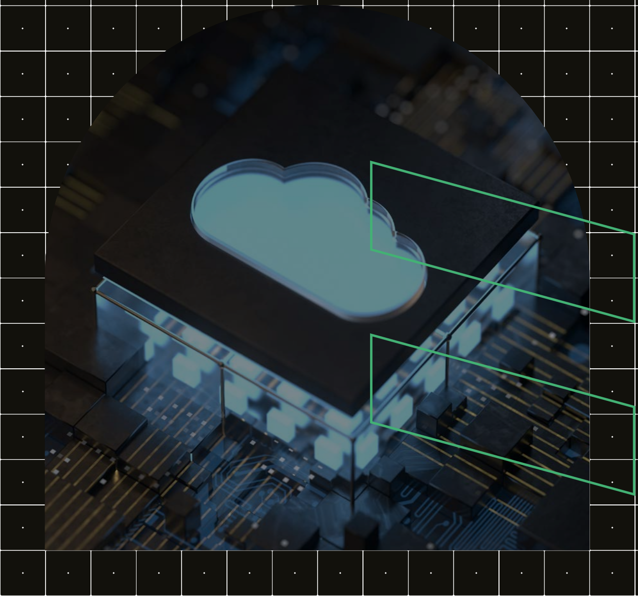
Whitepaper



# Secure Cloud Automation – Three Things Business Executives Need to Know

A TRA Perspective sponsored by Nexon

If you were asked to identify three core terms that describe a modern and agile IT infrastructure platform that could drive your organisation's success, it's likely 'cloud computing', 'secure', and 'automation' would feature. Yes, there are others, however in Tech Research Asia's (TRA) view these three are critical for success. Indeed, without them it is ultimately harder to be innovative and deliver great employee and customer experiences with the applications and data you use.

In this report we outline the "so what?" of cloud automation, security, and DevSecOps for IT and business leaders. We explain what each are, identify key considerations, and comment on the possible benefits. Finally, we offer a list of essential factors for your organisation to consider as it invests and upgrades its IT infrastructure platform.

Australian businesses continue to show robust demand for moving infrastructure and applications to 'the cloud'. By now a generic term, cloud brings benefits including agility, rapid deployment and a different cost-economic model that means businesses can respond more effectively to challenging business conditions. TRA data suggests that under 10% of businesses in Australia will use a single cloud environment to support their operations with a hybrid cloud model (a mixture of cloud, on-premises, etc) is the preferred approach. In this multi-infrastructure world with complex workloads, many companies are now looking to cloud automation to address infrastructure, data and application sprawl.

From a business perspective, cloud automation offers a number of potential benefits. Foremost of which is the potential for lower overall cost of ownership of cloud services. Automation removes a significant amount of expensive employees that oversee the management, troubleshooting and securing of cloud services, freeing them to work on higher value activities. In a similar manner, automation brings quicker completion of cloud tasks (through Infrastructure as Code, 'IaC') and an overall time saving of management and cloud services deployments.

The following delves more deeply into 'why cloud automation', issues to consider and the benefits.

TRA data suggests that under **10% of businesses** in Australia will use a single cloud environment to support their operations with a hybrid cloud model (a mixture of cloud, on-premises, etc) is the preferred approach.

## Why Cloud Automation?

1 **Public cloud leads and workload sprawl follows:** Cloud computing has established itself as part and parcel of most Australian organisations' IT strategies. Public cloud adoption has been impressive and is a great environment for many use cases and applications:  9 in 10 organisations are using some form of public cloud service (with IaaS and SaaS leading the way). However it's not a single, public cloud environment. Rather, organisations have different applications running in different public clouds increasing the amount of application sprawl they must manage.

2 **Application repatriation:** The focus in recent years for many CIOs has switched to a more considered approach for applications. Changing business priorities, cost focus, management priorities and security needs have seen organisations consider what and where is best for their applications' infrastructure. In a recent 2020 study TRA conducted in Australia and New Zealand we discovered more than 44% of organisations had either moved applications back from public cloud to private cloud (or on premises environments) or were considering such a move.

