



Embracing Secure Access in a World of Rapidly Expanding Virtual Borders

With organizational users and consumers both adopting cloud applications faster than ever before, enterprises are tasked to keep pace with a crucial responsibility: ensuring secure access to this multi-cloud reality.

Contents

A. THE IMPACT OF COVID-19 ON CYBER SECURITY ATTITUDES AND BEHAVIOURS

- a. Examining enterprise cybersecurity reactions in Singapore
- b. Critical risk, security and compliance considerations for the modern IT leader

B. MULTI-CLOUD: AN URGENT ENABLER FOR COMPETITIVE DIFFERENTIATION

- a. Evolving behaviours and technologies driven by consumers in the New Normal
- b. Maintaining visibility and secure access in an expanded cloud application ecosystem

C. VISIBILITY AND COMPLIANCE: A CHECKLIST FOR THE MULTI-CLOUD ENTERPRISE

- a. The necessity of consistent cross-cloud security policies
- b. Assembling the right cloud visibility toolkit for your enterprise (NDR, SIEM, etc)
- c. A purchasing guide: prerequisites for centralized cloud security tools

D. NAVIGATING THROUGH THE BLIND SPOTS OF RAPID, UNSECURED DIGITIZATION

- a. Urgent must-haves for expanding remote workforces and growing application stacks
- b. Business Continuity Planning (BCP): Readiness and reinvention
- c. Security implications and future-proofing lessons for a reality in flux

E. ZERO TRUST ACCESS POWERED BY SOFTWARE DEFINED PERIMETERS

- a. Key security learnings from business reinvention across industries
- b. Devising the right security formula for today's hybrid, adaptive modern enterprise
- c. The IT leaders toolkit for strategic user, endpoint and IoT security

F. ABOUT IVANTI

THE IMPACT OF COVID-19 ON CYBERSECURITY ATTITUDES & BEHAVIOURS

Examining enterprise cybersecurity reactions across Singapore


Against the backdrop of a new normal, C-level decision makers across enterprises have had to adapt to a constantly evolving reality by formulating agile plans to sustain, reimagine, and future-proof their businesses.



To this end, Frost and Sullivan analyzed the sentiments of one hundred (100) enterprises within Singapore to gain insights into their COVID-19 reactions, responses, and attitudes. A majority of the executives interviewed were CEOs, CFOs, or COOs (74%) at large enterprises over 500 employees (70%), over BFSI, retail, manufacturing and healthcare verticals. The key takeaways from this research revolved around the following critical learnings:

Reduced business demand:	Due to COVID-19, 59% of enterprises interviewed in Singapore reported a moderate reduction in demand for their business services and solutions by 1-9%. Enterprises in Singapore were noticeably less affected than the average (69%) that attested to the same across all interviewees in Singapore, Australia, and New Zealand.
Increased adoption of cloud:	48% of enterprises in Singapore stated that they had increased their adoption of cloud-based solutions during the pandemic, while 52% affirmed that this increased adoption was enabling them to better meet client needs.
Perceptions of cybersecurity:	Enterprises in Singapore showed a slightly lower average increase in cybersecurity licensing, with 56% of respondents reporting a 1-5% increase, compared to the overall average of 60% of enterprises reporting the same over all regions. The pandemic has also resulted in a reduction of cybersecurity budgets, with a majority of enterprises across Singapore (58%) stating that they would stop buying new cybersecurity solutions and only focus on vital refreshes.

Remote versus in-person offices:	Enterprises in Singapore, while open to the idea of allowing employees the flexibility to choose between remote and fixed office locations in the future (62%), were less supportive of this trend than the regional average (71%) over Singapore, Australia, and New Zealand.
Biggest challenges:	On average, the biggest challenge of remote work faced by enterprises in Singapore pointed to the undertaking of effectively securing remote devices. Other major areas of concern were new employee onboarding, data and application preparation, employee communication, patching and maintenance.



Critical risk, security and compliance considerations for the modern IT leader

Outside of just internal company toolkits, digital solutions encompassing all aspects of life and business have rapidly moved from physical to virtual environments.

Remote learning, teleworking, e-health services, online retail, online payment, and countless other offerings have taken day-to-day essential tasks and made it easy and convenient to accomplish the same goals virtually.

The enterprise attack surface has expanded, growing past physical and traditional bounds into a virtual plane with endless unsecured endpoints, IoT devices and a myriad of other digital enablers. At the same time, the pandemic has limited budgets, with enterprises in Singapore focusing only on vital refreshes and shaving down their cybersecurity investments. 58% of enterprises in Singapore stated that they planned to stop buying new cybersecurity solutions and would only proceed with vital refreshes while 32% claimed that they would only proceed with planned refreshes. In terms of critical areas for cyber security spending, respondents in Singapore pointed to secure web gateway (41%), software-defined perimeter (40%), network sandboxing (38%) and anti-phishing (38%) as the four leading solution approach areas.

On the other hand, respondents across all regions experienced a higher number of cybersecurity incidents during the pandemic. The percentage of respondents who experienced security incidents increased from 33% to 41%. This strongly outlines the case for enterprises to recognize security as a business enabler now more than ever, despite economic uncertainty, and to factor in contextual realities in their security strategies:

Simplifying security stacks



When the pandemic initially hit, businesses didn't have the time to thoroughly develop and implement new systems, or even conduct prior gap analyses of existing technology; they were forced to entirely digitalize almost overnight. This has led to a whole host of single-purpose point solutions, shadow IT, and band-aid technology fixes for ever-evolving business problems.

Now, CTOs and CIOs must step back, relook at their old technologies versus their newly digitized ones, and work toward a shift from monolithic technology stacks to flexible, dynamic combinations of cloud, microservices, and democratized data access.

Embracing integrated security



Despite the pandemic leading to a spike in compromised data and cybersecurity attacks, organizations continue to adopt single-pronged approaches to security, such as a single intrusion detection solution or ramped up employee authentication efforts. This is not an exhaustive stance: security that is truly holistic is integrated and goes beyond individual methodologies within a CIO's toolkit.

To be adaptable to future risk, and not just keep its head above water with the crisis of the day, a business needs a security strategy that is end-to-end, consistent, and automated.

MULTI-CLOUD: AN URGENT ENABLER FOR COMPETITIVE DIFFERENTIATION

■ Evolving behaviours and technologies driven by consumers in the New Normal

Multi-cloud ecosystems are the new reality, with Frost and Sullivan research revealing that 99% of respondents in Singapore use two or more public cloud service providers.

