COVER STORY

TOWARDS 'LEAK-PROOF' CLOUDS

As the region grows Opex-savvy, Cloud security market is gaining importance for reasons more than one. The proliferation of IoT, increased cyber attacks, BYOD and data exchange are just fuelling the fire; and before we blink and open our eyes, the global cloud security market is expected to reach USD 13.93 billion by 2024.

BY: ANUSHREE DIXIT <ANUSHREE@GECMEDIAGROUP.COM> ■ PHOTO: SHUTTERSTOCK

The growing trends of BYOD and CYOD are expected to boost the global cloud security market. The significant utilization or adoption of the cloud-based service computing in the various sectors such as healthcare, BFSI, IT and telecommunication, and others help fuel the growth of the global market. Additionally, the rising threats related to the cyber world increase the dependency on the cloud-based services which in turn attributes the growth of the global market.

SECURITY IN THE CLOUD

Tony Zabaneh, Senior Systems Engineer – Channel, Fortinet says, "As Fortinet, our security portfolio is on a constant growth and development trajectory, probably the most notable or major developments were adding FortiSIEM to our solutions to complete the security cycle, and introducing our Security Fabric, which is the deep and tight integration between the network security components." Furthermore, multiple Cloud services and offerings are nowadays sharing the same infrastructure, networks, storage, bandwidth, and many resources. "This meant that if a cyber threat is targeted against one cloud service; it will most likely impact another untargeted victims.Cloud driven services are now threatened by unprecedented evolving cyber threats, which have to be tied with unprecedented security to provide threat mitigation and containment. Today security is extended to be part of the services, applications, architecture, network, storage, access controls, and every aspect that touches the Cloud," says Mohammad Jamal Tabbara Senior Systems Engineer – UAE at Infoblox

For GBM, Cloud security seems to be gaining more popularity across the world and hence security has also become a prime concern. "CCSK certification by CSA has now been acquired by ISC2 and is renamed as CCSP, which means that even big certification companies feel the need to educate more professionals on cloud security. Breaches are continuously observed in both cloud and non cloud environment," says Hani Nofal, Vice president, Networking, Security and Mobility at GBM

Saeed Agha, GM Middle East at Palo Alto says that, As cloud presence and the offerings available increase in the region, the consistency of security policies and data security capability will be more critical for cloud operators and cloud users alike. "This is an area where Palo Alto Networks can add great value for its customers and partners."

CLOUD SECURITY LATEST BUZZ

Gemalto's 2016 Global Cloud Data Security Study has found that while 73% of IT professionals say cloud computing applications and platform solutions are important to business operations today, only 43% say their organisations have clearly defined roles and accountability for safeguarding confidential or sensitive information in the cloud.

"Last year has also seen a marked increase in the storage of customer information in cloud environments from 53% of respondents to the Gemaltostudy in 2014, to 62% in 2016.," says SebastienPavie, Regional Director, MEA, Identity and Data Protection, Gemalto.

According to Infoblox, in Private Cloud model, Cyber-Security Ecosystem integration within the Cloud was a highly desired aspect in 2016, and it will continuo to do so. SDN Security is as well a very trendy topic that attracted CIOs and CISOs adopting the SDN technologies. "Yet tying all the diverse Cloud Security solutions together and deriving security intelligence out of the integrations and analysis would be the ultimate goal in 2017," says Jamal.

And so, a key point in our view on security is the ability to detect an attack at one stage, and then automatically reprogram the security infrastructure to be able to prevent that attack at a later stage. That requires consistent security capabilities in all stages, in all occasions where that attack may spread.

