EYE OF THE STORM

Experts recently pointed toward security as the main obstacle for adoption of all cloud types and claimed that cloud security will be the main disruptive technology for 2013. But the Middle East has spoken out, and instead of running away, it looks to be chasing the eye of the storm.

We've seen an outrageous eruption in regards to cloud discussion over the past year in the Middle East, both public and private. Which solution is the safest, most cost-effective and best value-added is still a major debate, but at least the debate has moved from whether companies are actually going to adopt altogether.

Experts have spoken out and believe that the major talking point for 2013 is going to be tackling the object of protecting data within the cloud. As Florien Malecki, Head of Product Marketing, Dell SonicWALL, says, the reasons for adopting cloud solutions can no longer be ignored, but a level of understanding needs to be reached, and measures have to be taken to ensure that corporate data is safely stored.

"Consuming resources over the cloud can decidedly provide competitive advantages that businesses can no longer ignore. However, when leveraging the cloud, you also need to leverage the latest available technologies, such as application-intelligent Next-Generation Firewalls, to keep your cloud consumption secure, efficient and productive," he states.

Benoit Verbaere, Senior Portfolio Manager, Air Transport Industry Cloud, SaaS, SITA, adds, "Cloud is a volume game and so cloud providers can and must focus more on potential risks and put resources into avoidance because of the potential huge business impact threats and defects could have."

Chasing the storm

So what moves can businesses make to ensure that all data is fully secured before an attack is made?

Mikael Hansson, Head of Delivery Management Middle East, Ericsson, believes that selection of the right provider is key and that the company must be aware of a few critical pieces of information.

"Where the data is going to be stored and the local data protection laws in that area. How often does the provider have an independent security audit, and how well did it perform in the previous audit? And how accommodating will the provider be on your security policies?" he asks.

Cognizant's Mahesh Venkateswaran, Managing Director of Social, Mobile, Analytics and Cloud, believes that the early security measures come down to three points – robust security, trust and assurance, and monitoring and governance.

"Providing robust security means moving beyond a traditional perimeter-based approach to a layered model that ensures the proper isolation of data, even in a shared, multitenant cloud.

Providing trust and assurance - the company needs to have confidence in the integrity of the complete cloud environment.

And monitoring and governance - having utilities that allow customers to monitor the environment for security, as well as ensure compliance with other KPIs, such as performance and reliability. Using these utilities, customers should be able to perform these activities almost as well as they could in their own data centres."

The attack type

Brennan O'Hara, Security Solutions Manager, NetIQ, tells us that many of the attack strategies are the same as they have been over the last five or six years. Many security experts may argue with this point.

"The reality is that most successful attacks continue to use the same approaches that have been in use for several years. While concerns certainly exist among security professionals that cloud computing may introduce new vulnerabilities (and attacks that exploit them) we have yet to see specific examples of these. Rather, attacks still centre on the basics of exploiting poorly configured systems, tricking users into introducing malware into the network through things like targeted email attacks, and simply being opportunistic in taking advantages of unpatched systems and weak passwords," he says.

Mikael Hansson, Head of Delivery Management Middle East, Ericsson

The global cloud market will reach

$270BN

by 2020, analysts have predicted.

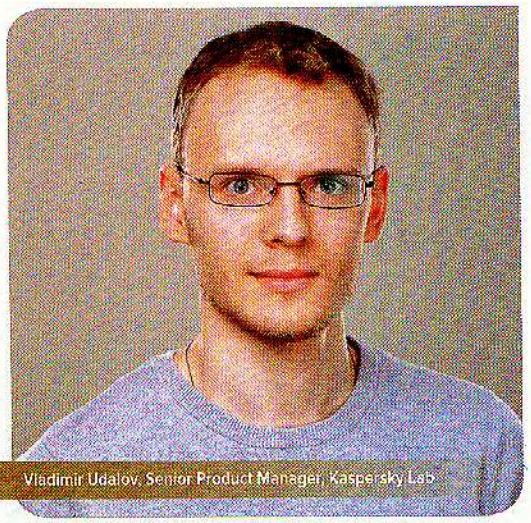
Nicolai Solling, Director of Information Services, help AG, seems to agree with this point, suggesting that the strategies and concerns are not what are changing, just the addition of some new concerns have been brought to life with the introduction of cloud.