Singapore respondents had the highest propensity of using over two providers, with 23% reporting the usage of three or more providers compared to the overall total of 19% who reported the same. In today's cloud-first world, businesses that are able to stay ahead of the curve are the ones who have perfected the art of customer-first service delivery. To stay competitive and to enable this complex ecosystem of critical priorities, CIOs and CISOs are focusing their innovation efforts around:



Personalising experiences by moving to unified platforms to allow consolidated customer touchpoints – traditional business models run different operations on a large number of fragmented media channels. Moving to a single unified platform allows for supporting seamless experiences across every customer touch point.



Collaboration that easily connects people, systems, and information – enabling visibility into every part of the customer journey. C-level executives who succeed at implementing this correctly are learning that this is the answer to some of their biggest challenges - providing a reliable and consistent customer experience, and curating top talent.



Allowing easy access to all the data needed to make important decisions

– Technologies such as the internet of things (IoT), artificial intelligence (AI), big data and machine learning (ML) are powering business decisions by boosting competitive insight efficiencies. This hasn't always been the case - the past few decades have been missed opportunities for insights and analytics. Today's suite of analytical technology enablers are pushing data-driven decision making to the forefront of business strategy.



Expanding the boundaries of a single cloud environment

– The shift to a multi-vendor cloud landscape is a result of several concurrent factors: separate internal teams sourcing their own cloud resources, shadow IT, compliance or integration requirements leading to the addition of new vendors - the list is endless. At the end, enterprises often end up with expensive and continually growing multi-cloud setups that are often more complex than initially imagined.

Maintaining visibility and secure access in an expanded cloud application ecosystem

Frost and Sullivan's research uncovered a general sense of overhaul amongst IT teams within enterprises in Singapore, who had to improvise their security support processes to adequately respond to the remote working landscape.

59% of businesses in Singapore stated that they created processes in an ad hoc manner to support this remote workforce, with 32% stating that they had to partially structure deployments following incomplete business continuity planning arrangements.

In the midst of this overhaul, a majority of respondents amongst enterprises in Singapore indicated that they only had partial visibility of their cloud applications (50%) while others (27%) stated that they in fact had minimal visibility, both in terms of volume of secure access and activity visibility.

To that end, it is all the more urgent to bring secure access and centralized visibility to the forefront of an enterprise's security strategy, given all of the following new catalysts driving today's risk landscapes:

1 Architectural complexity: With multiple cloud providers, an enterprise has to live in multiple ecosystems. This has created one of the biggest security challenges in multi-cloud environments: applying a single and comprehensive visibility and access strategy over the entire network becomes incredibly challenging. While each cloud provider that works with an enterprise might have a well-planned, seemingly airtight security strategy, plugging security gaps over providers across multiple cloud ecosystems becomes much more complicated.

2 Compatibility issues: Architectural complexity: With multiple cloud providers, an enterprise has to live in multiple ecosystems. This has created one of the biggest security challenges in multi-cloud environments: applying a single and comprehensive visibility and access strategy over the entire network becomes incredibly challenging. While each cloud provider that works with an enterprise might have a well-planned, seemingly airtight security strategy, plugging security gaps over providers across multiple cloud ecosystems becomes much more complicated.



3 Wider attack surface areas: The number of applications (and the volumes of data) that live in digital realms have surged through the roof. And with this, hackers have more opportunities. With more targetable points of entry than ever, security professionals have to work harder and smarter to effectively manage their threat perimeters.

4 Increasingly intelligent attacks: Hackers are getting more sophisticated, with smart, modern technologies acting as catalysts. The same advanced technologies (such as artificial intelligence) that are available to security professionals are also available to cyber criminals. With the addition of an enormous volume of devices and endpoints in varying degrees of architectural complexity when placed relative to an enterprise's core infrastructure stack, today's security challenges are framed by a new objective: to extend the boundaries of secure access beyond traditional network borders.

NAVIGATING THROUGH THE BLIND SPOTS OF RAPID, UNSECURED DIGITIZATION

Urgent must-haves for expanding remote workforces and growing application stacks

Enterprises cannot afford to stay in a static state of security transformation.



Every stakeholder in the ecosystem - suppliers, partners and end-customers - now demands a higher level of security compliance. The starter pack for laying out the right groundwork for an agile, responsive security posture revolves around the following foundations:

Modernizing the security solution stack: This points to implementing next-generation security technologies such as next-generation firewalls (NGFWs), next-gen endpoint security, identity and access management (IAM) and multi-factor authentication (MFA), and using these techniques in conjunction with a comprehensive breach response plan. There are endless technologies that exist just to make these toolsets easy to manage – and even apply Firewall policies, IAM, and MFA across entire ecosystems – whether an enterprise’s application suite lives on-premises or in the cloud.

Guard your endpoints with zero trust models: Endpoints are among the most vulnerable segments of multi-cloud environments, making it more necessary for enterprises to adopt uniform security solutions that support all of their individual cloud infrastructures. These endpoint security tools need to be firmly rooted in zero trust models to be effective, in addition to being centralised.



Enforce single pane vulnerability scanning: To centralise the highly critical process of vulnerability scanning, enterprises need to point the collective strength of their security products over all their constituent cloud services so that aggregated vulnerability data can be actioned on in one spot.

Business Continuity Planning (BCP): Readiness and reinvention

The lesson of 2020 is clear: businesses that want to survive need to develop agile business continuity plans that can outlast not just this pandemic, but crises of varying kinds and magnitudes.

Even after COVID-19, the future will continue to see unexpected challenges. Only 1% of respondents in Singapore attested to having pre-existing BCP plans that adequately catered to COVID-19, with 68% reporting that while they did have a predefined BCP in place, it was not designed to address the required pandemic response.

And here's where the need to reimagine BCP comes in. It is imperative that this plan is continuously updated and reviewed on a regular cadence whether it be weekly, monthly or quarterly, to take into consideration all internal and external factors that might require situational adaptability. In converting a static BCP to a dynamic one, the following are must-have characteristics to build a base of resilience in times of future crises:

	<p>Assess how existing BCPs are working on at least a semi-regular cadence: Identify and analyse any deficiencies in the current plan with a thorough root-cause analysis that spans all possible factors—infrastructure shortages, delayed action, staff shortages, and any external variables.</p>
	<p>Based on identified deficiencies, ensure that new internal guidelines are created and enforced in a timely, proactive manner. These guidelines, by function of being iterative, would be built around recent lessons learned and serve as living contingency plans instead of static, moment-in-time ones.</p>

Security implications and future-proofing lessons for a reality in flux



As organisations reimagine their supply chains, spin up more digital experiences, and brace themselves against the realities of mostly-to-fully remote workforces, threat actors are aggressively focusing on all the new vulnerabilities being exposed. In response, agile security leaders are leveraging approaches such as zero-trust frameworks to provide secure remote authentication to an expanded surface area. However, no single product or solution can replace the effectiveness of an enterprise-wide commitment to holistic security, and it is the responsibility of the entire organization to ensure that every business unit is on the same page when it comes to privacy and data security. More than just bleeding edge tools, businesses need consistent policies that are applied cohesively over the organization, that both make sense to stakeholders across business units and also can be put into motion easily and repeatedly.