3 **Hybrid is default:** A few years ago, "cloud-first" was the focus, today TRA cloud consumption data shows that just over 80% of Australian IT leaders say a Hybrid IT model is their target. In short it involves a mix of public cloud, private cloud, colocation and services. Add in the fact many organisations maintaining their own applications are moving to a microservices and DevOps approach, and it is clear we have a heterogenous environment. One that, when you factor in the growth in applications, data, and pressures on IT from digital business, demands some form of automation to manage it effectively and scale as required.

4 **Application management complexity:** This, to put it simply, is what cloud automation aims to address by using software and tools to automate the management of a hybrid IT environment. It differs somewhat from cloud orchestration (which is the scheduling and integration of automated tasks across systems), but many automation solutions offer a level of orchestration as well.

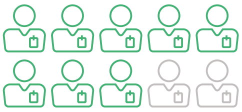
## 3 Things Businesses Must Consider for Cloud Automation

- A hybrid cloud environment means that the native tools in each cloud platform used for discovery and visibility integration don't necessarily combine well to provide a single pane of glass view. Consequently the integration between core systems or systems of record, the systems of operation, and systems of innovation is important and requires strong automation.
- As with on-premises infrastructure automation, cloud automation is not a "set and forget" strategy - you do need to continue to iterate and improve. Lifecycle management and continuous optimisation should be front and centre in your approach, so too should automated decommissioning.
- Extend your thinking to the cloud business model not just the technology infrastructure. The business case for cloud automation should sell itself, however management of the cloud environment is an exceptionally complex area and one in which automation, although difficult, can provide strong insights into cloud costs. Auto-scaling (see 'benefits' following) also allows greater cost control as it adds resources only when needed.

