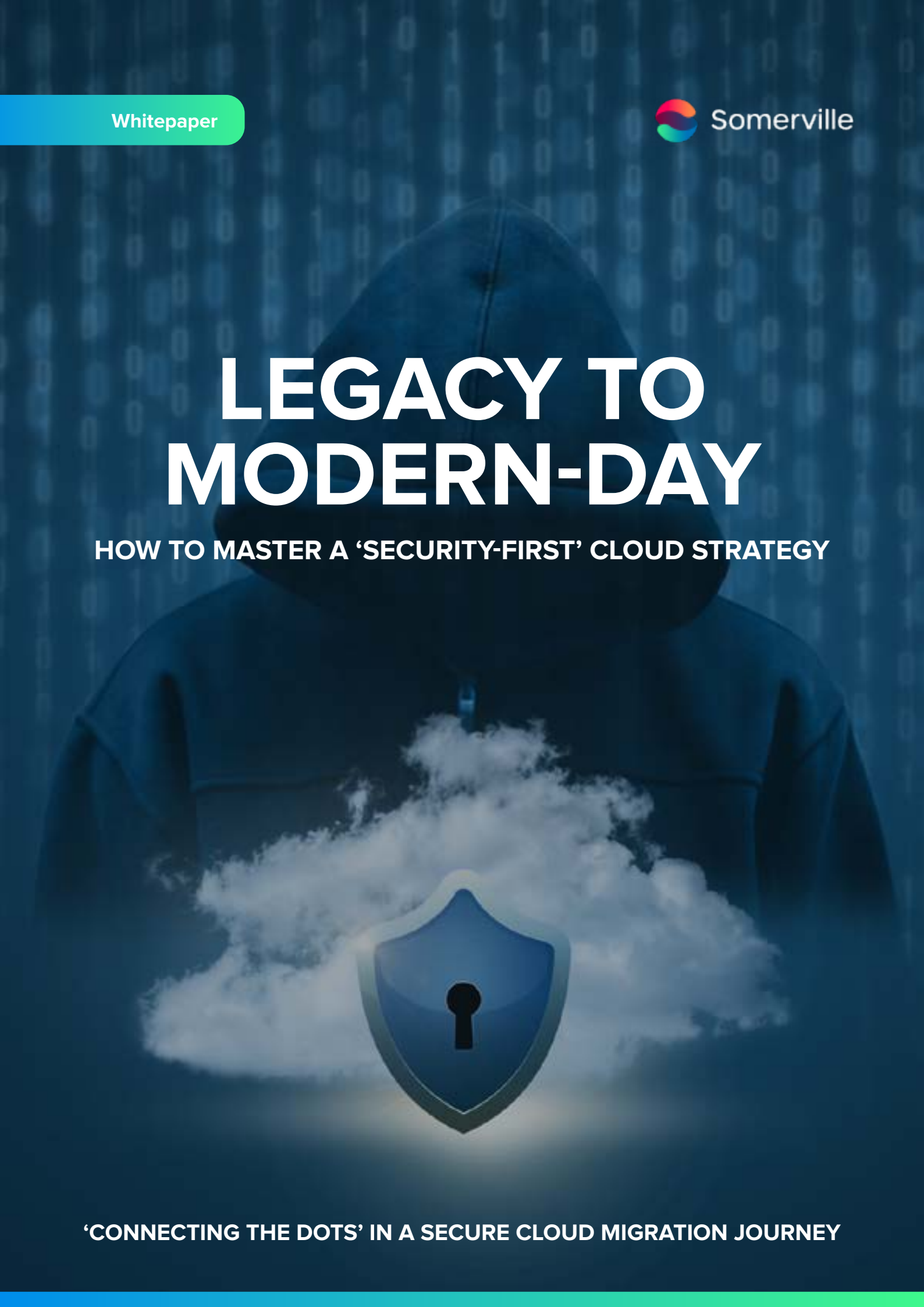
Whitepaper

Somerville

LEGACY TO MODERN-DAY

HOW TO MASTER A ‘SECURITY-FIRST’ CLOUD STRATEGY



‘CONNECTING THE DOTS’ IN A SECURE CLOUD MIGRATION JOURNEY

SECURITY IS

A CRUCIAL PART

OF THE CLOUD MIGRATION JOURNEY

Security is a crucial part of the cloud migration journey - particularly as organisations look to ditch their legacy systems and transition to a more agile and modernised world - but it's often the 'forgotten cousin' and relegated to the shadows.

In fact, many organisations aren't taking a 'security-first' approach and are failing to elevate security to its rightful and more prominent place in the IT food chain. Simply put, many organisations don't even know where to start, don't know how to control the security sprawl, and don't always consider adopting a 'multi-layered' approach as part of a centralised security strategy.

