HOW BEST SHOULD REGIONAL CIOs APPROACH THE TRANSITION TO THE CLOUD AND THE ADOPTION OF MODELS SUCH AS HYBRID CLOUD?

In May 2016 Red Hat's Alessandro Perilli, GM Open Hybrid Cloud, discussed in his article on our website how an open hybrid cloud consists of five core pillars: 'The first pillar is the capability to empower IT organisations with the right tools to address the demand of the line of business in the cloud era. The second pillar is the capability to embrace and support the IT diversity in an enterprise environment, irrespective of the selected IT strategy for cloud computing.'

'The third pillar is the capability to adapt to your IT maturity level, providing more sophisticated cloud capabilities only when the IT organisation is ready to deploy them. The fourth pillar is the capability to extend easily, supporting a broad set of hardware and enterprise management tools, thanks to a modular architecture and a rich ecosystem of partners. The fifth and final pillar is a strong foundation on open source technologies, which provide the innovation necessary to transform your IT,' he said.

IDC released predictions for this year and beyond at the end of 2015, noting that the big drivers for increased implementation of hybrid clouds are IT's continuing quest for optimised infrastructure, and the ability of solution builders to source application and infrastructure components from multiple providers to construct a hybrid cloud-based solution.

Furthermore, IDC predicts that by the end of 2018, 40 % of IT spend across hardware, software and services will be for cloud oriented technologies, and by 2020, 45 % - 50 % of all spend will be for cloud delivered models.

Rolf Haas

Enterprise Tech Specialist, Intel Security

While the popularity of cloud grows, it's clear to anyone in the industry that organisations are not simply moving all their applications and data into the public cloud. The reality is more complex and is a hybrid of public and private cloud (and existing in-house infrastructure and systems).

The rate of adoption of hybrid cloud varies widely depending on whose statistics you choose to believe. One study by IDG Research claims 83 % of CIOs currently use hybrid cloud or plan to do so in the future. Analyst Gartner, however, estimates between 10-15 % of enterprises have adopted a hybrid strategy. Gartner also predicts hybrid cloud will hit mainstream adoption within the next two to five years.

The benefits of hybrid cloud are clear for enterprises. It gives organisations the flexibility to use on-premise (or outsourced or off-premise but fully-owned) private cloud where appropriate or switch workloads into the public cloud and scale according to demand (or do both at the same time). Cloud provisioning can be done at the click of a mouse and investment only needs to commit to weekly or monthly rental.

As ever, the big issue for this new era of hybrid cloud is security. A survey by analyst 451 Research reveals that 59 % of senior IT executives believe maintaining consistent access security and authorization controls across a hybrid environment is a significant challenge.

At a more strategic level many of the concerns among organisations relate to the privacy issues around putting company data in the

public cloud. These fears centre on who might have the authority to access the company data hosted by the public cloud provider.

Clearly this is an issue that has to be overcome if organisations are able to reap the full flexibility and cost benefits of a hybrid cloud environment that allows them to push applications and data into the public cloud in line with business needs.

That is where hybrid security comes in. The key to this is for companies to be able to seamlessly push and enforce their own security policies from on-premise proxy infrastructure to a public infrastructure. For the enterprise this provides the ability, if required, to encrypt corporate data that sits in a public cloud service and offers complete protection for every endpoint.

Sachin Bhardwaj

Director Marketing & Business Development, eHosting DataFort

Before migrating to the cloud, CIOs need to assess the company's long-term business and infrastructure needs, establish realistic goals and priorities, set deadlines and consult with finance directors on IT budgets. This is important because reversing IT systems is time-consuming and expensive. Apart from having an understanding of what resources are available for implementation and maintenance,

CIOs should, with proper planning and strategy, keep the complexity and cost to a minimum. They need to determine whether the transition will be managed in-house or outsourced to a third party vendor.

CIOs need to evaluate both private and public cloud options and see which platform best meets their business requirements. Before moving information to the cloud, they need to conduct an internal review with business heads to identify which data can be moved to the cloud. Full cloud integration may cause regulatory compliance issues as certain data must be secured internally. Enterprises must also be cautious of where they store different types of data.

CIOs need to ensure that their organizations have effective data recovery and backup management tools in place in case of any loss during data synchronization. If the organization has planned to outsource the migration, it is important to know if the cloud services provider has a robust data backup strategy and recovery procedures.

While choosing a cloud vendor, it is important for CIOs to review and evaluate their security standards, policies and governance models to ensure that their organizations' data is safe, secure and protected at all times. They must be aware of procedural and policy differences between their organization and external companies and software vendors. They need to understand where the data will be stored and comply with the legal requirements in their own country as well as the country of the cloud services provider. Organizations can also consider a hybrid solution to secure critical data.

We recommend partnering with a cloud services provider (CSP) who offers service level agreements (SLAs), 24/7/365 support and follows security standards, processes and procedures to get the most value from a hybrid cloud model. Local CSPs could provide enterprises with a local data center and 24/7 bilingual local support.