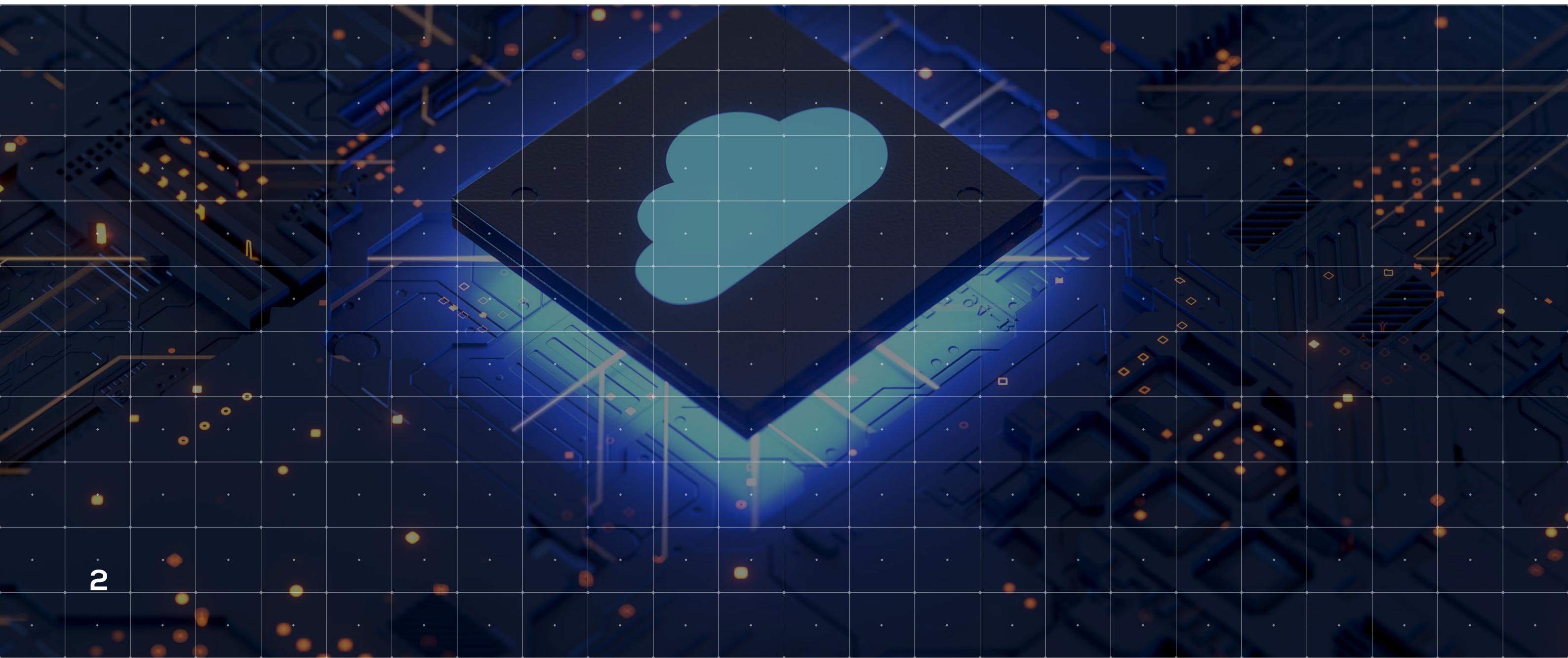
## 3 Key Benefits of Cloud Automation

- Reduction in time taken by employees to manage the environment creates the benefit of reallocating the employees to use on value creation. Automation tools also provide improved oversight to support a stronger governance capability.
- Greater backup and disaster recovery resiliency. Through automation, companies should achieve a state of frequent backups, either through direct cloud backup or automation of on-premises backup to the cloud.
- Certainly current business conditions have been somewhat more volatile and cloud automation helps address the fluctuation in operations through 'bursting' via auto-scaling (ie. you can scale your cloud environment up or down in line with requirements without having to manually add or remove your own physical infrastructure).

**9 in 10 organisations** are using some form of public cloud service (with IaaS and SaaS leading the way).



**80% of Australian IT leaders say** a Hybrid IT model is their (cloud) target.



# Cloud and security: are you secure?

For many reasons — including management of the cloud infrastructure, configuration of environments, varying access conditions — the traditional 'moat and perimeter' approach to cybersecurity is no longer effective in a cloud world.

In January 2021, TRA surveyed 300 Australian businesses about their security strategy and issues and the data revealed that:

1. While cybersecurity in its current form is a known factor (businesses are very familiar with the threats and solutions available), there is a continuous 'playing catchup' element as new threats and actors emerge, increasingly supported by payloads that are strengthened by machine learning (ML) and artificial intelligence (AI) .
2. Over 50% of security incidents are caused by people that work within your organisation - either malicious actions or by mistakes and misconfigurations - which is becoming an increasing challenge. Where your platform is located doesn't change this risk profile. The reality is public cloud security needs the same focus as security in any other environment
3. 52% of Australian organisations say they fell victim to a successful cyber security attack in the last 12 months. 69% of those breached described the data breach as either 'serious' or 'very serious' in its impact on their business operations.
4. Cybersecurity budgets remained largely unchanged as a percentage of revenue between 2019 and 2021, however there was a marked push to exert more centralised control and oversight with 64% of companies consolidating cybersecurity budgets within their IT groups, an increase of 14% over 2019.
5. Skills, budget, and organisational apathy are the top challenges. Most also say they cannot keep up with the pace of security developments. Nor can they ensure the rest of the organisation is adequately educated - over 70% of Australian companies surveyed by TRA stated that either 'totally agree' or 'mostly agree' with the following statement: "We struggle to provide adequate education to our leaders and employees regarding security."
6. Adopting hybrid IT (including cloud computing) and contemporary approaches to app development changes how you go about security. The traditional security perimeter no longer exists and the increased complexity of a hybrid environment means that, of those surveyed in Australia, using a managed services provider (MSP) is now the most preferred option to provide security solutions.

**50% +**
**of security incidents** are caused by people that work within your organisation

**52%**
**of Australian organisations** say they fell victim to a successful cyber security attack in the last 12 months.

**51%**
**of companies surveyed** stated backup data archives and 10% of secondary replicated copies were also attacked alongside production data.