With a front-row seat to the action, a group of IT experts from Somerville, along with industry analysts at the coalface of the IT and security market (from IDC, and Ecosystm/Veqtor8) take a deep-dive into the 'secure cloud migration' journey - and reveal some practical approaches and defence tactics needed to change 'mindsets' and safeguard the fort.

From the current state of the cybersecurity threat landscape, to common pain points plaguing today's overloaded IT professionals, to the importance and value in adopting a secure hybrid approach, the experts take the pulse on these - and other - trends shaping the sizzling hot IT and security arena in the age of cloud.

LIKE LIFE, SECURITY IS A JOURNEY, NOT A DESTINATION

IN FACT IT'S MESSY, NEVER-ENDING, COMPLEX AND CONVOLUTED.

"It's a whole concept (a mindset) that customers - and many IT departments - don't always embrace, particularly as it relates to a secure cloud migration," according to Somerville Chief Information Security Officer (CISO) Kevin Koelmeyer.

"In fact, many organisations don't realise that security is a never-ending journey. It's a continuous improvement process - and it's not just one platform, or one product, but an ecosystem of multiple products; a multiple set of interconnected platforms that form security," Koelmeyer said.

"We're moving from a world of reactive, 'bolt-on' security, to embedded security, and integrity, to a world that begins to address the real security concerns of today and that reflects the 'age of digital,' new ways of working and accelerated push towards the cloud," Koelmeyer said.

Indeed, migration to the cloud is critical for companies to achieve digital transformation, meet business demands, stay relevant, accelerate innovation and build competitive advantage. But the security paradigm must change for each and every organisation as cloud-based deployments demand a consistent, more robust security framework that spans the entire cloud infrastructure.

What's more, when migrating infrastructure, applications and services - either through one of three popular migration strategies - rehosting (lift and shift); replatforming; or refactoring - the process requires a careful understanding of the security implications, Koelmeyer added.
"A cloud migration journey requires a 'security-first' cloud strategy that involves baking security into every aspect of IT, protecting endpoints, access points and networks, and focusing on continuous monitoring and management of cloud security risks and threats. It requires complete visibility across the entire IT environment in order to secure data, users and apps in the cloud."

Certainly, a secure and successful cloud migration requires many steps and considerations - from knowing the applications, data and environment; to understanding connectivity; to providing continuous monitoring and visibility across the entire network.

But let's not jump ahead too quickly. A 'rethink and refresh' of security policies, practices and procedures - and 'elevating' the importance of security company-wide and across board level, and connecting it into boardroom strategy - is a good starting point, according to Andrew Milroy, cybersecurity analyst, Adjunct Professor, Principal Advisor of Ecosystm, and Founder of research and consulting house, Veqtor8.

"Security isn't just something that should be discussed by technical people, rather, it's a board- level conversation; it's a corporate strategy," Milroy explained.

What's more, in the age of digital, industry experts agree that IT security needs to 'exit the shadows' and claim a more rightful and prominent place on any corporate agenda.

In fact, a number of factors are elevating temperatures of today's overburdened CISOs including: the rapid rise of the digital economy; the acceleration of digital transformation and increased push towards cloud migration; the large-scale uptake of remote work and distributed workforces; the glut of legacy systems unable to meet bulging data demands; and the ever-escalating cyber threats and vulnerabilities.

"The time to escalate the security agenda is now," Milroy said, explaining the frenetic digital transformation push - fuelled by the cloud surge and accelerated by the global pandemic - means cybersecurity should be at the top of the CEO's priority list.

And don't expect it to slow down anytime soon. IDC expects global spending on digital transformation technologies and services to grow 10.4% into $1.3 trillion.

In Australia, 54% of Australian and New Zealand organisations increased investment in digital innovation during the pandemic - and two-thirds expect it to increase in 2021, according to Gartner's annual global survey of CIOs.

ELEVATE SECURITY, CHANGE MINDSETS

INDEED, THE TIME TO 'ELEVATE SECURITY' AND CHANGE MINDSETS IS NOW, IF YOU CONSIDER OTHER RECENT NUMBERS AND TRENDS.

Between January and April of 2020, **cybercrime saw a sharp increase by 630%** of the amount of threats from external actors targeting cloud services as new ways of working created new vulnerabilities to exploit, according to a McAfee report, '**Cloud Adoption & Risk Report - Work-from-Home Edition**.' Two main categories emerged – excessive usage from anomalous location; and suspicious superhuman (both typically involve the use of stolen credentials), the report said.