VISIBILITY AND COMPLIANCE: A CHECKLIST FOR THE MULTI-CLOUD ENTERPRISE

■ The necessity of consistent cross-cloud security policies

From a policy standpoint, Frost and Sullivan research found that enterprises largely developed endpoint device security policies specifically for the COVID-19 pandemic.



In Singapore, 53% of enterprises affirmed that their endpoint device security policy was created specifically for the pandemic, while 34% stated that while they had existing policies, these had to be further refined to better suit new requirements.

In terms of visibility, on the other hand, most respondents stated that they only had partial visibility of their cloud applications. Singapore respondents had the least amount of visibility over their cloud applications compared to Australia and New Zealand, with only 23% of enterprises in Singapore reporting full visibility, 50% reporting partial visibility and 27% reporting minimal visibility. In contrast, the overall total for enterprises reporting full visibility was 28% across all three regions, with 56% reporting partial visibility and 17% reporting minimal visibility.

With enterprises heavily adopting multi-cloud architectures, security leaders are moving towards integrated cybersecurity frameworks to provide the consistency in visibility and policy management they need.

A unified security layer provides comprehensive coverage for endpoints, enabling the application of a single set of rules and policies applied over the entire network, and allowing for visibility across the entire operation. With MTTR (Mean Time to Respond) being a key performance indicator of successful security strategies, shared threat intelligence and data analytics applied through integrated security suites allows for faster response and more thorough remediation. The biggest pitfalls of siloed approaches - blind spots, redundant complexities and areas of missed responsibility - can then be smoothed over by efficient, data driven threat detection.



Assembling the right cloud visibility toolkit for your enterprise

The threat detection landscape has grown more complex, with infrastructure having evolved beyond well-defined endpoint perimeters.

In today's reality in flux, the diverse combinations of Bring Your Own Device (BYOD), Internet of Things (IoT), and public cloud deployments are demanding significant retooling of traditional endpoint detection processes. In addition to shifting employee behaviours, enterprises have also begun expanding corporate information networks to keep pace with competitive needs, allowing their suppliers and partners greater access to their proprietary networks. Amidst all of these competing factors, overextended security teams are constantly in danger of threats going unnoticed - either getting lost in a storm of false positives, or slipping through the blind spots created by patchy, disconnected security infrastructures.

As a result, enterprises are using a multitude of approaches to successfully scale their security operations amidst these challenges: ranging from Security information and event management (SIEM), User and Entity Behavior Analytics (UEBA), Endpoint Detection and Response (EDR), and network-centric detection and response (NDR) tools such as from Network Traffic Analysis (NTA) and Network Forensics Tools (NFT) to Intrusion Detection and Prevention Systems (IDPS).

However, there are degrees of variability to these approaches depending on the scale, volume of critical assets, and range of solutions an enterprise functions on. An enterprise still needs to keep its eye on the prize: strategic, contextually aware, zero trust security. By basing core requirements around secure access and zero trust frameworks, security leaders can avoid two major pitfalls of an all-in-one approach:



Inaccurate security rules, algorithms or policy controls: In this case, a security leader could have the best and latest tools at their disposal but due to inaccurate policy setting, these products incorrectly identify certain endpoint behaviours as malicious and raise an alert, hence drowning security teams in an avalanche of constant false positives.



Correct security rules, but incorrect business/environmental context: Here, security products can flag valid alerts - detected behaviours are in fact malicious, but when observed in a business context lens, are either benign or even necessary. In this case, events such as employee-driven application repurposing or extended network rights to suppliers and partners can take up valuable remediation resources, moving attention away from unsecured and actual threat triggers.

ZERO TRUST ACCESS POWERED BY SOFTWARE DEFINED PERIMETERS

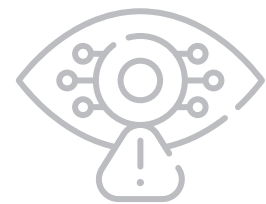
Key security learnings from business reinvention across industries

By creating systems that emphasize innovation as much as operational resilience, adaptive businesses are emerging as competitive leaders likely to be much more prepared for the next crisis. In thinking of the main catalysts behind shifting business processes, three leading drivers come first before all others:

Rethinking operational and service delivery structures:	By embracing flexibility, businesses are finding out of the box solutions to provide client service during unprecedented times. The opportunities here range from providing skinnier pricing packages that shave service down to the essentials, to providing repurposed versions of standard product lines more suited for the customer's current needs, to reducing operational expenses by rethinking delivery structures. With clients also experiencing their own host of unique pressures and challenges, they are likely to be a lot more open to unconventional offers and appreciative of vendors who demonstrate creative thinking in challenging times.
Enforcing cross-business security alignment:	As organisations reimagine their supply chains, spin up more digital experiences, and brace themselves against the realities of mostly-to-fully remote workforces, threat actors are aggressively focusing on all the new vulnerabilities being exposed. In response, security leaders are leveraging approaches such as zero trust frameworks to provide secure remote authentication to an expanded surface area. However, no single product or solution can replace the effectiveness of an enterprise-wide commitment to holistic security. More than just bleeding edge tools, businesses need consistent policies applied cohesively over the organisation, that make sense to stakeholders across business units, and that can be put into motion easily and repeatedly.
Powering enterprises perimeters with zero trust security:	Within today's newly remote world, a large number of popular communications options such as Slack or Zoom have still yet to meet comprehensive security requirements. While the utilisation of these applications is limited within industries like government or healthcare due to their high barriers for entry and stringent security requirements, this is not the case within the private sector where these applications are widely used. This is where zero trust models play effective gatekeepers: by analysing and monitoring security gaps resulting from the adoption of new platforms, zero trust policies are built around frameworks that minimize risk from external applications. Additionally, zero trust acts as a unifier for in-house authentication policies, filling in for the gaps and vulnerabilities created by the external vendors with insufficient safety controls.

Devising the right security formula for today's hybrid, adaptive modern enterprise

Cyber criminals are now targeting the underlying technologies that are supporting a growing remote workforce, such as video conference platforms, project management and collaboration tools, and virtual private networks (VPNs).