## 4 Things businesses must consider for cybersecurity

1. **Cybersecurity is a company-wide consideration, not just for IT.** As more line of business operations move applications to the cloud (potentially outside the remit of IT), companies need to consider how to combine group-wide cybersecurity awareness training, process audits and technology.
2. **For developers, code security by design should be a core part of every coding effort and not a bolt on after the fact.** This is especially important if you are undertaking your own development and releasing updates frequently. Security will make or break not just a product or service success, but also the reputational damage of individual leaders and potentially organisations overall.
3. **For Deployment (IaC)** - Introduce infrastructure as code which uses machine-readable definition files to manage data centre resources instead of physical hardware configuration or interactive configuration tools. This allows it to be automated to a much higher degree and as such, should help with reducing human error.
4. **Protection: Continuous Monitoring & Response:** – Mitigating threats as much as possible, but also preparing for the time that an attack is successful. TRA data suggests that it is not just production data that is targeted in cyberattacks: 51% of companies surveyed stated backup data archives and 10% of secondary replicated copies were also attacked alongside production data. Ensuring employees (and tech partners) have well tested data recovery plans in place is critical. More broadly, the most common internal cybersecurity skills in short supply are application security, cloud and analysts. If your company doesn't have them, make sure your core suppliers do!

# What is DevSecOps and why is it important for my business?

As cloud adoption has increased, so too has the shortening of application development cycles. In the past, waterfall development models saw security 'coming in' towards the end of the process as cybersecurity professionals reviewed the application and identified potential vulnerabilities.

As we outlined earlier, in a cloud world of increased agility and speed to market, cybersecurity now needs to be a company-wide focus, and from a software development perspective, application and infrastructure security needs to be considered right from the very start of any development activity. For many companies this has seen the adoption of a 'DevSecOps' development philosophy.

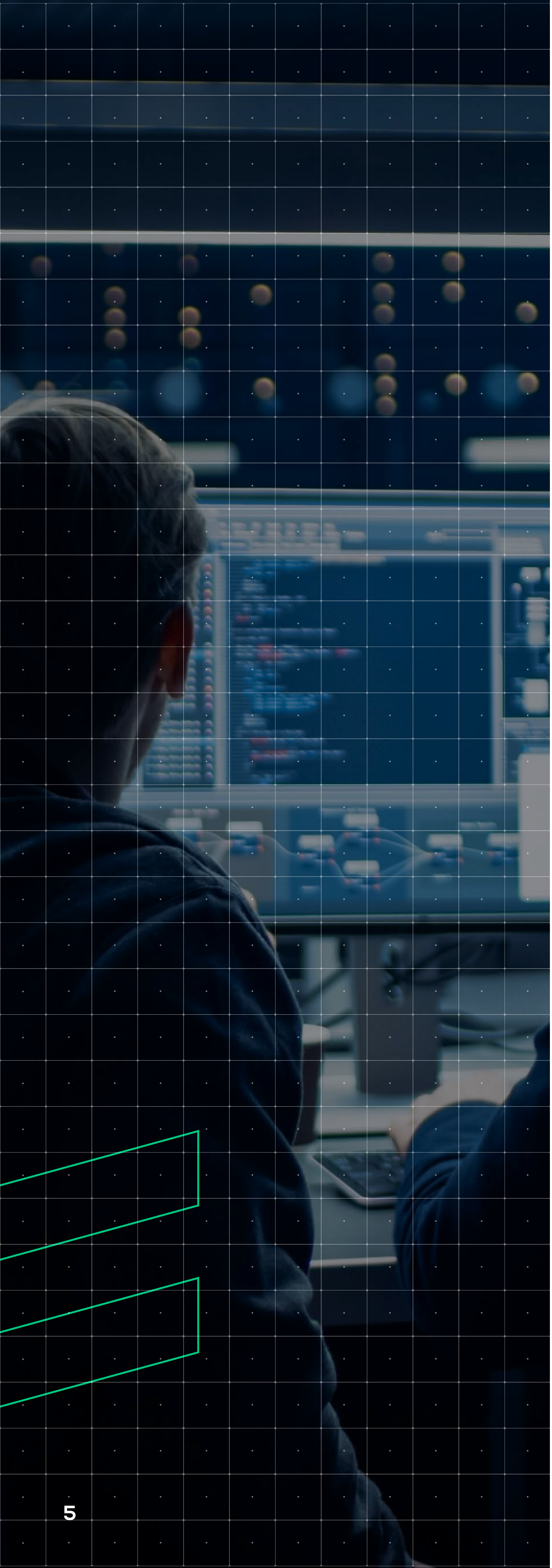
DevSecOps is a relatively recent addition to the IT landscape and represents 'development security operations'. Essentially it takes the philosophy of DevOps, (focused on accelerating software development speed), and incorporates security within each part of the software development cycle, without any detrimental impact on software release times.