Assessing today's global threat landscape - a world facing increased risk from the global health pandemic - analysts tell us that six main vulnerabilities and breaches dominate the charts >
Here in Australia, between July 1, 2019 and June 30, 2020, the Australian Cyber Security Centre (ACSC) responded to 2,266 cybersecurity incidents and received 59,806 cybercrime reports. On average, 164 cybercrime reports are made by Australians every day, or one report every 10 minutes, according to the **ACSC Annual Cyber Threat Report.**

"People don't realise there's no time to waste," Koelmeyer explained. "Every day that goes by, it's a case of new organisations getting infiltrated and compromised. In this day and age, the bad actors are going after the backups to encrypt them, destroy them, and encrypt the infrastructure. It's a nightmare - so companies need lots of education about the scare tactics of the dark web."

SIX MAIN VULNERABILITIES

- **social engineering** (the lion share of breaches in 2020 incorporated social engineering techniques, of which 90% were phishing);
- **ransomware**;
- **DDoS attacks;**
- **cloud computing vulnerabilities;**
- **access control;**
- **human error** (including mistakes in cloud configuration.

2,266

CYBERSECURITY INCIDENTS

59,806

CYBERCRIME REPORTS

164

DAILY CYBERCRIME REPORTS IN AUS

Throw in the complex issue of legacy systems (including the traditional 'legacy way' of securing applications and data) that are deeply entrenched and embedded across many private and public sector organisations, and there's clearly an unprecedented level of complexity and risk to mitigate - and why security evidently needs a 'front-row seat' to the action.

"Legacy security, in particular, means companies now have a lack of a cohesive security strategy, which has resulted in major confusion today," Koelmeyer added, explaining legacy systems lack performance, security and capability.

THE TOP CLOUD SECURITY CHALLENGES

There's lots to consider on the cloud security front. According to the Cloud Security Alliance (CSA), the top cloud security challenges are:

- data breaches;
- misconfigurations and inadequate change control;
- lack of cloud security architecture and strategy;
- insufficient identity, credential, access and key management;
- account hijacking;
- insider threats;
- insecure interfaces and APIs;
- weak control plane;
- metastructure and applistructure failures;
- limited cloud usage visibility; and
- abuse and nefarious use of cloud services.

CHECKLIST TO A 'SECURE AND SUCCESSFUL' CLOUD MIGRATION:

- Plan the migration approach to ensure apps are well suited for the cloud, and new designs on the cloud architecture are effective within the IT environment. (Somerville's Axen)
- Ensure data is encrypted (consider data in use/data in-transit) and understand data is the organisations' responsibility. (Veqtor8's Milroy)
- Ensure IT and security teams are working as a single entity, not as different units with competing objectives, to fully understand the difference between on-premise and cloud demands. (IDC's Piff)
- Make it a risk conversation - be aware of risk when moving to the cloud - and ensure the necessary controls are in place. (Milroy).
- Ensure security policies are applied in the cloud - for many companies it's an afterthought. (Milroy)
- Ensure visibility across all cloud assets. (Somerville's Koelmeyer)
- Forget about prevention - monitor the attack surface continuously and mitigate the damage in the event of a breach. (Milroy)
- Develop the infrastructure and access controls to limit the damage an intruder can cause. (Milroy)
- Take a cue from the physical security world and start locking down company information and data, put it in a safe, and lock the doors. (Somerville's Ranaweera)
- Ensure backup of your data/workloads - anything could happen or go wrong during a transition). (Ranaweera).
- Ensure you don't expose your data. (This could be using encryption through your systems, software or via using secured links). (Ranaweera).

COMMON PAIN POINTS UNMASKED

LET'S FACE IT: THE ISSUE OF SECURITY ISN'T GOING AWAY ANYTIME SOON - THE THREAT LANDSCAPE IS RAPIDLY EVOLVING - AND EDUCATION IS DRASTICALLY NEEDED.

In fact, as more and more organisations look to securely and successfully transition to the cloud (with hybrid cloud the preferred option–in part, for operational flexibility and more data deployment options), there's a host of security challenges and misconceptions to overcome. Here's a Top Ten list of customer 'pain points' to consider as organisations look to adopt a more modernised, agile and flexible IT environment, and aim to ditch legacy:

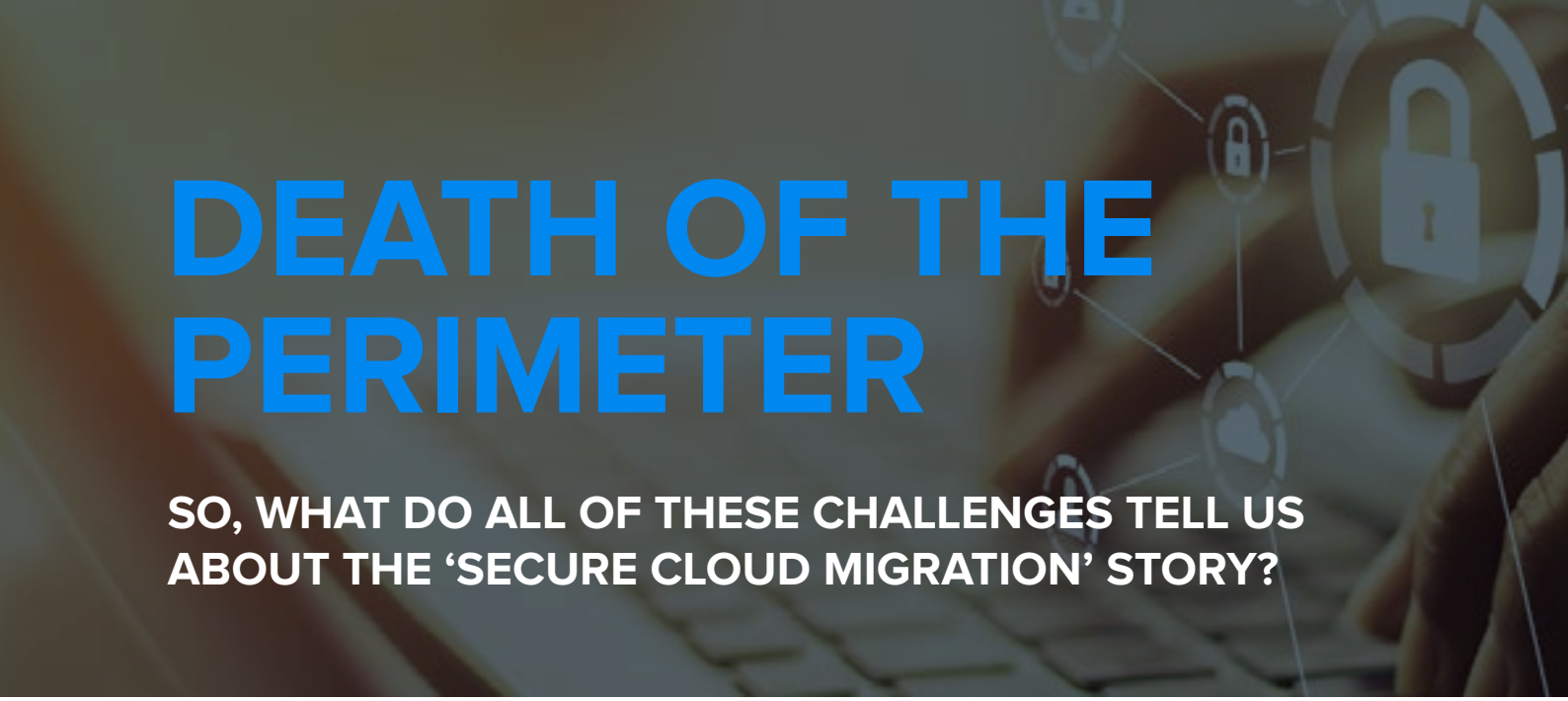
- Lack of understanding of IT environment and apps (and where workloads reside);
- Unsure what 'cloud' actually means, and the costs involved;
- Perception 'cloud' is either more secure or less secure;
- Unaware that 'security in the cloud' is still a customer's responsibility;
- Lack of messaging by public cloud players about customers' security responsibility;
- Unsure about changes in business/processes;
- Lack of understanding about hybrid and multi-cloud approach - and the fact many organisations can't go 'pure public';
- Unclear about minimum architecture or planning requirements;
- Lack of documentation on legacy apps and processes; and outdated hardware/ platforms that haven't kept pace with modern authentication methods; and
- Lack of understanding about the importance of a cohesive and continuous strategy.

Certainly, customers have a host of concerns, and many are centred around what "they aren't sure of; what they can't see; who's handling their data; and what type of support is on offer," according to Somerville Cloud Services Manager, Aden Axen, who suggests a 'workshop' approach is the only way to get to the bottom of it.

"It's like connecting the dots on how it works, all the way from the user endpoint right to the cloud - and 99% of the time when we sit with customers, workshop and listen, and discover their challenges (and also factor in the behaviours of the environment and different historical trends), we tend to reach a point of ease and comfort," Axen said.

He said customers need the right network administration and monitoring tools to analyse data usage, the bandwidth, throughput and performance in a bid to assess hidden costs, latency issues and other important factors.