Critical assets and customer data reside within these applications, widely flung over the network edge, scattered over an ever-expanding net of endpoints.

Manual, disparate tools are not sustainable, and by having fragmented and overly complex security stacks, enterprises often unwittingly make it easy for vulnerabilities to be exposed. These blind spots - whether related to people, processes or technology - muddy the waters of risk reduction efforts. As a result, security leaders have to work twice as hard to gain visibility into their network, core, and cloud edges. Frost and Sullivan's research uncovered that:

While **consolidation and integration of solutions** was very important to respondents across Singapore, Australia, and New Zealand, fewer enterprises in Singapore found this relatively very important (69%) than the total average (71%).

At the same time, the importance of **zero trust frameworks** increased across the board with 75% of all enterprises interviewed stating that this was very important during the pandemic, compared to the 64% who felt the same before the pandemic.

To that end, the modern enterprise's security toolkit can begin with a two-part technology approach that focuses on:

- 1 Complete visibility and centralised control** by deploying solutions that provide a single view of threats, technology management, vulnerabilities and perceived risks across an organization's entire environment. When enterprises enter the market for new security vendors, the key features they need to look for include threat detection and response, penetration testing, vulnerability testing and scanning and security technology management.
- 2 Support for multi-cloud and diverse environments:** In order to address the mounting challenge of protecting globally dispersed data and compute environments, it is critical that the modern enterprise's security stance encompasses assets in all environments, whether on-premises, public clouds, private clouds, or a mixed setup.

The IT leaders toolkit for strategic user, endpoint and IoT security

A strategic CISO's objective in today's world of rapid innovation is to make sure that their security deployment is operating in a truly end to end cohesive, collaborative manner: starting from the core, extending to the edge and encompassing the cloud.

When security processes are aligned with business goals, it becomes monumentally easier to ensure that security planning maps to the business, stays in sync with IT initiatives, and helps win executive buy-ins faster.



Steps towards this goal include, but are not limited to:

Being end-to-end: By using a zero trust strategy, an organization can seal up every access point, making it easier to construct and maintain a robust security architecture. End-to-end encryption then closes the loop so that data can never be accessed by unauthorised users.



Being cohesive and collaborative: Making sure the entire security stack communicates within itself is the first piece here. The second is putting the user of data, whether person or device, at the centre of the security stack's focus.

Leveraging real-time threat intelligence: With today's highly sophisticated threat landscape, security solutions need to be smarter, quicker, and almost all-knowing. AI-enabled machine learning makes this possible, fuelling real-time threat intelligence for highly automated prevention, detection and mitigation processes.

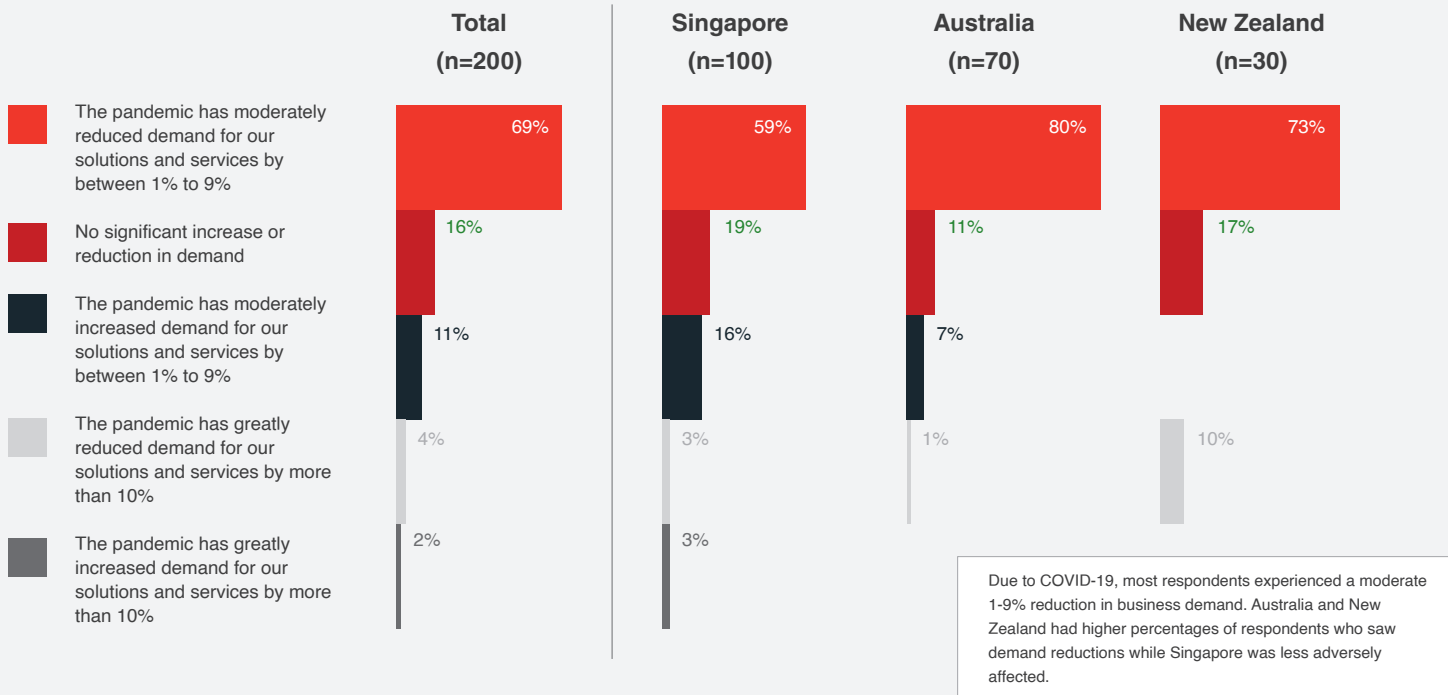


Regardless of an enterprise's chosen security stack, zero trust access forms the glue that binds together any number of toolkits, applying a laser focus approach to leverage the optimal competencies of each layer. Given the massive and multiplying expanse of users, endpoints, multi-cloud and distributed networks and rich IoT diversity, IT leaders can harness the power of automated visibility, access provisioning and threat response to truly safeguard their critical business networks.

DATA APPENDIX

Data callout #1: Due to COVID-19, 59% of enterprises interviewed in Singapore reported a moderate reduction in demand for their business services and solutions by 1-9%. Enterprises in Singapore were noticeably less affected than the average (69%) that attested to the same across all interviewees in Singapore, Australia, and New Zealand.

Figure 1: COVID-19 has negatively impacted business for enterprises



Data callout #2: 48% of enterprises in Singapore stated that they had increased their adoption of cloud-based solutions during the pandemic, while 52% affirmed that this increased adoption was enabling them to better meet client needs.