In other words, a DevSecOps approach means your business can move more quickly, more securely, with resulting benefits including reduced threat of reputation damage, loss of customer or other sensitive data, improved effectiveness in rebuffing ever-constant ransomware and other malware attacks and improved governance and compliance postures.

It is particularly useful for organisations that are moving towards continuous delivery and integration with their applications as it creates solid frameworks, involving highly consistent processes with uniform tooling and automated controls. **The Cloud Security Alliance (CSA)** defines six pillars for the movement:

1. **Collective Responsibilit**y, ie. cyber-security is the responsibility of everyone within the organisation, not just the IT and security groups.
2. **Collaboration and Integration.** Confrontation on cyber-security weaknesses in an organisation is counter-productive and organisations need to ensure that they strive to create a culture of supportive collaboration.
3. **Pragmatic Implementation.** Organisations differ in their software lifecycles and there is no one-size fits-all set of tools for implementing DevSecOps. Choose what best works for you.
4. **Bridging Compliance and Development.** Compliance requirements are not always easy to reflect in secure, product development activity. Companies must identify applicable compliance requirements and translate them into appropriate software measures and within the software lifecycle to be automated and measured to improve quality.
5. **Automation.** Processes that can be automated should be automated, and those that can't should be automated as much as possible or be considered for elimination.
6. **Measure, monitor, report and action.** Without metrics, progress can't be assessed nor  processes improved. The Cloud Security Alliance suggests the most critical metrics include deployment frequency, vulnerability patch time, percentage code automatically tested, and automated tests per application.

While DevSecOps is still nascent in the Australian market we expect it to establish a strong presence based on the sound foundation DevOps adoption. Two thirds of Australian enterprise organisations say they are "mature" with DevOps and agile development methodologies. A similar amount express confidence that they are also mature with containers and microservices. However maturity does not automatically imply security as Australian companies have indicated that between 20% and 60% of all currently deployed applications require modernisation to run in a secure cloud automation environment.  Companies need to review their applications environments to determine potential weaknesses and work with internal teams and partners to priorities and address modernisation activity.



## 3 Things Businesses Must Consider for DevSecOps:

1. What is your starting point with DevSecOps? Is it to establish a robust, securely coded application? Does it focus on integrating security practices into the development cycles? DevSecOps isn't simply a software tool that is deployed once. Rather it is a philosophy that spans technology, culture and collaboration activities… oh, and it doesn't stop. It's a continuous approach.
2. DevSecOps moves security into being everyone's responsibility. It is as much about a cultural change as it is implementing processes and tools. Undertaken correctly, it fills the gap between applications development and security. In this context, does your current technology culture consist of an 'us and them' development and operations mindset? If so, this needs to change to reflect a more integrated, shared responsibility for DevSecOps to be effective.
3. Is your business ready to move at speed? Cloud and digital transformation has seen the rate of deployment of new applications rapidly increase and if unprepared, this rate of increase can quickly overwhelm security teams. What processes are in place to ensure that this does not happen?

