THE DARK SIDE OF THE CLOUD

COVID-19 HAS ACCELERATED CUSTOMER DEMAND FOR CLOUD-BASED TECHNOLOGIES, BUT SECURITY STILL REMAINS A TOP CONCERN.

The pandemic-induced migration to the cloud is gaining traction in the Middle East. Major players such as Microsoft, AWS, Oracle, and IBM have set up their cloud data centres in the region, enabling businesses to be more agile and efficient.

According to Gartner, the global end-user spending on public cloud services is forecast to grow 23.1 percent this year. The research firm says the events of last year allowed CIOs to overcome any reluctance to move mission critical workloads from on-prem to the cloud.

Though service providers claim the cloud is inherently more secure, some cloud security breaches have recently made news headlines. More than ever before, businesses are now far more concerned about data privacy and compliance, and many CIOs worry about the security of their data stored in the cloud.

"Cloud security threats closely mirror current industry trends. With the pandemic driving remote work, and thereby the transition of employees to new environments, the main security issues pertaining to the cloud relate to application vulnerabilities, email-based attacks, incorrectly configured firewalls, and authentication and secure access," says Maroun Hashem, Manager, Public Cloud and Alliances - Middle East, Africa, Pakistan & Turkey at Barracuda.

Frank Kim, a fellow instructor at SANS Institute, says whether it's sensitive data that can be easily monetised, intellectual property that can be stolen, or business proprietary information the cloud now has it all. The business drivers for moving to the cloud are undeniable and organised crime, nation-states, and your competitors understand this. "They may target your cloud systems and infrastructure directly or, more often, go for the weakest link in your people, whether they be malicious or negligent insiders," he says.

According to a recent McAfee report, the number of threats from external actors targeting cloud services increased 630%, with

Frank Kim

Gregg Ostrowski

the greatest concentration on collaboration services like Microsoft 365. The security vendor has observed 3.1 million external attacks on cloud accounts from more than 30 million cloud users during Q4 2020.

"Numerous 'breaches' have occurred in IaaS environments, but they do not look like your typical infiltrate-with-malware type of scheme. In most cases, the Cloud-Native Breach (CNB) is an opportunistic attack on data left open by errors in how the cloud environment was configured. Adversaries can exploit misconfigurations to escalate their privileges and access data using native functions of the cloud, instead of malware," says Vibin Shaju, presales director, EMEA enterprise, McAfee.

The elastic nature of cloud environments is another challenge. "With an on-prem traditional network it is relatively easy to keep track of workloads and applications. However, with cloud environments, it is difficult to know just how large the footprint might be. This is because non-IT functions — such as marketing, developers, and others will create, then sometimes abandon, cloud assets. This makes it difficult for the security team to gain a true view of all cloud inventory, including containers that spin up and disappear just as quickly,"

WHAT THE EXPERTS SAY

The pandemic resulted in a dramatic increase in cloud adoption, which was already on an upward trajectory even before the shift to remote work following COVID-19. On top of this, many enterprises opt for multi-cloud environments rather than hosting their data, applications, and services on a single cloud platform. This further complicates security responsibilities.

Cloud security follows a shared responsibility model. Configuration of the cloud environment is the responsibility of both the clients and the service providers. Though appropriately configuring the cloud environment seems like an obvious thing to do, the grey areas of shared responsibility mean that misconfigurations are more common than we might expect. Poorly configured cloud systems, tools, and accounts can be abused by attackers to exfiltrate data or launch attacks.

Manikandan Thangaraj, VP at ManageEngine

Migration to the cloud needs to be properly prepared and planned for by applying the "security first" guiding principle, and this could be particularly challenging considering the lack of security talents in the market. Cloud computing services are available online and as a consequence, anyone with an internet connection, the correct URL (web address) and the right credentials can access it. This is particularly attractive for cybercriminals who constantly attempt to violate systems, identifying vulnerabilities in order to exploit them to perpetrate malicious activities.

Giuseppe Brizio, CISO EMEA at Qualys

With every passing day, an increasing number of organisations are migrating their sensitive data and business applications to the cloud for operational flexibilities, cost efficiencies and quick scalability. To avoid vendor lock-in on a single Cloud Service Provider (CSP), many organisations are opting to work with multiple CSPs in a multi-cloud environment.

Lack of proper security and key management practices in a multi-cloud environment will only increase the organisations' attack surface, with cybercriminals being eager to take advantage of it as they get smarter and more sophisticated. Luckily, there many industry best practices, such as Bring Your Own Key (BYOK), Bring Your Own Encryption (BYOE), and centralised and automated key lifecycle management that can optimise data protection in the cloud.

Sebastien Pavie, regional VP for data protection solutions at Thales

Maher Jadallah

Maroun Hashem

Vibin Shaju

says Maher Jadallah, senior director - Middle East & North Africa, Tenable

Common cloud security mistakes

If you look at how rapid rollouts used to work, in many cases, technologists only had to concern themselves with their own environments. But today, behind every cloud-native application is a veritable smorgasbord of technologies, many of them third-party — integrated tools, platforms, interfaces and more. When organisations migrate to the cloud, they lose visibility and hence control of such dependencies.

"To compound this issue, enterprises often do not have the right tools, policies, and standards in place to ensure that security is an integral part of the innovation lifecycle. One of the most common missteps is to try and implement cloud services in a vacuum. This results in organisations having to perform intensive audits just to understand what cloud services are being used and what data is being stored there. Sound governance and effective internal collaboration are critical to the long-term success and scalability of digital experiences," says Gregg Ostrowski, regional CTO, AppDynamics.

Shaju from McAfee says keeping track of security incidents in IaaS is increasingly difficult when you operate in multiple cloud service provider (CSP) environments. "There is an interesting awareness trend here as well, similar to the "Shadow IT" we've seen for years with Software-as-a-Service (SaaS) applications being brought into the enterprise. At McAfee, we wanted to uncover the prevalence of these breaches and the impact they are having on companies worldwide. The most common point of leverage for a "Land" action is a misconfiguration in an IaaS resource, which is wholly the responsibility of the cloud customer but often overlooked," he says.

Tips for cloud security

It may seem overwhelming at first but it's also straightforward to get a handle on your cloud security, according to Kim from SANS Institute. Learn the cloud provider's services in detail so you can use and secure them properly. This means multiple providers like AWS, Azure, and Google because your business will likely be using more than one in a multi-cloud world.

"Ensure you have appropriate monitoring and visibility to identify anomalous activity. Finally, establish consistent controls and governance processes. Remember, it's easy to make a mistake, but you have to expect that these mistakes will occur. Leveraging automation for consistency and embedding security into your business and technical processes will help ensure you can build correctly from the start," he says.

Hashem from Barracuda says with their ability to protect cloud applications from a broad range of attacks ranging from DDoS to bots, web application firewalls (WAFs) are a critical component of the cloud security equation.

He adds it's also important to recognise that cloud apps will inevitably be targeted. So, understanding what happened is critical to both prevention and remediation. Unfortunately, far too many organisations either don't maintain logs, or have logs available in machine language alone, making them unusable for this purpose.

Jadallah from Tenable urges companies to return to the basics of cyber hygiene by leveraging vulnerability management and honest assessment of the challenges they face. This way, they can understand where the risks exist within their infrastructure, however dynamic, remote or short-lived they may be, as well as establish an efficient process to measure overall risk and secure the network.

"The security team needs to make sure it can actively detect all assets and identify key processes across the entire attack surface wherever it resides — including any assets in the cloud and container environments," he says.