Figure 2: Enterprises have had to adopt the cloud more during the pandemic

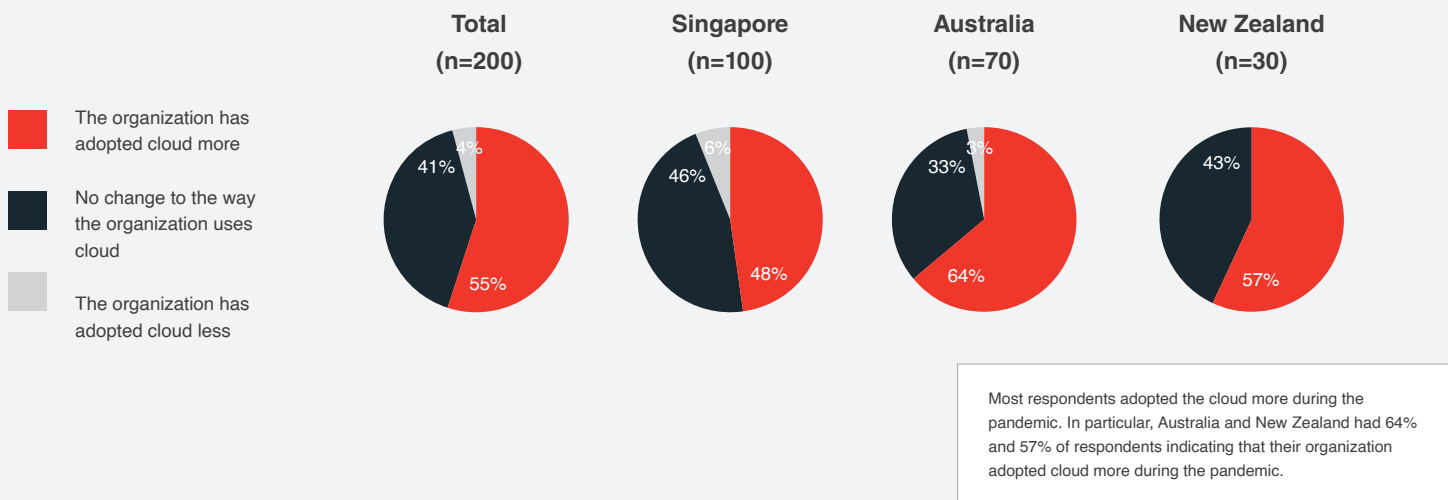
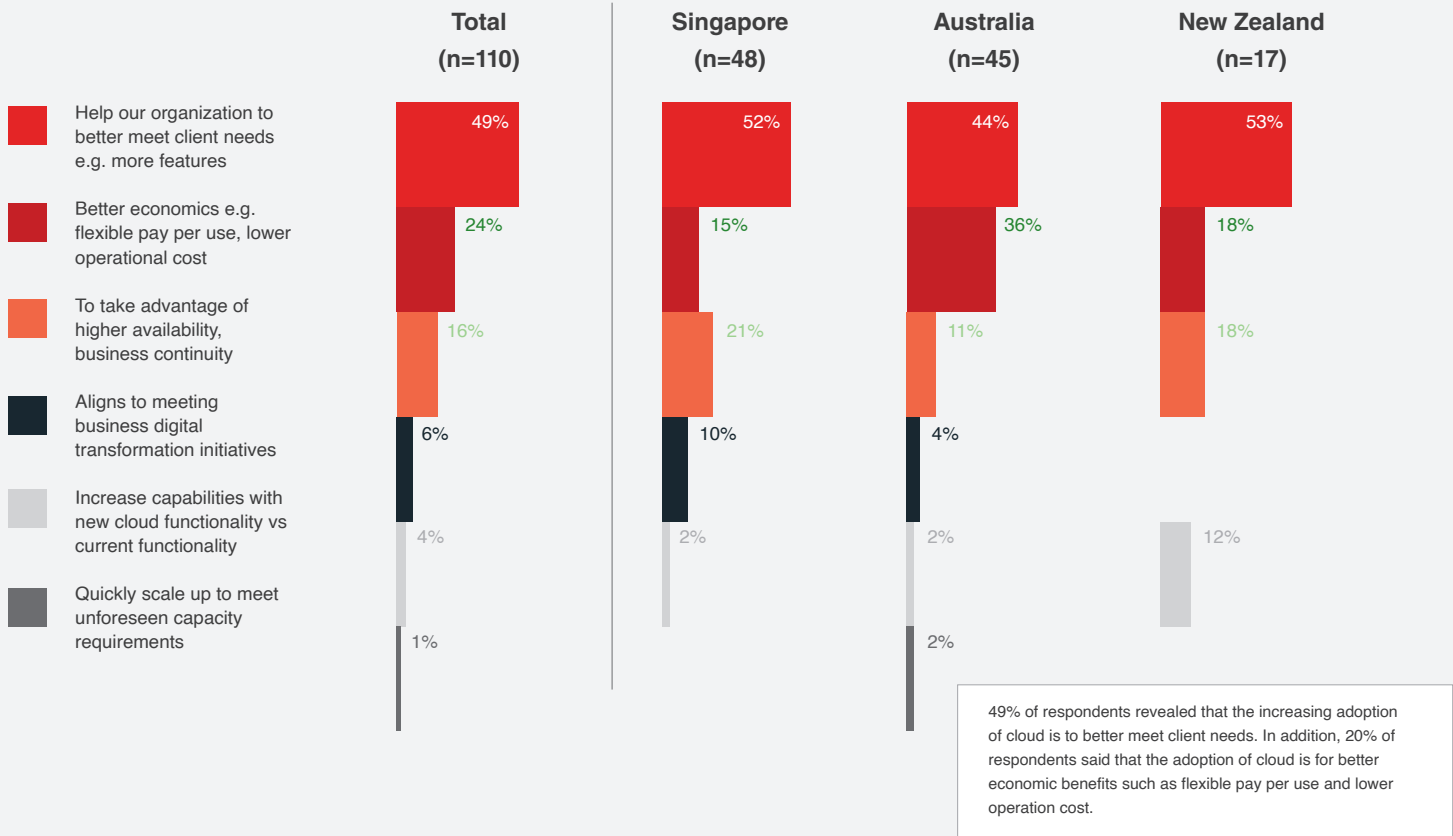
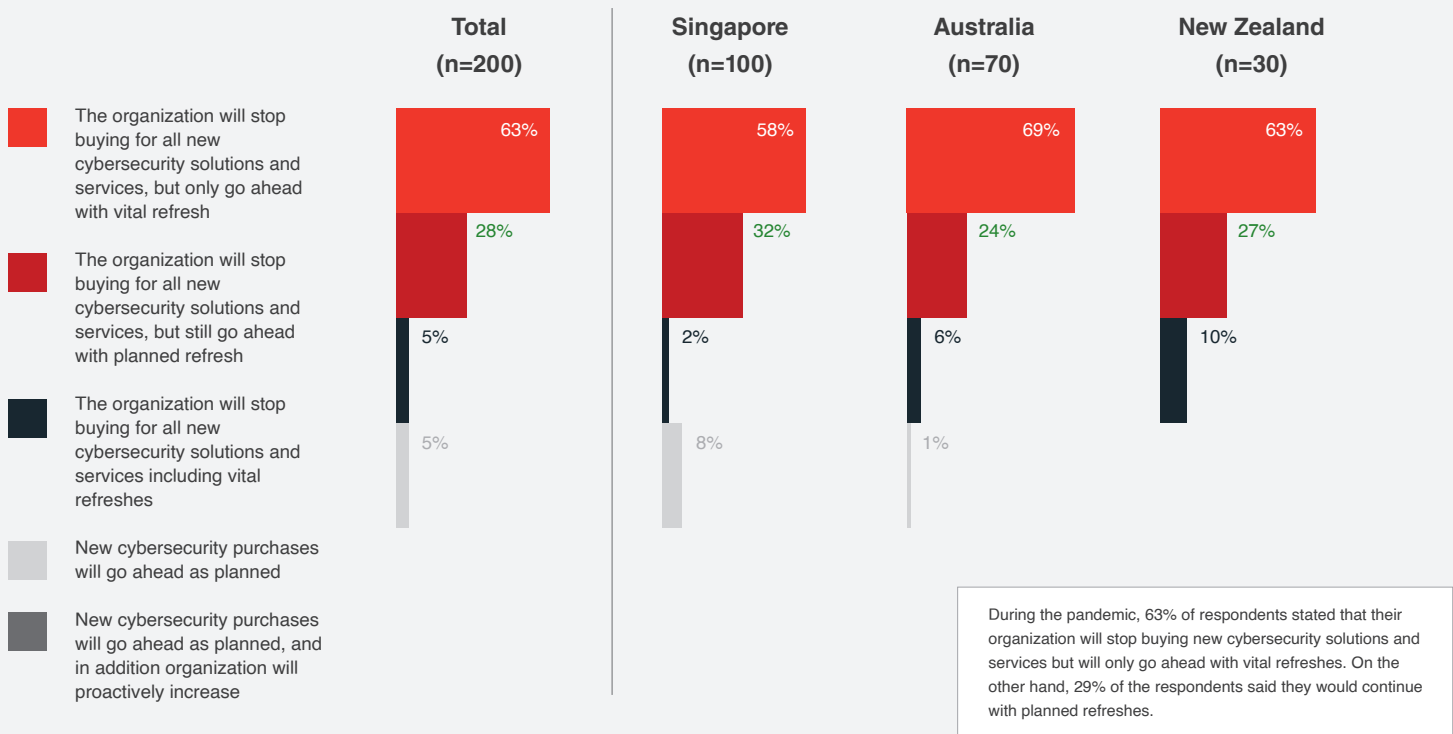