## The Benefits of DevSecOps

There are a number of business and technology benefits that accrue from adopting a DevSecOps philosophy including:

- **Business operations and costs:** A more rapid detection of security vulnerabilities brings with it a reduced cost of application development and deployment, and, in a related area, more efficient management of resource libraries also contributes to cost savings. Critically, the risk of reputational damage and/or risk and legal liabilities due to a security breach are potentially substantially reduced.
- **Security posture:** A 'secure by design' principle ensures a more robust, cost-effective development process and, when coupled with automation (eg. Code reviews, security testing), a significantly improved security posture.
- **Culture:** As with its relative, DevOps, DevSecOps encourages an 'everyone is responsible' approach to security, creating a more open and engaged culture. In turn, this transparency and agility supports a focus of continuous, iterative improvements resulting in faster, more secure delivery of upgrades, features, products and services.

As with all technologies, adoption brings both benefits and complexity, and cloud is no different.

For many organisations the hybrid cloud environment is the default infrastructure platform and whilst significantly beneficial, realising its benefits of scalability, agility and security requires greater management attention than a single cloud infrastructure. The security landscape is ever changing in its complexity, and as technology innovation increases, is becoming more and more challenging for organisations to navigate on their own. Being successful with Secure Cloud Automation should be a goal for all IT and business leaders. Consider how these factors can be incorporated into your organisation's capabilities. Learn from others, look to partners and trusted vendors that can support your goals and have clear competencies in areas such as IaC, DevSecOps, cloud migration and professional services.

# The essential list

There are several important factors to consider in your technology strategy. We encourage leaders contemplating Secure Cloud Automation to consider the following principles as they execute on their plan:

**Workload by workload playbook:** Embrace the right location and architecture based on the outcomes desired from each application workload. This will involve enabling IT at the edge through to your core such that it incorporates a multi-cloud + data centre, multi-partner platform architecture.

**Security, Ethics, and Privacy by design:** Ensure that security experts, privacy leads and ethical considerations are included at the start of any new product or service developments and during the frequent releases you undertake, and are not bolted on after the fact. Beyond just including them in development, ensure you are striving to continuously improve them.

**Driven by customer and employee experiences:** In contemporary markets this should go without saying. But it is worth reinforcing in any changes or new projects you undertake.

**Space for innovation:** Embed a culture and structure that allows you to embrace new and innovative ways of operating and building products or services. Consider agile development, continuous integration and design thinking principles. Come to view innovation and disruption as a perpetual need.

**Network on demand:** Choose networking services that can be provisioned in real time, when you need them, allowing you to implement new projects, or add/change connectivity, at the pace you want to execute.

**Lowest latency performance and reliability:** Aim for the highest network and application performance to exceed customer or employee expectations. Take advantage of newly available, lower latency options as and when they are made available.

**Scalability:** Make sure you have the ability to scale as your business grows and changes – in size, volume and across geographic locations. Having scalability may also mean being able to scale your bandwidth up and down on demand, for burst requirements, or consistently.

**Automation everywhere:** Reduce the per transaction cost of every interaction by implementing system and process automation at every level. This can be as simple as automating common processes and releasing expensive IT employees to concentrate on higher value projects and tasks. Or automating identity access and management of employees to quicken the onboarding/offboarding processes.

**Sustainable management:** This may mean employing environmental sustainability, but it also relates to being able to ensure you can manage the APIs, data and overall systems you have alongside your cloud strategy and business roadmap.

**Commercial Flexibility:** Ensure you have a choice in CapEx and OpEx expenditure and outcomes-based contracts.

# The Nexon perspective

Through the development of expertise and strategic partnerships over nearly a decade Nexon has gained the position as trusted advisor for hundreds of Australian organisations who are on their own personal transformation journey.

At Nexon, we believe we can create the best value for customers if we place the right workloads in the right cloud. We manage and secure services for customers which have workloads across private, Nexon & public clouds. We also understand that whilst it may be 'Cloud First', the question remains '…but which Cloud?'.

It is undeniable that to stay competitive organisations must migrate core services to the cloud as it gives a level of visibility, flexibility and accessibility that just cannot be delivered with on premise technology.

A Multi-Cloud environment is the new norm for many businesses. Without doubt this approach brings many benefits yet it also increases the management complexity, can encourage application and infrastructure sprawl and requires a rethink of traditional security approaches.