"First of all, a cloud environment is a shared environment, which means that your 'next-door neighbour' in the cloud provider's environment could impact your data. If, for example, your neighbour is a politically active entity that uses the cloud service for news-casting of radical opinions, they may upset other people with different views and they may be the target of DDOS attacks. This attack may impact your services," he suggests.

Looking out for number one

Another key argument in the cloud sector is focused on who is actually responsible for the protection of the data. Traditionally, the company housing its own data centre would be responsible for protecting all the information inside but with third-party providers offering their space in the cloud up for adoption, are they then the key minder for what's inside?

Vladimir Udalov, Senior Product Manager, Kaspersky Lab, believes it's not that simple.



Vladimir Udalov, Senior Product Manager, Kaspersky Lab

"Technically, the cloud service provider is responsible for protecting data in the cloud, but from a legal point of view, it depends on legislation of the country where the customer of the cloud service resides. In many countries, all liability lies completely on the customers, and in case data is lost or stolen, the customer will have to take legal responsibility for that," he says.

And Noman Qadir, Acting Country Manager, Citrix MEA, also supports this view.

"Service providers are responsible for the protection of data in a public cloud," he says. "They should be able to provide security in a multi-tenant environment which makes sure tenants are not able to access the data of another tenant. In a public cloud environment, where there are multiple users across multiple organisations, encryption is a critical safeguard to ensuring data is safe and accessible only to the right users."

However, Miguel Braojos, Vice President of Sales for Southern Europe, Middle East and Africa, SafeNet, disagrees, arguing that the full responsibility should rest on the shoulders of those who own the data.

"Companies themselves should be responsible to protect their data in a public cloud. Companies need to make sure they control and own their data completely; the adoption of strong security solutions is and will continue to be key for them. In cloud environment, companies need to regain ownership, control and governance of their digital assets."

Experts believe, then, that IT teams will have to start building more relationships with these cloud providers and also see more IT budgets going down this route. The contract agreements become crucial in this area, where the discussion of lost or harmed data is concerned.

In many countries, the law says that 100% of the liability of lost or stolen data lies with the customer.

Srinivas Mamidala, Team Leader, Wintel and Storage Support, Emitac, says that one of the main consequences of data breaches may be the confusion over where the responsibility lies, saying, "Apart from the service level agreements and other important attributes of the cloud, customers should be aware of the legal terms in case of information theft. It is an important question to ask before signing a cloud computing contract."

However, Alexander Zarovsky, Director of International Sales and Business Development, InfoWatch, makes the point that, despite all the concern over the risks of this technology, larger vendors should in fact have the means to provide more security than ever before. He feels that with substantial investment, cloud solutions are far more secure than traditional solutions.

"Ideally, cloud services should be even more secure than traditional data centres. But this requires larger investments into information security. Thus everything depends on the service provider. If the provider has many clients then it has enough funds to invest into infrastructure and security. Therefore its cloud services can be even more secure than traditional company infrastructure."

But Khalid Muasher, Business Development Manager, Bitdefender, Middle East, claims that, again, it's not that simple, and that some companies can be found to be very underprepared and very unsecure.

"There are private data centres that are extremely secure, while there are, unfortunately, others that are shockingly unsecure. It is likely that an organisation with a well-secured private data centre that also uses public cloud will do so securely. Security is ingrained in the people, processes, and technology choices. An already unsecure organisation that also uses public cloud is likewise likely to end up with a poorly secured public cloud implementation."

Experts, it seems, are urging companies to manually seek out the most secure providers as well as to prepare themselves for any data attacks prior to the cloud deployment itself. Cloud adoption will continue to grow in the Middle East and worldwide, regardless of security concerns, but the consensus is that organisations must be aware that they're moving toward the eye of a storm. ■