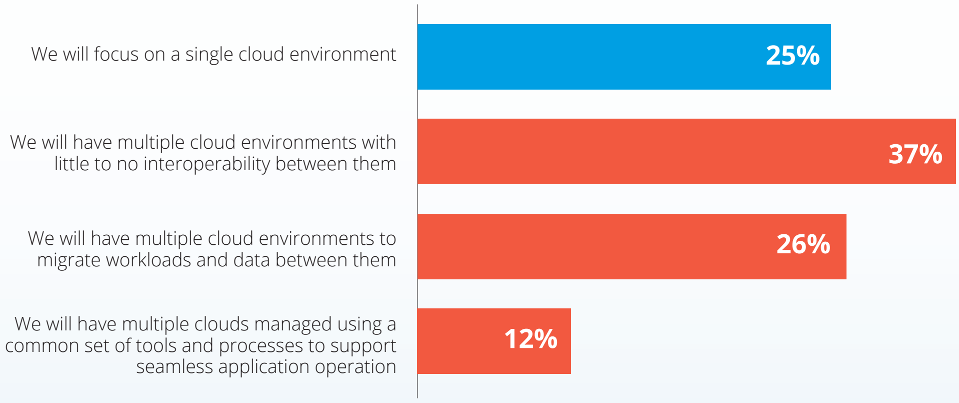
Securing a Multi-Cloud Software-Defined Enterprise

Q. How do you expect your organisation's cloud strategy to evolve over the next 2 years (through 2021-2022)?



Source: IDC's Worldwide Cloud Pulse Survey, December 2020

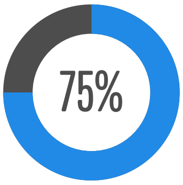
IDC believes that secure multi-cloud IT will be the most fundamental pillar of enterprise innovation and transformation.

Security considerations for an ever-expanding IT perimeter

The onset of the pandemic, along with the organisational desire to digitally transform, has resulted in a significantly accelerated shift to hybrid IT and multi-cloud environments. As organisations rely on technology to navigate the challenges of the pandemic, cloud technologies have not only emerged most central to organisations' survival but also become key to helping organisations along their business resilience and recovery path.

According to IDC's Worldwide Cloud Pulse Survey 2020, 75% of organisations are strongly motivated to have a multi-cloud strategy going forward. However, organisations are also aware of the increased security challenges created by a multi-cloud environment.

The increasing pervasiveness of multi-cloud environments across organisations has brought the importance of security and risk management to the forefront. It requires secure WAN access to different types of applications which are distributed across on-premises datacentres, infrastructure as a service (IaaS) clouds and software as a service (SaaS), and which encompass different security profiles and vulnerabilities. While SD-WAN brings together different access mediums to address the multi-cloud conundrum, organisations are increasingly looking to address the security vulnerabilities of an enterprise IT environment expanding rapidly. In the IDC COVID-19 Impact on IT Spending Survey 2020, organisations were asked about changes to technology budgets for the year and cloud security came out on top with most expecting at least an 11% increase in their cloud security budgets.



of organisations have a multi-cloud strategy going forward to help with business resilience and recovery.

SD-WAN integrations with third-party security services and other network services in a branch context have been pursued by enterprises, but they **are complex and difficult to execute.** These challenges are driving the need for an integrated security approach for today's hyper-connected, multi-cloud, and software-defined enterprise.

Top priority

When asked to identify features that are required in a next-generation SD-WAN platform, integrated security functions and services came out on top of the list, according to IDC's Worldwide Communications and SD-WAN Survey 2020.

The need for a trusted partner in SD-WAN solutions

The **integration of network, security, and management functions** represents an evolution of the SD-WAN market towards a broader software-defined branch, but this journey is incredibly challenging to execute. Responding to the evolving security threat has not been easy because of the following challenges:

Focus on Business Essentials	The COVID-19 pandemic forced many businesses to focus on enabling security technologies such as VPNs, firewalls, and email security.	**No Expertise Available**	The cybersecurity skills shortage continues. Organisations seek security tools that empower security analysts to be more efficient and effective.
Digital Transformation	New, hybrid, and cloud environments complicate security and require expansion of features and form factors.	**Evolving Needs**	Buyers require less complexity, and fewer but more actionable results. Noisy alerts are shunned in favour of automation, orchestration, and playbooks.

As a result, organisations should look for service providers to help them undertake this integrated security approach.

How to get started

As you revisit your security posture, here are some best practices to help you get started:

Consider security and SD-WAN as one. Evaluation, selection, and implementation of security technologies must factor in application-specific characteristics, deployment types, and the destination, as much as possible. Working with a service provider with an integrated SD-WAN, security design, and management approach will help organisations address their challenges efficiently.

Augment in-house security capabilities with a managed security provider. Cybersecurity skills are and will continue to be at a premium in the market. Organisations need to evaluate their in-house security expertise and augment it with managed services from preferred partners.

Select service providers with robust growth and partner ecosystem to access the latest technologies and platforms. An integrated security partner does not only address the current security challenges but also foresees future problems and proactively suggests relevant upgrades and security optimisation. Selecting service providers that are progressive and routinely involved in co-innovation exercises with security vendors and hyperscalers will bode well for long-term goals of securing the enterprise.

Message from Singtel

The Singtel SD-WAN solution simplifies multi-cloud environments with end-to-end visibility and granular control across all cloud environments. With integrated security and network functionality in a unified solution, enterprises can lower their risks and enforce application policies through a centralised management console, while reducing cost and complexity. Reach out to us to simplify your multi-cloud networking journey.

Contact us today.