TRUST ISSUES

Storing data in the public cloud can be both convenient and cost-effective. However, shared access to stored information can be a nerve-wracking prospect for some users. Vendors can do some things to ensure security – authentication codes and log-ins, for example – but is data stored on the public cloud ever truly safe? CNME investigates the benefits and pitfalls to storing data on the public cloud.

With a large number of Middle Eastern businesses treading carefully in terms of public cloud adoption, there remains a degree of mystery and mistrust around the concept. Its financial benefits are clear, and in the age of business/IT alignment this is one of several key drivers behind their adoption. They are able to turn capital expenses into operational expenses, in a pay as you go model, saving an organisation from building their own entire data centre. Greater economies of scale is another key bonus; private clouds struggle to compete with the likes of Google and Amazon in terms of price.

There are also a variety of practical benefits, including improved elasticity. While organisations could in theory find a way to consume all of their own computing power on their private cloud, the same happening on the public cloud is unlikely. Nonetheless, security concerns are never far from the minds of IT leaders. The physical location of servers, and issues surrounding data ownership, as well as entrusting data and applications to a third party is too much for some. For a large number of organisations in the Middle East, it will take time and an evolution in the technology before paranoia surrounding the issue dissipates.

Cherif Sleiman, General Manager, Middle East, Infoblox, believes the underlying risk associated with public cloud means a worst case scenario qualifies it is a risky option for IT leaders. "The common saying in business is that the value of an organisation lies in its assets and its people," he says. "In today's information age, an organisation's data is absolutely its most important asset, making data loss the biggest risk posed by the public cloud. If the data is breached, depending on the sector and the nature of business, it could be catastrophic for the organisation."

In the eyes of a number of IT leaders, there remain a number of unanswered questions surrounding public cloud. Security issues stay top of that list, while reliability, availability and regulatory compliance issues are subsequent headaches.

> Non mission-critical data and applications that do not require highly specialised and customised IT infrastructure would benefit from using the public cloud. Examples of data which can be safely stored in the public cloud include shared documents and files, webmail and CRM applications."

Rajesh Abraham, Director Product Development, eHosting DataFort

> In today's information age, an organisation's data is absolutely its most important asset, making data loss the biggest risk posed by the public cloud. If the data is breached, depending on the sector and the nature of business, it could be catastrophic for the organisation."

Cherif Sleiman, General Manager, Middle East, Infoblox

The issue of legacy technologies that are not yet fully adapted to the needs of public cloud is a niggling threat that could be off-putting for those looking to adopt. "When it comes to security, most public cloud environments are based on inconsistent network architectures common in traditional data centres and still rely on legacy security technologies – such as stateful inspection and port-based firewalls – that aren't capable of securing public cloud or hosted VDCs against sophisticated cyber threats," says Saeed Agha, General Manager, Middle East, Palo Alto Networks. "Enterprises are keen to take advantage of the agility, scalability and cost benefits of cloud-based virtual data centers (VDCs) by building their own private cloud, purchasing public cloud services from providers, or adopting a hybrid cloud approach. Most enterprises are ultimately aiming for the portability of both the application and security policies, regardless of where the application is deployed."

A move towards a hybrid model could be the answer for allaying insecurities surrounding public cloud. It is also key to have a clearly defined policy as to what types of data and applications

ENJOY SAFER TECHNOLOGY™

SECURE DATA
ENDLESS POSSIBILITIES

Enjoy Safer Technology Protected by ESET

Our line of solutions for business ensure that all your vital IT infrastructure that runs your business is protected. From servers to the last smartphone out on business, you can relax and enjoy your safer technology, looked after by ESET.

www.eset.com/me I Info@esetme.com I Tel +97143754052 I Fax +97144290967 I Office 305, Building 2, Dubai Internet City

> Most public cloud environments are based on inconsistent network architectures common in traditional data centres and still rely on legacy security technologies that aren't capable of securing public cloud or hosted VDCs against sophisticated cyber threats."
>
> Saeed Agha, General Manager, Middle East, Palo Alto Networks

should be stored in what environment. Rajesh Abraham, Director Product Development, eHosting DataFort, believes that this differentiation is key. "Non mission-critical data and applications that do not require highly specialised and customised IT infrastructure would benefit from using the public cloud," he says. "Examples of data which can be safely stored in the public cloud include shared documents and files, webmail and CRM applications. Industries with highly sensitive & confidential data, including hospitals, government, financial institutions, and police departments must be vigilant when storing critical information on the public cloud. For such organisations a hosted private cloud is more suitable."

There are a number of reasons why a lack of trust towards the public cloud could be unjustified. Cloud firms seek to hire the best available security professionals, and attempt to harden their defences through numerous varied hacking attempts and investments in the latest technology. With most organisations not specialising in data security, the risk of breach can increase. A prevalent feeling in the industry seems to be that if data and applications are stored on the internal network then they must be secure. Whether or not that is actually the case, a number of organisations still need convincing as to the safety of public cloud.

Sleiman touches on the desire to retain IT within an organisation's physical parameters as a concern in private cloud adoption. "If you really think about it, cloud computing is not a new concept," he says. "The fact is that people are starting to see readily the proposed value of the public cloud, SaaS and IaaS models. And there is always apprehension that when something looks too good to be true, there's the possibility that it is. Traditionally, IT teams have always wanted things to be within their own four walls but the organisation has fundamentally changed. Today, work is no longer a place you go to but rather a thing you do. So as we develop new ways to consume IT we have to also look at new ways to deliver IT."

A key step for any organisation in ensuring the integrity of data stored in the public cloud is by establishing thorough and precise Service Level Agreements. This is an important part of the process in terms of ensuring any vendor is holding up their end of the bargain in all respects, mainly that they have requisite hardware and software to protect data. SLAs will also allow end-users to define exactly what they want from their public cloud.

Agha highlights the allure that is drawing organisations to the cloud, but is equally aware of the need to ensure security appliances can cope with these new demands leveraged by SLAs. "As you evolve your data centre towards a cloud-based architecture, you begin orchestrating the automated tasks for provisioning workloads (compute, storage, network)," he says. "Unfortunately, securing these workloads with today's existing network security appliances is a manual, time-consuming process. Security teams simply cannot keep up with how quickly these workloads are being provisioned by the virtual infrastructure teams."

Sleiman is clear on the most direct way that organisations can protect their data. "The best method of protection for data stored on the public cloud is encryption," he says. "Of course this has to be for data that is in transit as well. The fact is that once you trust it to a public cloud provider, you have no control over it and you cannot be aware of what backdoors are available to attackers. But if you ensure that data is transmitted in an encrypted format, this no longer remains a concern. If a breach were to occur and data was lost, it would be irrelevant as with encryption, the data is unreadable." ■