AN INTERCLOUD WHITEPAPER

BALANCING FLEXIBILITY & SECURITY:
A GUIDE TO ACHIEVING MULTI-CLOUD SUCCESS

IDG

interCloud

The emergence of multi-cloud may be front of mind for leading CIOs, but it does require IT and business leaders to strike a fine line to balance flexibility and security.

Cloud is at the heart of the new technology revolution transforming business and public services. Public and private cloud revenues accounted for 48.5% of the total worldwide IT infrastructure spending in the second quarter of 2018, a rise from 43.5% a year ago, and these revenues will continue to rise, according to analyst group IDC.

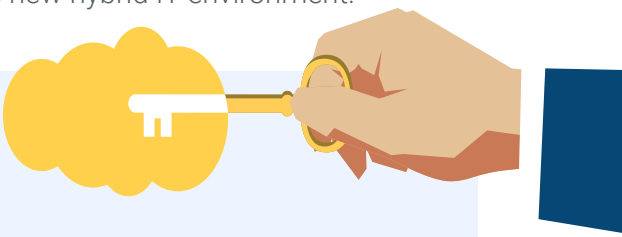
'Cloud, which once used to be an emerging sector of the IT infrastructure industry, is now the norm,' said Natalya Yezhkova, IDC research director, IT Infrastructure and Platforms, before adding that enterprises now need to 'not only decide on what cloud resources to use but, actually, how to manage multiple cloud resources.'

The spectacular growth in hardware spending highlighted by IDC is matched by that for cloud-based Software as a Service (SaaS), Infrastructure as a Service (IaaS) and Platform as a Service (PaaS), as public cloud use becomes deeply embedded in our everyday lives.

Analyst group Forrester says its data shows 'more than half (53%) of European businesses with over 1,000 employees now use a public cloud platform'.

However, most enterprise cloud users are increasingly running more than one type of cloud deployment (PaaS, IaaS, SaaS, private, hybrid, and public) and working with more than one major public cloud provider, in a bid to leverage the best features and services from an assortment of vendors. Indeed, IDC estimates that a staggering 90 percent of European businesses will make use of multiple cloud services by 2020.

This world of hybrid or multi-cloud deployments brings enormous benefits and significant new challenges and priorities. The reason is simple. There is a fundamental difference between deploying multiple cloud technologies and having the skills and processes in place to effectively manage this new hybrid IT environment.



Managing and securing the multi-cloud environment

Moving from multiple, relatively uncoordinated clouds, towards a more mature multi-cloud environment requires decision makers from enterprise IT, DevOps, and Line of Business (LOB) to thoroughly review the range of cloud solutions being used across the organisation, focussing on data integrity, security, confidentiality, compliance, business continuity and business risk.

For analyst group Forrester, this requires a rethink in enterprise security that is as fundamental as the change wrought on enterprise IT by cloud itself. The analyst is urging organisations to adopt a 'Zero Trust' architecture that abandons the concept of a trusted network inside a defined corporate perimeter, to focus on securing the data.

Traditional security models cannot cope with cloud and multi-cloud environments, says Forrester, which urges that a focus on perimeter defences and secure gateways be superseded by the creation of micro perimeters of control around sensitive data assets. This has the double benefit of allowing organisations to both deliver protection and gain visibility into how data is used across their complete ecosystem, the analyst says.

Whether or not organisations buy into Forrester's Zero Trust security model, those that are developing an effective, unified multi-cloud management strategy are realising they need to use the same management tools, processes and metrics to manage all their cloud resources, and rely on an appropriate connectivity solution to ensure business continuity and performance.

They are also increasingly seeking out technologies and services that help manage their relationships with multiple cloud suppliers and protect against the threats that exist on public networks.

Solutions can be found from cloud brokerage firms, from managed cloud security services providers and organisations such as InterCloud, whose carrier and data-centre neutral Platform offers enterprises a private network that while physically connected to all major cloud providers, is completely isolated from all public networks. This means it is much more resistant to everything from cyberattacks to service interruptions that are typically experienced by services running on the internet.

WHAT IS DRIVING MULTI-CLOUD ADOPTION?

The first step to managing multi-cloud adoption is to understand what is driving it. We have come a long way from the early days of cloud platforms when public cloud platforms in particular grew and gained publicity from their adoption by start-ups. Bright, young entrepreneurs with a clever idea, a browser, and a credit card could launch in the public cloud and grow a new business.

Enterprise deployment of public cloud services was, even a few years ago, of necessity, much more tentative and limited. New workloads, test and development, experiments and proof of concept (POC) trials and the conversion of large volumes of low-risk historical data might be handled in the cloud. Core business processes and data were, however, kept in on premises or co-located data centres.