"But remember security isn't a race - it's a continuous marathon. We have to protect and control heightened threats and vulnerabilities continuously - and customers need a good support team around them."



DEATH OF THE PERIMETER

SO, WHAT DO ALL OF THESE CHALLENGES TELL US ABOUT THE 'SECURE CLOUD MIGRATION' STORY?

First and foremost, "there's lots of confusion," according to Simon Piff, Vice-President, Trust, Security & Blockchain Research at IDC Asia/Pacific.

"To begin, I think we need to acknowledge the challenges of legacy security and the lack of a cohesive strategy that has resulted in the confusion of today. Most security solutions have been built as an after-thought to a business-driven 'productivity' solution. The timeline looks a bit like:

- Build/ install a computer – add passwords;
- Buy PC's – install antivirus;
- Connect to the Internet – install firewalls and VPN;
- Then it was 'protect the perimeter,' which has now been eroded by laptops, mobile devices, the cloud, IoT and Edge.

"When it comes to the cloud, organisations are challenged with how to address security. It requires a different approach to traditional on-premise IT security, and while most understand the semantics of the changes, many are challenged to make the leap to execute security procedures in a new way," Piff said.

So, what's driving this new way of thinking and seismic shift? In fact, it's super significant given the industry is witnessing the "death of the perimeter," Piff explained.

"The traditional tools of malware, firewall and VPN used to be sufficient, but with the growth in mobile devices, IoT and of course cloud, the 'edge' of corporate networks have dissolved over time. So traditional security approaches of 'defence in-depth' only work for part of the environment - and not the new extended environment."

What's more, the main shift from an on-premise viewpoint to cloud, Piff explained, is that on-premise has traditionally looked at networks, systems and devices, while cloud demands we look at identity, data, applications and device/ endpoints.

Given this new reality, Piff said organisations need to ditch the "bolt-on-after-the fact" security approach that companies typically engage in. Instead, start with data in mind, and ask the question: How can we use the data in the manner it's being used?

"Who could and should have access to this data? In what format? How is the data acquired and then curated? What applications touch the data, and what needs to be secured to ensure that only the approved applications touch the data?

"Then extend that thought process to identities, which could also include systems and devices. The business of IT is Information Technology - it has always only been about the information gleaned from the data, so ensuring its security and integrity should be the starting point."

In fact, with data as the starting point, there's a massive opportunity to take on a more 'proactive security' approach," Piff explained. "But all too often, the business is driving a demand for capability and capacity, which gets funded, and the IT team is responsible for ensuring the security, which gets underfunded, if considered at all."

QUICK CLOUD MIGRATION POINTERS

- Know your IT environment;
- Know your backup environment and regime;
- Understand your data and security;
- Perform cost control and monitor your environment;
- Ensure senior management buy-in;
- Know your support applications;
- Acquire the right applications; and
- Establish the right performance levels.

BUILD A SECURITY-FIRST STRATEGY

Certainly, a lack of apparent and obvious ROI from security means the discipline has generally been underfunded and under-resourced. So, how should companies overcome these challenges and think about security and the cloud migration journey - and get started today?

First, adopting a 'security-first' approach is one practical solution, Somerville's Koelmeyer said, and requires a multi-layered approach that involves "baking security" into the entire migration process.

"Security is a big part of migrating to the cloud. But many IT departments don't realise the cloud is inherently more secure. It has more bells and whistles, levers and knobs, so you can enable the security.

"But if you don't turn it on (adopt security measures like 2-factor authentication and continuous access) and enable it from the get-go (as soon as you migrate and as soon as you move in), then it's not worthwhile. In that case, practically speaking, you're not maximising the benefits of true cloud security," Koelmeyer said.

Better still, think of security at all times, and embed it across every aspect of the business. "A 'security-first' approach is the way forward and requires adding security aspects to everything we do. For example, if we need a new finance platform, ask the questions: Where is the data stored? How is the authentication done? Is there two-factor authentication?

"If the organisation needs a new product or platform and it doesn't have the proper security in place, then look at alternatives or push the software developer to upgrade to a more secure setup."

The approach also involves evaluating IT systems and determining where workloads need to reside, and controlling the security sprawl, Koelmeyer added. "Sometimes it may be appropriate to have the IT infrastructure in a datacentre or even on-premise, while other workloads are fit for SaaS or IaaS. The goal is to pick the right approach, and then wrap security around any multi-cloud approach."

And size doesn't matter when talking about a 'security-first' approach. "Companies of all sizes need to take security seriously. If not, they won't last long in business. They need to budget for security platforms - and it's not just anti-virus and anti-malware that's needed. It's not just one or two components. It's multiple components: Endpoint protection, firewalls, log analysis, vulnerability scanning, visibility and constant review."