Figure 2.1: Acceleration to the cloud occurring now to better meet client needs



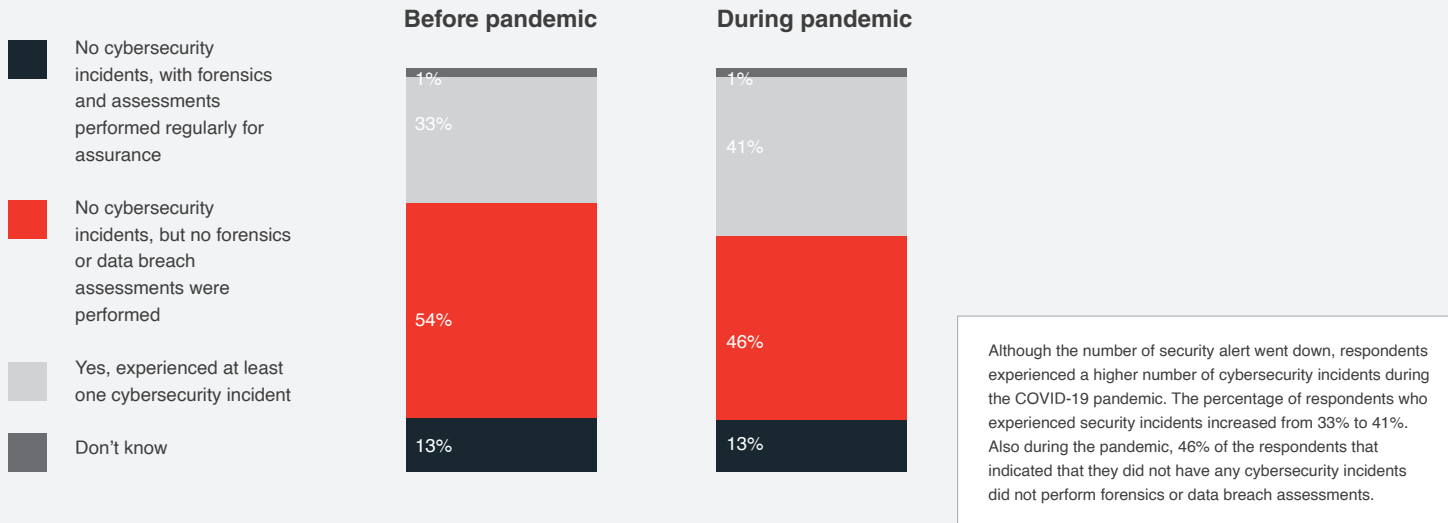
Data callout #3: 58% of enterprises in Singapore stated that they planned to stop buying new cybersecurity solutions and would only proceed with vital refreshes while 32% claimed that they would only proceed with planned refreshes

Figure 3: Leading to enterprises focusing only on vital refreshes and slowing down cybersecurity investment



