Threatening Cloud? Opportunities & Pitfalls

Cloud throws up opportunities and pitfalls at the same time. According to experts, huge growth is coming but end users need to get educated to ensure they get solutions that offer dependable data security.

JUST a few years ago, the cloud was an enigmatic buzzword, a platform that was more conceptual than actual; certainly not the place where businesses would trust their infrastructure and business continuity. But that's all changed with the introduction of the major players in cloud hosting. AWS, Microsoft Azure and Google Cloud have become an accessible, big brand solution for small and medium sized enterprises to use and benefit from cloud computing's promise of low OPEX and scale up and down server use.

SaaS has kept pace with that new opportunity as new subscription services offer a plethora of technologies and applications in monthly payment schemes or as used data stream models. Clearly a tipping point is under way. A recent McAfee study found that in 15 months, 80 per cent of all IT budgets will be committed to cloud apps and solutions, yet just 23 per cent of organizations today trust public clouds to keep their data secure.

These 2 opposing realities point to a critical challenge. Trust in public clouds is an inhibition to greater uptake – fear is driven by security threats. There are also menacing regulations, like the recent US Cloud Act, that have sent a chill through those using US data centres and cloud platforms. However, armed with a security first philosophy, the cloud's benefits can be realised, and its dangers mitigated, and cloud can be used in private and hybrid solutions to connect on-premise with public clouds in a secure way.
The Cyber Security Threat is Real

Recent data breaches didn't surprise anyone who eyed the cloud suspiciously. In 2017, Pro Wrestling organiser WWE had 3 million re-

Clavister E10 cyber security appliance.

Mattias Nordlund, Clavister.

cords compromised in a data breach on an Amazon Server. Six years later after the fact and we've now come to realise how serious the dropbox 2012 data breach was. Hackers tapped into more than 68 million user accounts – email addresses and passwords included – representing nearly 5 gigabytes of data. Stolen credentials reportedly made their way to a dark web marketplace paid in bitcoins. Dropbox responded by requesting a site-wide password reset from the user base. They also promised an ongoing commitment to data security.

Then there was the situation that Yahoo found itself in where more than one billion user accounts were compromised in the attack. This includes first and last names, email addresses, dates of birth, and questions and answers to security questions. This incident is on record as the largest data breach in history and unrelated to a separate incident that exposed 500 million accounts months prior. The cloud has proved itself to be a place that needs security. Global Cloud Cyberattacks could cost $US53 billion according to Lloyds Insurance, but they also admit that risks are very hard to quantify.

Meanwhile, Skyhigh has collated data from 30 million users and their findings are telling, showing that 18.1 per cent of cloud-based file sharing and collaboration contained sensitive data from a variety of sources – from financial reports, payment information to health, revealed by merely searching the internet. The average enterprise experiences 23.2 cloud related threats per month – an increase of 18.4 per cent from 2016 and nearly every organisation gets at least one threat per month. But there's an irony, as Gartner's Jay Heiser, vice president and cloud security lead, explains.

"Contrary to what many might think, the main responsibility for protecting corporate data in the cloud lies not with the service provider but with the cloud customer – we are in a cloud security transition period, in which focus is shifting from the provider to the customer," Heiser wrote recently.

These observations bring home that there is an urgency that end users have more to do than they realise in the domain of security, both on-premise with physical next generation firewalls, or using virtual firewall instances in secure zone configurations.

"We've seen an increase in our customers using our virtual firewalls to deploy in the cloud, no doubt about it," says Mattias Nordlund, product manager at Clavister, a cybersecurity vendor based in Sweden whose Australian distributor is Sensatek.

"What we see is that data centres are becoming more 'cloudified' and that in turn attracts customers who want to reap the benefits of cloud computing and data storage. This is a good thing, but we need to ask the hard questions: do you really know who your neighbours are in that cloud?

"Do you believe that you should just leave your data unprotected in the cloud?" Nordlund asks. "Our position is simple. That you should use a virtual instance to protect against east-west threats, that there are things that you can do to create a firewalling of your organization in that realm and it's a minimum requirement should you choose that route".

Clavister was one of the first to create a virtual firewall in 2008 and has spent 20 years creating cybersecurity solutions for over 20,000 customers in 154 countries. This means Norlund is part of a team that's being confronted with the cybersecurity challenges of secure cloud daily.

"I would say that our customers in the Nordics are slightly more advanced in cloud topics than other parts of the world and so we've had to learn how to handle the problem," Norlund says. "For instance, we have a large MSP that uses our solution brilliantly to protect their customers and we've learned a lot from that. Our experience is that there needs to be education on the topic and that cloud solution providers, as well as their customers, need to take security serious and not simply believe the cloud platform will provide all the answers.

"We have surveillance providers that use both our physical and virtual NGFWs to secure those large streams of data going to the cloud and once you map the level of risk, they completely understand that they need to take more steps by way of security."
Clavister's Jan Nahlbom, concurs.

"Education is so important," he says. "For instance, we have a roadshow with one of our partners happening next month and one of the main topics we'll be discussing is the newly legislated US Cloud Act which states that if you store your data in the cloud with any US cloud provider or data centre, your data can be exposed to the US government upon request.

"We at Clavister have a strict no back-door policy which means that we'd never allow our customers' data to be given over to authorities, so we'd advise using a non-US based cloud solution for a start."

For more information about cloud security, contact Clavister at sales@clavister.com.