What's more, it needs to be a multi-layered approach to achieve optimal security, and a centralised security strategy, Koelmeyer added. "All of the main security players, from Palo Alto Networks to Check Point Software to CrowdStrike, have a public cloud offering. So don't just depend on the native security of the public cloud, but look to add on third-party security components - and layer it."

8 HOT TIPS FOR A 'SECURITY-FIRST' CLOUD MIGRATION

- Implement a phased migration approach (helps IT teams develop familiarity with cloud);
- Check data integrity;
- Ensure backup;
- Encrypt the data (both at rest and in-transit);
- Minimize data loss;
- Understand the shared cloud responsibilities (data, applications, identities and devices used to access cloud systems are still the responsibility of the cloud customer);
- Know the compliance requirements; and
- Centralise monitoring (consider adopting a SIEM).

Better still, consider adopting SIEM (security information and event management), which provides organisations with advanced visibility, detection, analytics and response, according to Koelmeyer. “This pulls in logs from your local infrastructure, local servers, and workstation, as well as putting SIEM logs from the public cloud, so you have complete visibility across all clouds: public, hybrid, private.”

“You can pick up those needles in the haystack using SIEM platforms.”

Digging deeper, many security vendors are either moving into the SOC (Security Operations Centre) arena or extending their offerings, and pushing the technology ever-closer to the end user, Koelmeyer said.

“Vendors know they can scale it - and more protection is moving towards endpoint devices because of COVID-19. But endpoint devices are also being targeted more - so vendors are putting more focus in that area.”

Undoubtedly, what these and other defence measures highlight is that security is a “continuous journey” and organisations need to adopt a “review and revisit” security mindset, Koelmeyer suggested.
“Here’s a practical example: When we migrate a customer to Office 365 and enable 2-factor authentication and continuous access, we review two to three months down the track to ensure the security posture is correct,” Koelmeyer said.

“You have to continuously update the settings, and ensure you’re still at best practice – still moving forward in a secure environment - and then extend it down. How is your endpoint? Does it need updating? It needs to extend down (and not just into Office 365), but into all aspects of the organisation.

“It needs to extend to the users - and consider their inherent way of thinking. We need to foster a security mindset for the organisation and for staff, from securing the devices and the network at home to connecting it back into corporate.”

LEGACY SYSTEMS LACK PERFORMANCE, SECURITY, AND CAPABILITY

Somerville’s Ranaweera reveals the common pitfalls with legacy systems:

- Businesses today need high performance. You need quick turnaround times to keep your business moving. Legacy systems are not built with this in mind.
- Security was an afterthought in most legacy systems – security wasn’t a consideration when systems weren’t connected like they are today. But most systems and applications are now connected to the Internet and highly sensitive data is now stored in systems.
- Legacy systems lack the capability and functionality required by the users today. Technology has come a long way and modern systems are user-friendly and are built with efficiency in mind. And also allow great levels of connectivity.

According to IDC’s Piff, legacy systems age, and mostly, need more support over time.

“Unless the system is being retired on purpose due to declining use, something that rarely happens, then the main issue is being able to deliver the capacity required on aging infrastructure and applications.

“Hence the need to -re-architect for the cloud. But all too often systems outlive their working lives, draining valuable IT resources and frustrating the user with outdated processes and slow response times.”

OSHADHA RANAWEERA
Somerville Connect Services Manager

MAKING SECURE CONNECTIONS

At the same time, don't forget about the importance of connectivity when speaking about a secure cloud migration and a 'security-first' approach. according to Oshadha Ranaweera, Somerville Connect Services Manager.

"One of the primary considerations during any cloud migration is to determine how you establish connectivity between your workloads such as between private cloud to public cloud," Ranaweera explained.

"Here you need flexibility and the ability to scale capacity as needed. Many companies struggle here with mediocre Internet connections as the primary way of moving data between the clouds. Depending on the size of your workloads/data, you need to establish what level of connectivity requirements are needed. A few of the main considerations include:

- Capacity of the link;
- Link quality and symmetrical data transfer;
- Link capability to allow different configuration to allow the best level of setup;
- Ability to easily provision between DC and cloud environments; and
- Flexibility in the contract terms.

In fact, Ranaweera said 'connecting the connectivity dots' is all part of a good security transition plan and helps to foster a 'continuous' security mindset. "Transitions need to happen in a timely and secure fashion. But poor and unsecured connectivity prolong project timelines and expose sensitive data," Ranaweera said.