Not anymore. Almost all enterprise CIOs operate in organisations that depend on running some applications and workloads in the public cloud, some on hosted or on-premises private clouds, some in old school co-location facilities, with some still run on dedicated, non-cloud systems in their own data centres.

There are few organisations anywhere that don't deploy, somewhere, SaaS delivered productivity suites or tools, sales and customer relationship management systems or human resources systems, where staff use consumer grade file sharing and collaboration tools for work related activity.

The chances of an organisation remaining in business that has no virtualised systems deployed in its on-premises data centres, are slim. So too are the prospects of organisations that don't have external managed service providers either to deliver a service such as disaster recovery, or to maintain dedicated capacity.

If agility and competitiveness are the key drivers for the proliferation of multiple cloud services within organisations, they have manifested themselves in ways that challenge traditional technology management strategies. Enterprise operations teams today have to deal with:

- The proliferation of roles making technology purchasing decisions, including line of business leaders, developers, DevOps, marketing and customer experience teams.

- The emergence of best-in-class, market leading SaaS companies, such as Salesforce.com and Workday that are entering the enterprise.

- The realisation that different clouds and different technology stacks are best suited to different tasks.

- The rapid benefits of deploying desktop virtualisation and client-based SaaS solutions such as Office365.

- The enduring requirement for private cloud to run critical workloads, systems that support significant revenue, that provide secure control of enterprise critical data, and meet compliance and risk mitigation requirements.

- The spread of industry and community-specific clouds.

All these drivers create challenges for those who have to deploy, manage, automate and orchestrate the resulting hybrid, multiple cloud environment.

> **"Less than 10% of European organisations are ready for real multi-cloud."**
>
> ***– IDC Survey, May 2018***

IS MULTI-CLOUD ENVIRONMENT BY ACCIDENT OR DESIGN?

The key question for CIOs and the operations teams they lead is whether their infrastructure is 'hybrid by design' or 'hybrid by accident'.

Forester analyst Chris Gardner says, 'Let's be frank: you are probably doing hybrid by accident – just about everybody is.
'Gardner defines hybrid by accident as:

- Integrating public cloud with on-premises tech without standardising on a common infrastructure-as-code practice
- Shadow IT cloud "experiments" that suddenly become production (often to the chagrin of the infrastructure team)
- Outdated governance practices that slow everybody down

Hybrid by design, says Gardner, 'is trickier to execute. Most don't get it right out of the box, but it can pay off huge dividends.' Hybrid by design, he says, is:

- Realising that infrastructure as code is a fundamentally different beast that requires different skill sets, policies, and practices to optimise
- Understanding that your I&O (Infrastructure & Operations) pros are now essentially developers, and you need to execute with a developer's mindset during every step of the delivery cycle
- Recognising that you are not going to get anywhere without automation, particularly configuration management and continuous delivery release automation tools
- Coming to grips with the fact that security without automation is a fool's errand
- Understanding that the legacy players are evolving right alongside you

For IDC's Giorgio Nebuloni, research director, European multi-cloud Infrastructure, hybrid by design is genuine multi-cloud. 'Hybrid cloud consisted mostly of ad hoc bridges between different cloud environments,' says Nebuloni, whereas, 'multi-cloud is about IT decision makers … measuring the costs and ensuring everything runs to perfection.

'It means moving from a multitude of unmanaged, potentially cost-inefficient cloud services to a programmatic setup of resources and a redesign of the internal processes.'

Orchestrating multiple clouds means organisations have to deal with technical complexity and ensure they have the right people and skills to manage their new infrastructure. They have to develop new business processes, new ways of managing costs and contracts and all the while, ensure data integrity, compliance and security are not compromised.

An IDC survey in May 2018, which looked at a range of business and technology factors, found less than 10% of European organisations are ready for real multi-cloud. The majority, some 80%, are battling through a transition process from hybrid cloud environments, while 10%, have little multi-cloud experience or ambition.

If IDC is sounding a wakeup call, Jerome Dilouya, CEO of InterCloud the European leader in Cloud connectivity as a Service is keen to offer some perspective as well as some solutions. 'Organisations have found themselves with multiple cloud environments for good practical and commercial reasons.

'Cloud meant IT departments could spin up extra compute power to meet peaks in workloads, DevOps teams could access resources more quickly than internal IT could provision them, line of business leaders were attracted to best of breed solutions, though sometimes without regard for the systems management, data integrity, security and compliance implications.

'Cloud has proved its worth and business technology leaders are working out how to get the maximum benefit. However, a successful multi-cloud strategy cannot be implemented without an appropriate & secure connectivity.

WHAT'S THE ROLE OF SECURITY?

Security is a key part of the evolution from an unmanaged sprawl of ad hoc cloud services towards a genuine multi-cloud environment, and every step of the journey should be about reducing overall risk and maintaining compliance.

