Cloud Security Trend

Brandon Chen, NubeSecure Partner Consultant

March 7th, 2016

We had a great time attending 2016 RSA Conference in San Francisco just a few days ago and can't wait to share with the community about what we learned. Let's jump right in.

SaaS is the future. For any company that's migrating toward SaaS complied, there is a problem to solve called Shadow IT. Shadow IT refers to the services used by business without the official internal IT backing. For example, business units will use a credit card to pay DropBox or Box for file storage/sharing because the convenience their internal IT couldn't provide in time. The risk is very high when this type of services are not monitored and controlled by policies. Virus/ Malware can be easily uploaded to the shared storage and spread to the computers used by other members of the same service account. As a matter of fact, Shadow IT is becoming such a prominent problem and business is trying very hard to catch up. This leads to the service provided by cloud access security broker (CASB). CASB can curb fan-out malware attack in a multi-cloud setting. It detects malware in realtime, monitor data exfiltration, look for abnormalities and enforce a common set of policy at a since point.

Realtime intrusion detection based on big data analytics and machine learning is on the rise. This naturally extends the traditional auditing capability. Consolidating monitoring, auditing and even data encryption in-motion to a single point of control has led to more adoption of API gateway. It's estimated 85.4% of US companies will use it.

By 2020, there will be 500 million smart phones in Africa and 200 billion devices globally. Today only 41% of the internet traffic is generated by human. The Internet of Things (IOT) has a huge potential.

DevOps security is gaining attention. In general, the exhibited solutions provide security measures for continued integration process and verify container configurations where micro services are deployed. Today about 23% micro services are deployed with docker. Some business has concern that docker executes as a root user, but docker related jobs has

increased more than 17 times in the past year. RackSpace is working on a secure docker container called “Carina”.

Multi-Factor authentication (MFA) has been around for a long time, but its significance is not shadowed by the newer biometric authentication methods based on iris, eye print, facial, voice and finger prints. Duo Security provides cloud based MFA and its business is soaring. Biometric authentication has its own limitation for being less definitive. It will continue to be used as part of a composite solution.