Add in the fact that many organisations that maintain their own applications are moving to microservices, pursuing an agile development capability supported by DevOps and it is clear we have a heterogenous environment with kinetic applications that move across the hybrid infrastructure environment.

We firmly believe that in this environment, when businesses consider the growth in applications, data, and demands on IT from digital businesses, that automation is one of the key tactics that ensures companies can effectively manage and scale their IT infrastructure and applications as and when required.

From our deep experience of cloud, security and automation for our enterprise customers, we see endless benefits depending on the organisation's needs and different use cases in different sectors.

With the multitude of Cloud solutions in the market choosing the solution that best fits becomes difficult, particularly when the wrong solution has the potential to add significant complexity to employees.

The integration capabilities and ongoing support of each service becomes a critical factor in ensuring that the new integrated cloud managed service isn't just a collection of siloed technologies supported by different providers.

Navigating these worlds of cloud, security and automation is complex and many organisations turn to cloud service providers, such as Nexon for help and success. At Nexon we pride ourselves in understanding your business and delivering the right cloud for the right workload load.

## About Nexon Asia Pacific

Nexon Asia Pacific (Nexon) is an award-winning digital consulting and managed services partner for mid-market, and government organisations across Australia.  We have a uniquely broad suite of solutions to service clients who require end-to-end capabilities coupled with specialist expertise in security, cloud and digital solutions.

Our end-to-end solutions help clients to solve problems, address frictions and accelerate growth. Committed to the highest standards of responsiveness, competency and transparency, Nexon is built on a unique client care model that is fuelled by continuous feedback. With over 400 staff, we employ some of the country's most experienced consultants and empowers teams to make decisions that accelerate change for client organisations.

As a certified and accredited local and state government provider, CREST and ISO-certified, Nexon partners with world-class technology vendors to deliver innovative solutions and service excellence.

We help our clients move from a position of overwhelm to empowerment, looking forward to a more agile and digital future.

## About NetApp

In a world full of generalists, NetApp is a specialist. We're focused on one thing, helping your business get the most out of your data. NetApp brings the enterprise-grade data services you rely on into the cloud, and the simple flexibility of cloud into the data center. Our industry-leading solutions work across diverse customer environments and the world's biggest public clouds.

As a cloud-led, data-centric software company, only NetApp can help build your unique data fabric, simplify and connect your cloud, and securely deliver the right data, services and applications to the right people—anytime, anywhere.

## About Tech Research Asia

TRA is a fast-growing IT analyst, research, and consulting firm with an experienced and diverse team in Sydney | Melbourne | Singapore | Kuala Lumpur | Hong Kong | Tokyo. We advise executive technology buyers and suppliers across Asia Pacific. We are rigorous, fact-based, open, and transparent. And we offer research, consulting, engagement and advisory services. We also conduct our own independent research on the issues, trends, and strategies that are important to executives and other leaders that want to leverage the power of modern technology. TRA also publishes the open and online journal, TQ.

**www.techresearch.asia**

**Copyright and Quotation Policy:** The Tech Research Asia name and published materials are subject to trademark and copyright protection, regardless of source. Use of this research and content for an organisation's internal purposes is acceptable given appropriate attribution to Tech Research Asia.  For further information on acquiring rights to use Tech Research Asia research and content **please contact us via our website or directly**.  Disclaimer: You accept all risks and responsibility for losses, damages, costs and other consequences resulting directly or indirectly from using this research document and any information or material available from it. To the maximum permitted by law, Tech Research Asia excludes all liability to any person arising directly or indirectly from using this research and content and any information or material available from it. This report is provided for information purposes only. It is not a complete analysis of every material fact respecting any technology, company, industry, security or investment. Opinions expressed are subject to change without notice. Statements of fact have been obtained from sources considered reliable but no representation is made by Tech Research Asia or any of its affiliates as to their completeness or accuracy.

Talk to Nexon today to discuss how we can support your efforts to transition to a more dynamic business model that allows you to do more. call us at **1300 800 000**, email us at **enquiry@nexon.com.au**, or visit **nexon.com.au**