Securing the Cloud

Cloud adoption in the region is presently at a nascent stage, but steadily on the rise. Organizations in the Middle East are rapidly adopting cloud strategies, which include deploying business applications on public, private, or hybrid clouds. This continuing growth in cloud based services has translated into a growing demand for security services as well. In an escalating threat landscape as data continues to grow in the cloud, organizations, both large and small need to increase their focus on cloud security.

According to 451 Research, 60 percent of workloads worldwide will run in the cloud by 2018, driving greater agility and scalability, higher performance, and faster access to innovative technologies, all of which enable organizations to gain a competitive edge. As per the research and advisory firm, Gartner, public cloud services market in the Middle East and North Africa region will grow by 22 percent in 2017 to total USD 1.2 billion.

One of the main contributors to the upsurge in cloud adoption is the region’s focus on digital transformation. In the connected world, as the region looks forward to implementing smart cities, both public and private segments are focusing on harnessing latest technologies.

Yasser Zeineldin, CEO, eHosting DataFort

“Business operations are being moved into the cloud for higher return on investment, to fast-track their business growth, prepare for new business opportunities and market competitiveness. The move towards 360 degree security now includes not just a focus on visibility, prevention and management of threats, but also highlights the importance of compliance which has been gaining traction in the region,” said Yasser Zeineldin, CEO, eHosting DataFort.

According to Gartner, one of the challenges thus far was the lack of Tier 1 local cloud service providers, which forced local enterprises to look for cloud data centers outside the GCC, thus increasing application latency and possibly non-compliance from a regulatory standpoint.

Santhosh Rao, Principal Research Analyst, Gartner

However, IaaS cloud adoption is set to accelerate with AWS launching its local cloud data center in the GCC, as well as local hosters and telcos transforming themselves into cloud providers.

“While this is expected to stimulate interest, cloud technologies involve a learning curve that most enterprises would need to traverse,” explained Santhosh Rao, Principal Research Analyst, Gartner.

Harish Chib, Vice President MEA, Sophos

“We have noticed that organizations in the region are increasingly adopting cloud computing – either all-at-once or methodically over time and we see this as a big opportunity to help organizations secure their public cloud deployments,” added Harish Chib, Vice President Middle East & Africa, Sophos.

Savitha Bhaskar, COO, Condo Protego added, “Ensuring security in the cloud is similar to ensuring security for on-premises data centers – be it protection against deletion, theft, or leakage.”

Savitha Bhaskar, COO, Condo Protego

“Except now, security tools are expected to manage and protect corporate data using the same security controls and monitoring tools, regardless of where the data and applications sit. We work closely with leading global cloud security vendors such as Dell EMC, RSA, Symantec, and Veritas to build cloud security solutions for their customers,” continued Bhaskar.

According to Ossama Eldeeb, Senior Manager, MENA Partner Organization, VMware, channel partners play a key role in ensuring that data protection strategies and processes are in place.

Ossama Eldeeb, Senior Manager, MENA Partner Organization, VMware

In line with this, VMware and its partners across the Middle East, are also working closely with organizations on their digital transformation strategies, especially in securing their digital cloud workspaces with encryption, firewalls, data backup, and identity access management.

Rao explained that while the systems infrastructure provided by the cloud providers is inherently secure, enterprises are expected to take responsibility of the overall security function, and ensure the application stack and its underlying infrastructure is secure by implementing the right security controls.

Tarek Abbas, Systems Engineering Director – Emerging Markets, Palo Alto Networks

Palo Alto Networks 2017 survey into cloud security found 48 percent of UAE CIOs use public, private, or hybrid clouds. The report also revealed UAE organizations face a major disconnect between cloud aspirations and secure cloud infrastructure, with two-thirds (64 percent) of CIOs in the region ranking cloud security as important, but one-third (34 percent) admitting that they do not know if their cloud is secure.

“Security teams need to ask the right questions to effectively protect data and applications in the public cloud from a multitude of ever-evolving security threats,” said Tarek Abbas, Systems Engineering Director – Emerging Markets, Palo Alto Networks.

With the advent of BYOD, those who circumvent security regulations can put the organization’s data at risk. There is a need for the region’s CIOs to understand that despite increased cybersecurity spending, it’s more important to change traditional security models to secure applications. Equally important is for organizations to train their staff in cybersecurity tools and processes. By using secure cloud services, cyber-threat prevention, along with backup and disaster recovery solutions, Middle East organizations can manage business applications securely across clouds.