GOING PUBLIC

Public cloud continues to progress leaps and bounds, with all avenues pointing to mass adoption over the coming five years. Whilst the likes of Amazon, Microsoft and Google continue to dominate the global market, regional offerings continue to gain momentum in the Middle East. But can Middle East CIOs overcome security concerns? *CNME* investigates.

No technology has bulldozed its way onto the global scene and promised to revolutionise enterprise IT as much as cloud computing.

Every CIO in the world has thought about it in one way or another, with many large organisations dabbling in the technology with regards to private or hybrid models, often with applications like email hosted on the cloud, whilst the more critical data remains in-house.

Public cloud, however, is a completely different kettle of fish. Whilst the cost and efficiency benefits are clear, issues surrounding security and data privacy have largely held back adoption to date.

Despite this, Gartner has predicted that 30 percent of IT companies from the Global 1000 organisations will integrate, aggregate and customise two or more cloud services for internal and external users by 2014, up from the current five percent.

Closer to home, Saudi Arabia and the UAE are leading the trend with the adoption anticipated to grow up to 43 percent in the Saudi market and 40 percent in the UAE in 2013.

According to Rajesh Abraham, Director, Product Development, eHDF, a local cloud-service provider, the trust concerns around public cloud can be attributed to the lack of understanding around the technology.

However, he believes all these concerns can be addressed by implementing proper security controls and mechanisms.

Jatin Sahni, VP, Large Enterprise and Business Solutions, du, which also offers cloud services, says the uptake of the technology has been led by SMEs, followed by mid-marked and large enterprise.

"Large enterprises are critically looking at public cloud computing services for services such as test labs, migration tests, and proof-of-concepts, as well as their non-critical IT application requirements," he says. "While organisations such as IDC are looking at an 18 percentage CAGR growth of public cloud services, we are seeing a rapid increase in the uptake of cloud services from SMEs and mid-market organisations."

Leading the offerings from the global players in the Middle East is Microsoft, which naturally claims that public cloud services will be the most popular cloud computing model for the foreseeable future.

Over 81 percent of its enterprise customers in the Gulf region have already implemented a project on the cloud, which it touts as reducing the costs of purchasing and maintaining hardware.

"In a nutshell, we have seen definite interest and willingness to virtualise from our customers across the region," says Goksel Topbas, Server and Tools Business Group Lead, Microsoft Gulf.

They do sometimes receive security and privacy questions with regards to data protection, Topbas admits, adding that they understand that unless they are responsive to customers' and regulators' questions about data protection in public clouds, they will not earn the necessary trust.

Indeed, these concerns are more prevalent in the government and financial services sectors, where

81%
of Microsoft's enterprise customers in the Gulf have already implemented a project on the cloud.

> "While organisations such as IDC are looking at an 18 percentage CAGR growth of public cloud services, we are seeing a rapid increase in the uptake of cloud services from SMEs and mid-market organisations."

Jatin Sahni, VP, Large Enterprise and Business Solutions, du

“They prefer having their data in-house or at a third-party data centre located within the same country where they have easy accessibility to their data. Keeping data locally would also make it easy to conduct things like periodic audits. With cyber-crime on the rise, it is probably good to keep the data within the region as it allows the enterprises to remain in control of it.”

Rajesh Abraham, Director, Product Development, eHDF

The MENA market for public-cloud services is predicted to grow this year by

15.3%

CIOs feel pressured to stay in full control of their organisation’s data in order to adhere to the various regulatory requirements.

“They prefer having their data in-house or at a third-party data centre located within the same country where they have easy accessibility to their data,” Abraham says. “Keeping data locally would also make it easy to conduct things like periodic audits.

“With cyber-crime on the rise, it is probably good to keep the data within the region as it allows the enterprises to remain in control of it.”

Currently, key government agencies are working to address these concerns, but no specific laws are in place at the moment.

Generic compliances such as PCI, SAS70, ISO and HIPPA provide an umbrella assurance for customers, but these standards are international.