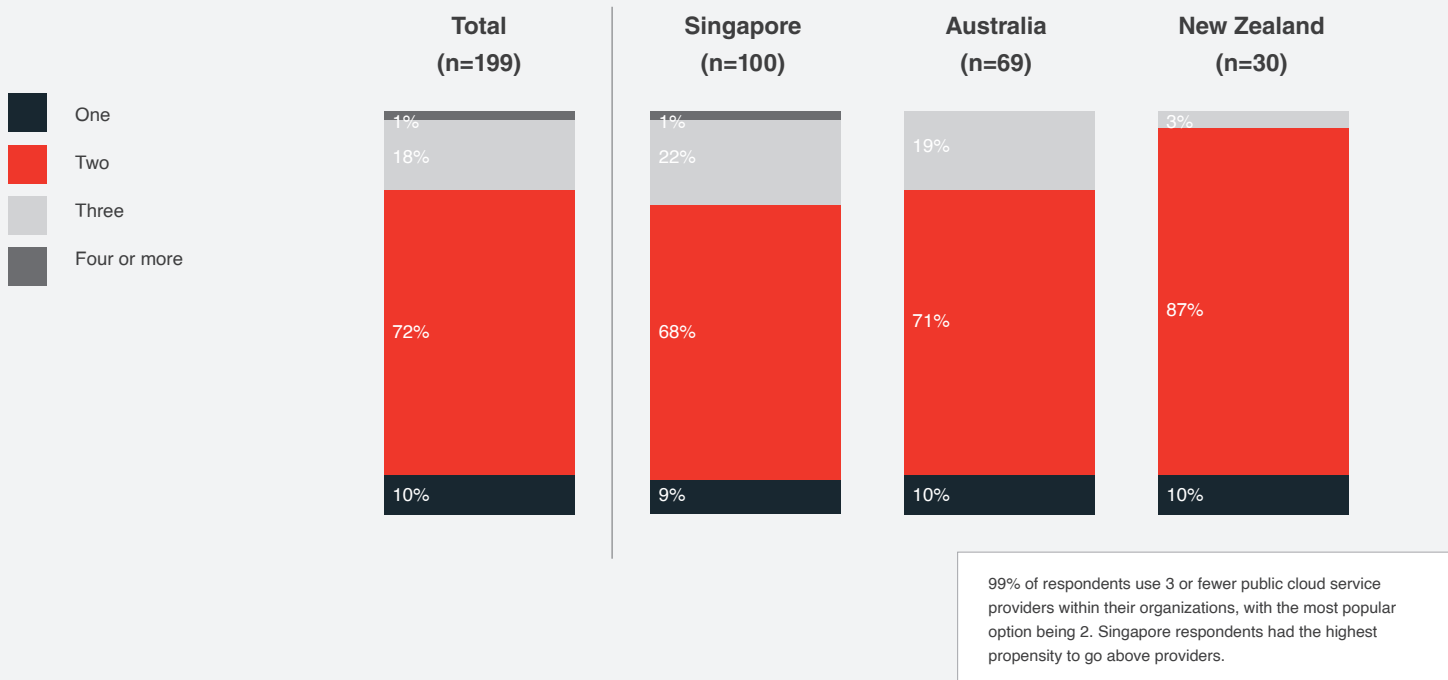
Data callout #4: On the other hand, respondents across all regions experienced a higher number of cybersecurity incidents during the pandemic. The percentage of respondents who experienced security incidents increased from 33% to 41%.

Figure 4: Enterprises more at risk today during the pandemic



Data callout #5: Multi-cloud ecosystems are the new reality, with Frost and Sullivan research revealing that 99% of respondents in Singapore use two or more public cloud service providers. Singapore respondents had the highest propensity of using over two providers, with 23% reporting the usage of three or more providers compared to the overall total of 19% who reported the same.

Figure 5: Multi-cloud is the new reality with 90% of enterprises using 2 or more cloud SPs



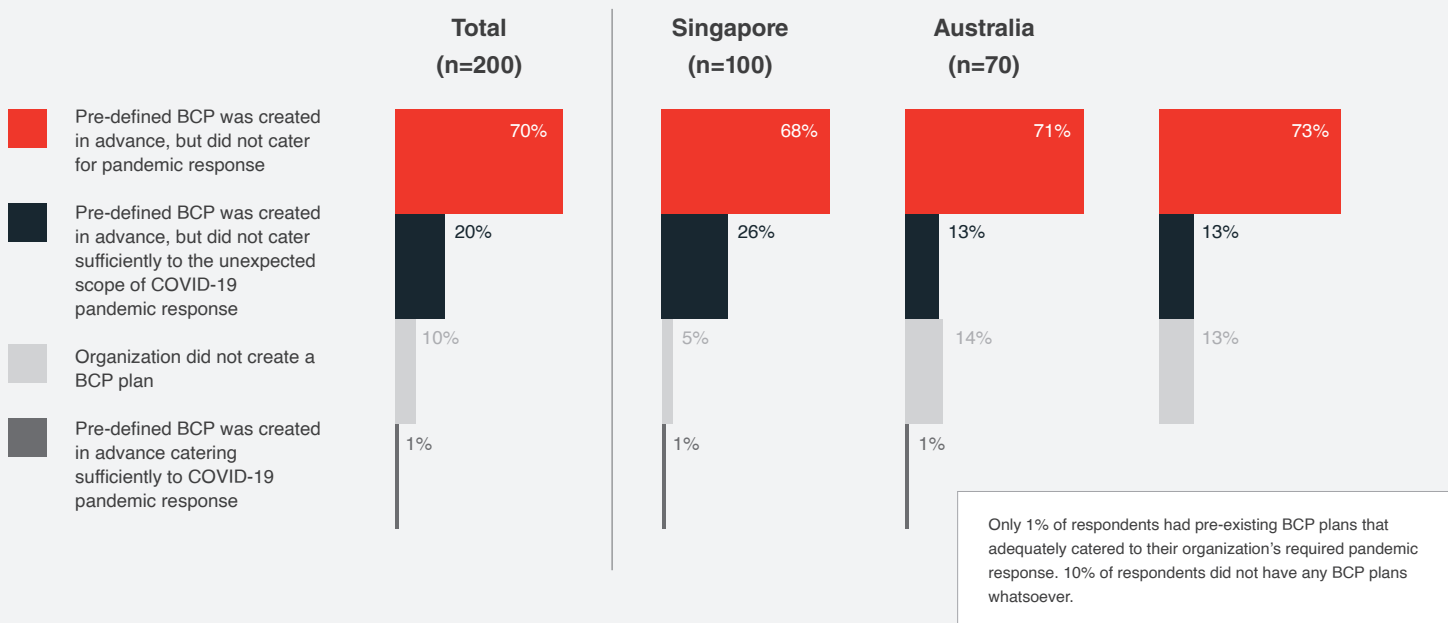
Data callout #6: In the midst of this overhaul, a majority of respondents amongst enterprises in Singapore indicated that they only had partial visibility of their cloud applications (50%) while others (27%) stated that they in fact had minimal visibility, both in terms of volume of secure access and activity visibility.