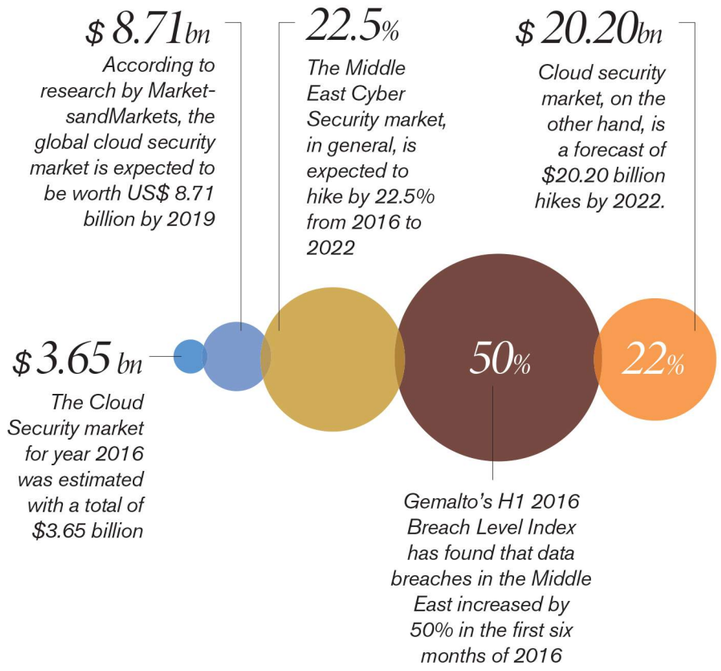
Cloud security currently is in the middle of two major changes: one is securing the exponentially growth of endpoints of connected devices in the Internet of Things era, vital for securing critical national infrastructure, and the other is defining cloud security policies rather than policies for private clouds on data centers.

DEEPAK NARAIN,
REGIONAL PRESALES MANAGER – MENA, VMWARE

"VMware NSX software-defined networking platform, which provides the foundation for agile cyber-security policies in virtualized and cloud environments, is on a USD 1 billion run-rate for FY2018."

HANI NOFAL,
VICE PRESIDENT, NETWORKING, SECURITY AND MOBILITY AT GBM

"Our approach to providing security solutions to our clients is an end to end approach, which means that GBM has the reach to multiple partners and the ability to understand the technology to help our clients in achieving the highest level of security."



TONY ZABANEH,
SENIOR SYSTEMS ENGINEER – CHANNEL, FORTINET

"Fortinet is the only network security solution vendor with an end-to-end portfolio designed to work together as an integrated and collaborative Security Fabric."

SEBASTIEN PAVIE,
REGIONAL DIRECTOR, MEA, IDENTITY AND DATA PROTECTION, GEMALTO

"It is no longer an option to secure one part of the ecosystem – security is required throughout the entire data lifecycle, from the cloud and core of the enterprise to the edge of the network."

SAEED AGHA,
GENERAL MANAGER - MIDDLE EAST AT PALO ALTO NETWORKS

"As cloud presence and the offerings available increase in the region, the consistency of security policies and data security capability will be more critical for cloud operators and cloud users alike."

RAJIV PRASAD,
CIO AT SAVANT DATA SYSTEM

"We also employ stringent security audit performed by the internal security team and third party integrators to raise the level of confidence for our partners to embrace cloud platforms and solutions."

SECURITY TIPS FOR THE CIO

The biggest value of cloud security strategy and tools is the capability of integration with the rest of the network.

CIOs should be aware of any laws and regulations that may apply to them and their data when opting for the cloud model.

Consider third party controls from service providers in their clouds security plans, especially in terms of compliance and data sovereignty, along with end-point security.

current security best practices are not enough to stop lateral movement inside the data center in the event of a breach

CIOs can create a network micro segment that is a bespoke perimeter for the application, where a much more granular set of policies can be applied.

With cyber-attacks exist, CIOs should implement effective compliance, governance and risk interventions

Storing data in the cloud without properly considering security is the same as locking your front door but leaving the garage open. Your network may be secure, but it means nothing if the cloud isn't equally secured as well.

Making Cloud access with consistent security policies for employees and contracts a requirement.

Security policy must be based on context such that policy does not have to change the underlying mapping to what is happening from a dynamic, automated nature

MOHAMMAD JAMAL TABBARA,
SENIOR SYSTEMS ENGINEER – UAE AT INFOBLOX

"InfobloxActiveTrust Cloud provides a significant security for the Oxygen of the Internet –i.e the DNS."