"Data and workloads require security. In a digitised world, all-important data is kept and stored digitally. Traditionally, important data is kept securely in locked up physical storage; similarly all digital data needs some level of protection.

"And when it comes to the cloud, this is more important than ever. As workloads can be located anywhere from the local DC to anywhere in the world. Security needs to be at the forefront when it comes to the cloud and any level of transition work."

Indeed, positioning security 'front and centre' of a cloud migration is critical considering more and more companies are moving away from legacy systems to modern-day technology - and need to ensure their security needs are met with minimal pain and aggravation.

"It takes time and careful planning to minimise pain. You need to segregate data from the systems. It's important to understand that what you need security for is your data. The system allows that security. As long as you have a transition plan to move your data from legacy systems to a new system/technology, you can minimise a lot of challenges you may otherwise face."

‘ZERO TRUST’ ON THE AGENDA

So, what other security defences can be applied? Milroy suggested organisations take a ‘zero trust’ approach as part of their ‘security-first’ strategy, which means being vigilant and adopting a “super breach” mindset.

“Assume you have a breach; assume you’re attacked and someone has broken into your system. You have to ensure the damage is limited - which means taking a ‘security-first’ approach,” Milroy said.

“Assume there’s someone in there doing bad stuff - so spend your time ensuring your systems, software, and network are secure and developed in such a way that the damage the intruder can cause is very limited.

“We’re in a world where you will be breached. It’s naive to think you won’t – and zero trust covers a lot: Assume a breach, never trust, always verify, and adopt the principle of least privilege. Make sure access is tightly restricted. Hackers are looking for people with the most credentials: the CEOs, and heads of department, or IT administrators.”

Certainly, zero trust offers an in-depth, formidable line of defence, agreed Somerville’s Koelmeyer. He said it delivers a range of benefits including: support for cloud migration; advanced visibility; reduced IT complexity; less demanding security workloads, data protection, and enhanced user experiences.

“With the traditional ‘perimeter-centric’ security strategy failing, a zero trust approach provides greater visibility, control and protection of users,” Koelmeyer said. “By never trusting and always verifying users, devices, applications and packets - the corporate network is better prepared and protected.”

BIG RISE OF CONTAINERISATION

Technological advancements are accelerating the world of security - and a popular trend to unfold is the rise of containerisation, according to Somerville’s Axen.

Containerisation offers big benefits on the road to digital transformation, Axen said. In short, it creates agility across the application life cycle, and delivers more strategic services, clouds and iterations. What’s more, it results in better resilience and continuity in the event of a failure.

“There are some exciting technology breakthroughs that have rocked this space. Containerisation is one of them. It’s exciting - we can get our DevOps teams to develop and deploy applications faster and more securely to what we’ve traditionally experienced, which has typically introduced barriers and slowed down agility,” Axen said.

“Serverless computing is yet another example of a tech advancement that runs code-on-demand without needing to host it on a server and managing infrastructure.”

Like Axen, Milroy said the security implications for organisations from the advent of containerisation are significant.

“We can now develop these little containers that are reusable, adaptable and flexible, and you can create a situation where if there’s a security breach, it only affects one small container.

“It’s a great way of taking security and being ‘security-first’ minded in your coding - meaning if there’s a breach, then only a very small amount of damage can be done to a tiny bit of a program,” Milroy said.

TAKING A SECURE 'HYBRID' APPROACH

At the same time, taking a hybrid approach - combining a private cloud with one or more public cloud services and mixing it with on-premise - is yet another powerful option for organisations looking to modernise the IT environment and safeguard the fort, Koelmeyer suggested.

Certainly, as both public and private clouds evolve, there's a surge to evaluate, design and build applications on hybrid cloud architectures - and many organisations are finding success moving towards a secure hybrid cloud approach.

Just consider the numbers: Global hybrid cloud growth will reach $53.3 billion in 2021 from $28.1 billion in 2019 - 93% of enterprises have a multi-cloud strategy; while 87% have a hybrid cloud strategy, according to the Flexera 2021 State of the Cloud Report.

But "one size never fits all", particularly when dealing with legacy apps, according to Somerville's Axen. "Each customer requires a very different approach; we focus on moving workloads into where it's best suited, either public or private solutions."

Reducing costs, gaining flexibility, scalability and improving collaboration are high on a customer's wish list. "So too are an always-on solution and zero downtime. Customers want better security controls and data security. They want to eliminate the term legacy - stop being tied to hardware - and want the freedom to roam, and the ability to innovate and move quickly on new business ideas and initiatives."

What's more, a hybrid cloud strategy, said Axen, is often the preferred option (it tends to become a necessity as companies expand and grow), as it gives customers the ability to choose the optimal solution for each task and maximise workloads.