Figure 6: In spite of strong move to the cloud by enterprises, visibility of user access is poor



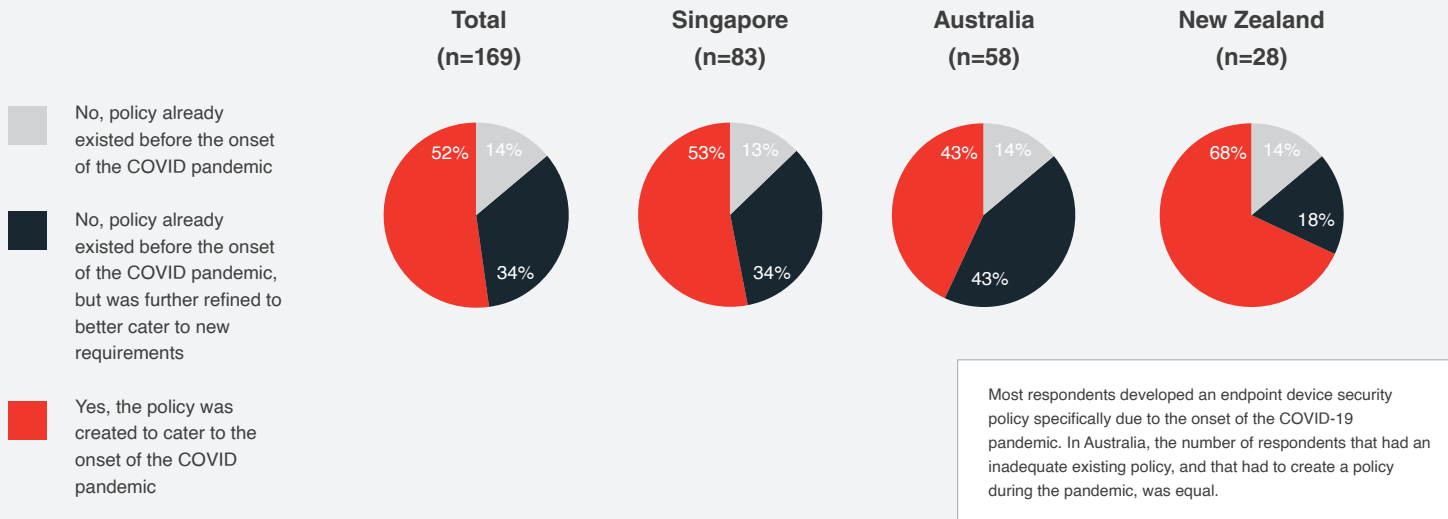
Data callout #7: Only 1% of respondents in Singapore attested to having pre-existing BCP plans that adequately catered to COVID-19, with 68% reporting that while they did have a predefined BCP in place, it was not designed to address the required pandemic response.

Figure 7: Enterprises were not prepared in their BCP for pandemic response



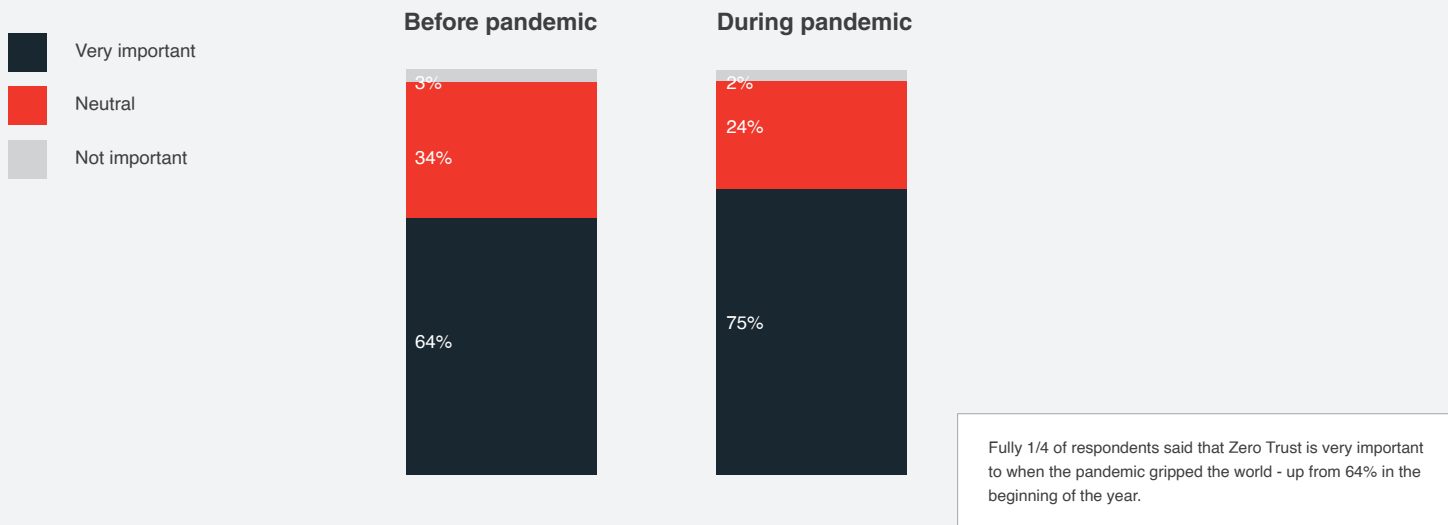
Data callout #8: In Singapore, 53% of enterprises affirmed that their endpoint device security policy was created specifically for the pandemic, while 34% stated that while they had existing policies, these had to be further refined to better suit new requirements.

Figure 8: As team shifted to WFH, policies had to be created to cater to the pandemic



Data callout #9: At the same time, the importance of zero trust frameworks increased across the board with 75% of all enterprises interviewed stating that this was very important during the pandemic, compared to the 64% who felt the same before the pandemic.

Figure 9: Importance of Zero Trust Approach - Total





About Ivanti

Employing over 1,700 people, Ivanti IT software is used by 78 of the Fortune 100. Enterprise IT departments use Ivanti to marry their ITSM, IT asset management, IT security, endpoint management, and supply chain capabilities. Ivanti's mission is clear—to help our customers succeed through the Power of Unified IT.

The Ivanti automation platform makes every IT connection smarter and more secure across devices, infrastructure and people. From PCs and mobile devices to virtual desktop infrastructure and the data center, Ivanti discovers, manages, secures and services IT assets from cloud to edge in the everywhere enterprise -- while delivering personalized employee experiences.

In the everywhere enterprise, corporate data flows freely across devices and servers, empowering workers to be productive wherever and however they work. Ivanti is headquartered in Salt Lake City, Utah and has offices all over the world.