“Even if public-cloud providers are complying with security and operational standards, they are bound by national security laws from where they operate, as well as the laws that apply to where they are incorporated.”

“The key is the hosting of localised in-country instances of cloud to assure customers of data privacy and concerns relating to foreign governments getting access to their data,” Sahni says. “Offline capability remains a challenge, however, and technologies are fast-changing to remove this barrier as well.”

Much of the problem to date has been confusion around the relevant laws and standards, especially when different locations are involved in the process.

“Even if public-cloud providers are complying with security and operational standards, they are bound by national security laws from where they operate, as well as the laws that apply to where they are incorporated, which can sometimes override corporate security policies,” says Pappu R. Rao, Technical Support Services Director, GBM.

As more data moves to the cloud, this uncertainty about legal and regulatory obligations related to that data could limit the growth of cloud computing, Topbas confirms.

He believes the technology industry has an important responsibility to pursue initiatives that improve the privacy and security of cloud computing.

The private sector, however, cannot build confidence in the cloud alone. A cooperative effort from all cloud stakeholders, including governments, is necessary.

“Elements of a strong legal and regulatory framework for cloud computing already exist, but many aspects of this framework were designed for earlier technologies and leave important gaps in protection,” Topbas says. “Ultimately, the technology industry, users of cloud services, and governments must agree on certain core cloud privacy practices that span across industries and are harmonised across borders.

20% of all cloud services will be consumed via internal or external cloud service brokerages, rather than directly, by 2015.

"Elements of a strong legal and regulatory framework for cloud computing already exist, but many aspects of this framework were designed for earlier technologies and leave important gaps in protection. Ultimately, the technology industry, users of cloud services, and governments must agree on certain core cloud privacy practices that span across industries and are harmonised across borders."

Goksel Topbas, Server and Tools Business Group Lead, Microsoft Gulf

"Such agreements will provide greater clarity and predictability for individuals, customers, and cloud providers."

Pulling the anchor

However, despite these anchors currently holding back adoption, the fact remains that the gradual transition is still taking place.

Rao attributes a lack of choice for Middle East CIOs as further contributing to the slow uptake, but with more providers looking to launch public-cloud offerings which allow data to be kept within the region, regional adoption is likely to increase considerably.

Whilst eHDF and Injazat look to take a lead in this space, the UAE's two telcos, Etisalat and du, already have an end-to-end portfolio of cloud services covering various managed services, complimented by relevant security solutions. Both telcos look to further add to these offerings, which are hosted at local data centres backed by leading certifications and SLAs.

"With availability of quality cost-effective broadband, credible players offering secure, reliable products backed by SLAs, concerns and barriers are being peeled away one by one."

Topbas calls the technology a "complete game changer" and believes it is only a matter of time before the hype translates in increased uptake of services across the region.

Gartner forecasts the market for public-cloud services will reach $378.5 million in the Middle East and North Africa this year, a growth of 15.3 percent. And whilst IDC's projection that spending on public IT cloud services will reach $47.4 billion in 2013, and $107 billion in 2017, is a global figure, the growth is expected to be suitably reflected in the Middle East market.

Furthermore, according to another report by Gartner, by 2015, at least 20 percent of all cloud services will be consumed via internal or external cloud service brokerages, rather than directly, up from less than 5 percent today globally.

"With availability of quality cost-effective broadband, credible players offering secure and reliable products backed by SLAs, concerns and barriers are being peeled away one by one," Sahni says.

"Providers now offer a greater level of control of the cloud instance through informative portals and alerts, security certifications, and back-to-back SLAs to assuage some of the key concerns of customers around cloud. The situation can further improve in future"

As the public cloud continues to demonstrate its business benefits, it has been adopted in various ways across the region and globally, Topbas adds.

"We foresee this trend of virtualisation continuing to increase — according to recent research, over 70 percent of CIOs will embrace a cloud-first strategy in 2016." ■