top of this, satellite services are playing a critical role in helping organisations increase their uptake and utilisation of cloud services. A combination of edge-based computing, connected via low-latency satellite services back to cloud infrastructure, is allowing businesses and government agencies to rethink their strategies for remote locations. Satellites are effectively connecting all corners of the country, allowing for equalisation of thinking between both cities and regional or rural communities.

From under the sea and right into space, connectivity is what will take your business further and faster. From incorporating IoT in cities to improve the lives of citizens, to worldwide internet coverage via satellite, the way we work and live ultimately relies on robust networks and telecommunications. It's impossible to have one without the other, so there is no better time than the present to invest in your infrastructure with an industry-leading partner by your side.

Conclusion

While unforeseen circumstances and events like COVID-19 may be out of your control, there are certain critical strategies and actions that you can adopt to help future-proof your business as much as possible.

There's a saying amongst builders: "The house won't fall if the bones are good". And when it comes to your business, driving growth and innovation is possible even amidst widespread disruption, as long as you have the right foundations in place.

Your IT solutions and network infrastructure provide the core framework for smarter, safer operations, offering protection from security threats, streamlined access to mission-critical data, and better experiences for your employees and customers. Making proactive moves and smarter decisions about your networks and infrastructure helps pave the way for your business's success well into the future.

References

https://www.vocus.com.au/news/vocus-inspire-technologies-to-change-the-world-with-dr-bruce-mccabe

https://www.vocus.com.au/news/six-insights-on-cyber-network-security

https://www.vocus.com.au/news/new-risks-and-emerging-threats-in-cyber-security

https://www.cybersecurityconnect.com.au/industry/7039-vocus-and-aws-team-up-for-future-state-program

https://cybersecuritystrategy.homeaffairs.gov.au/

https://hbr.org/2019/03/cybersecurity-is-putting-customer-trust-at-the-center-of-competition

https://deloitte.wsj.com/articles/cybersecurity-building-consumer-trust-1500436943

https://www2.deloitte.com/us/en/insights/industry/retail-distribution/cyber-risk-management-in-consumer-business.html

https://www.wired.com/story/yandex-ddos-fortinet-passwords-security-news/

https://employmenthero.com/blog/remote-working-statistics/

https://www.forbes.com/sites/ashiraprossack1/2021/02/10/5-statistics-employers-need-to-know-about-the-remote-workforce/?sh=5ddb1c79655d

https://www.bigcommerce.com.au/articles/ecommerce/ecommerce-trends/#14-ecommerce-trends-leading-the-way

https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digitizing-customer-journeys-and-processes

https://www.insiderintelligence.com/insights/ecommerce-industry-statistics/

https://www.mckinsey.com/featured-insights/future-of-work/ai-automation-and-the-future-of-work-ten-things-to-solve-for

https://www.pwc.com/gx/en/issues/upskilling.html

https://blog.commissionfactory.com/ecommerce-marketing/analysis-of-australian-ecommerce-statistics

https://www.ncver.edu.au/__data/assets/pdf_file/0035/2948129/Webinar_SkillingForDigitalDisruptionAndTheFutureOfWork_PresentationSlides.pdf

https://www.wired.com/story/ai-coming-most-mind-numbing-office-tasks/

https://itbrief.com.au/story/migration-regret-australias-cloud-industry-has-communication-problem

https://www.ifs.com/au/news-and-events/newsroom/2020/06/30/70-percent-of-businesses-increase-or-maintain-digital-transformation-spend-amid-pandemic-ifs-study-s/

https://www.globaldata.com/enterprise-ict-budget-in-australia-to-decline-in-2020-due-to-covid-19-says-globaldata/

https://secure2.sophos.com/en-us/content/state-of-cloud-security.aspx

https://www.dta.gov.au/our-projects/secure-cloud-strategy

https://www.gartner.com/en/newsroom/press-releases/2018-12-03-gartner-says-the-future-of-it-infrastructure-is-always-on-always-available-everywhere

https://www.itnews.com.au/news/vocus-backs-leo-satellites-to-bridge-regional-broadband-divide-555219

https://www.nokia.com/about-us/news/releases/2021/08/16/nokia-and-vocus-launch-200g-optical-network-in-australia/

VOCUS

vocus.com.au