The first steps might be as simple as using automated tools to discover sanctioned and unsanctioned cloud applications that are in use. This does not end with an audit of cloud tools commissioned by line of business leaders, marketing and DevOps teams. It should include consumer-based apps such as Dropbox, and it should be followed by the application of security controls. Cloud security gateway solutions provide discovery and monitoring of cloud apps, as well as encryption and data loss prevention.
Organisations should also start encrypting by default cloud data at rest as well as in flight. Data encryption is referenced in the European Union's General Data Protection Regulation (GDPR) legislation as a key technical and organisational measure for organisations to secure personal data, and you should already be encrypting data used in your on-premise applications.

The deployment of single sign on (SSO) technologies though essential for your infrastructure optimisation and digital transformation efforts, also helps you limit, control and monitor who can commission and have access to cloud workloads. As such it represents another significant step to creating a genuine multi-cloud environment.

Your deployment of Web Application Firewalls (WAF) and Distributed Denial of Service (DDoS) protection systems must be optimised for the clouds your organisation deploys and, as Application Protocol Interfaces (APIs) and Container technology becomes more prevalent, the deployment of API gateways can enhance security.

Maturity matters in a multi-cloud world

Despite the high level of cloud adoption, most organisations are facing challenges involving people and organisational structures, operational processes, IT culture, and technology adoption, and are still working to improve their cloud strategies. To help business technology professionals on this journey, IDC defines five levels of cloud maturity:

- **Ad hoc:** These organisations are beginning the process of increasing awareness of cloud technology options and are turning to cloud because of the immediacy of their need, often in an unauthorised manner.

- **Opportunistic:** These organisations are experimenting with short-term improvements in access to IT resources through the cloud. They usually consider cloud for new solutions or isolated computing environments.

- **Repeatable:** At this level, organisations are enabling more agile access to IT resources through standardisation and implementation of best practices. They rely on self-service portals to access cloud services.

- **Managed:** These organisations are implementing a consistent, enterprise wide best practices approach to cloud and are orchestrating service delivery across an integrated set of resources.

- **Optimised:** These organisations are delivering innovative IT-enabled products and services from internal and external cloud providers and driving business innovation through transparent access to IT capacity, based on the value to the business and transparent cost measures.

‘While customers implement multi-cloud and hybrid cloud strategies to improve their organisation’s agility, we handle the hidden complexity for them,’ says InterCloud’s CEO.

A number of vendors are now offering cloud workload security (CWS) solutions that deliver an automated and centralised way of securing enterprise cloud workloads.

Organisations are also looking at ways to further protect their data and the cloud services they use from the threats found on public networks.
InterCloud, for example, provides an application-centric platform that combines cloud workload security technologies with secure, private access to any cloud provider globally. Resources, whether they are in the public or private cloud, in hosted data centres, co-located or in your legacy, on premises apps are connected through the platform, where they are optimised and secured.
InterCloud’s primary cloud partners include AWS, Alibaba Cloud, Google Cloud, IBM Cloud, Microsoft Azure, Oracle Cloud and SaaS giants such as Salesforce.com, while customers include blue chip organisations such as SNCF, Société Générale and Schneider Electric.

‘While customers implement multi-cloud and hybrid cloud strategies to improve their organisation’s agility, we handle the hidden complexity for them,’ says InterCloud’s CEO.

‘We interconnect all their cloud resources, guaranteeing fast, reliable and compliant access to all applications, backed by strong SLAs. In addition, we offer application-level features such as security and application performance management, while our platform model allows enterprises to integrate cloud connectivity into a continuous integration and deployment cycle.’

These sorts of services can make a significant difference to organisations as they mature their cloud deployments and develop well managed multi-cloud solutions that balance agility, speed, cost, compliance and security to deliver maximum value for customers, staff and shareholders.

Organisations that want to maximise value for their customers and shareholders, while minimising the risks of living in a multi-cloud environment need to make some fundamental changes. None of them can be achieved overnight, but CEOs, CIOs, line of business and business technology leaders have to set the line of travel and drive towards their ultimate goal.

- Identify and contain security threats. Map and meet compliance requirements and create common security policies across the organisation for all users, data, and applications.

- Simplify global connectivity between data centres and public clouds to reduce maintenance and operations costs and make management easier.

- Deploy common, integrated performance monitoring and management tools across cloud-native, on premises and legacy applications to enable cost optimisation across multiple clouds.

- Avoid cloud vendor lock-in by planning for a cloud exit strategy before signing a contract. Also review service level agreements to understand the key metrics across networks, applications, and infrastructure.

© INTERCLOUD IN PARTNERSHIP WITH IDG (2018)