Once ensuring the most relevant security control policies and procedures are in place, it enables customers, for example, to use a combination of on-premise infrastructure to store sensitive data and meet compliance regulations; and public cloud services for application development.

But a 'lift and shift' approach isn't always ideal, Axen explains. Organisations mistakenly think 'lift and shift' is the 'simple first step' towards a hybrid cloud - an easy way to move the apps most ready, and best suited to a private or public cloud, while continuing to host other application workloads on-premises.

But "going the extra mile" and considering other cloud options (and the associated security measures) like 'cloud-native' is often a better approach, Axen suggested.

"Legacy apps have always been a point of discussion - and typically we see the fastest method is to 'lift and shift' the application. But we take it that little bit further with the approach and consider other options - first around security controls, then around the application exposure - and whether a cloud native scenario is more suitable," Axen said.

"We determine what can be refactored to enable a native cloud experience, and what's best suited to leverage a SaaS model. You'll want to be leveraging cloud native options, as best as possible, and wherever you can.
"It's all about determining the right workload for the right location. And we're able to help join up the dots in every situation."

Certainly, "connecting the dots is crucial," Koelmeyer agreed, explaining the 'lift and shift' scenario is often "the worst approach." Instead, he encourages customers to perform a business analysis and process analysis, so "they can re-tool, or change the process to work with the cloud, be it public or hybrid."

This 'gap analysis' helps determine how the cloud environment will affect the security paradigm; and determines the impact of a cloud-based network on overall risk management.

PARTNERING FOR SUCCESS

What these and other points of discussion highlight is the fact that many organisations have questions – and need some answers on the security front. And if history teaches us anything, it's that collaboration and forging partnerships are critical to success. This adage has never been truer than in the world of IT - and in the cloud era.

And businesses need help - particularly the mid-market, which tends to "lack a real and solid understanding of the relationship between security and the cloud" - resulting in many turning to a trusted partner to ensure a secure and successful cloud migration and rollout of a continuous security strategy, according to Veqtor8's Milroy.

Certainly, aligning with partners and trusted advisors is critical in the cloud migration game - particularly as it relates to security, agreed IDC's Piff.

"When it comes to cloud security, which is a relatively new idea as compared to other forms, it pays to talk to as many experts as possible to understand the nuances that make cloud security so different."

Somerville's Koelmeyer agreed, saying organisations need help 'connecting the dots' when it comes to security - particularly in the 'age of digital,' and operating businesses in a world becoming cloud-centric.

"There's still organisations with server rooms on-premise, and all of their workloads on-premise, with no care or consideration for security. It's a case of trying to open their minds to think of security first."

What's more, companies need the freedom to focus on their core competencies, drive their businesses forward, and seek the guidance of a trusted partner to help them achieve best practices, establish a robust security plan, and embark on the journey, he said.

"Organisations need to depend on their partners, work with them and make sure the security approach is right for them. Once they realise that IT security is a never-ending journey (a continuous process), and with the help of their partners, they can take a risk-based, outcome-driven approach that meets their business needs, their budget, and their key objectives."

But choose your partners wisely - and always ask questions. "Partnering is the key. Internal IT needs to realise they aren't always the experts and don't have all of the answers, so rely on your chosen partners.

"And do your due diligence: Make sure the partner has the proper cloud credentials, and is focused on 'security-first.' If you pick the wrong partner and they have a lapse in security, it can be disastrous for the migration and the company."

Certainly, "security is a journey - and like in life - it's much better shared with a partner," Koelmeyer said.

THANK YOU TO OUR CONTRIBUTORS

SIMON PIFF

Vice-President, Trust, Security & Blockchain Research at IDC Asia/ Pacific

ANDREW MILROY

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

KEVIN KOELMEYER

Somerville Chief Information Security Officer (CISO)

ADEN AXEN

Somerville Cloud Services Manager

OSHADHA RANAWEERA

Somerville Connect Services Manager

About Somerville

As one of the most experienced end-to-end IT service providers in Australia, Somerville have been delivering almost 40 years of exceptional service and value to our customers across a wide range of industries including; finance, education, legal, insurance, superannuation and automotive. We believe in forging genuine partnerships with our customers, and take the time to understand business needs and internal IT capabilities, to develop innovative solutions to IT challenges that enable change for tomorrow and beyond. Our services include; connectivity, security, cloud, modern workplace, and hardware and software procurement, delivered by our Australian-based team of skilled engineers and all backed by proactive 24x7x365 support, so organisations can rest assured their critical systems are up and running round the clock.

Somerville Technology Pillars

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