Security in the age of cloud: From challenges to opportunities

James Peek
Senior Consultant
Sourced Group

James Peek is based in Toronto, having been with Sourced Group for 4 years. His passions include helping businesses enable secure public cloud consumption at scale. In his free time, he enjoys skydiving, scuba diving and motorbikes.

Equating cloud security with network security is one of the biggest shortfalls for businesses today, as they attempt to use identical tooling in the hopes of fortifying their security posture across both areas. Cloud security, however, includes more than merely securing the network from unauthorised access. It encompasses a wider range of multi-faceted organisational controls required in a dynamic environment. As such, businesses without a hybrid approach to encompass Cloud-native services and automation usually end up exposing themselves to a host of threats, inadvertently worsening their overall security posture.

Enterprises today are more prone to cloud security risks than ever before, owing to a combination of several factors:

- **Missing cloud security protocols,** derived from a general misunderstanding on how to successfully implement cloud security, which may place a higher dependency on traditional network controls
- **Consuming unauthorised cloud services** through Shadow IT, owing to the dramatically lowered barriers to entry for cloud consumption services
- **Increased surface of attack** from purchasing new products/services with insufficient knowledge on safeguarding one's cloud assets
- **The prevalence and ubiquity of the Internet** creating widespread open source knowledge and expertise for anyone to learn and execute coordinated and randomised attacks

In order to thrive in 2020, reimagined security solutions are needed to lower the risk of security breaches in the modern workplace, which often come at a great cost to organisations. Here is what you can do to proactively safeguard your business.

Conduct a cloud security maturity assessment

Being in a known good state ensures solid foundations to build upon. As such, organisations should start by assessing its current provisioned environment and workloads. This includes determining the maturity of its security, operations, risk management and organisational readiness.

Planning for scale is a strategy that compels companies to unbiasedly benchmark themselves against present industry standards and best practices. This would allow them to better qualify the gaps required to successfully adopt secure Cloud at Scale, allowing for cost and time optimisations as it avoids re-works in the years ahead.

Security in the public cloud domain follows a shared responsibility model. Therefore, recommending appropriate controls to ensure confidentiality, integrity, availability and non-repudiation of systems and data is an essential part of this assessment. A set of weighted and prioritised remediation recommendations should then be put forth, to best optimise the organisation's people and workloads.

Implement a robust cloud security protocol

It is imperative for companies to conduct their due diligence by ensuring that their cloud security protocols are both in place and kept up to date. To do so, it is recommended to align to one or more standard security frameworks early in the cloud adoption journey, such as the NIST Cybersecurity framework, or the CSA Cybersecurity Masterplan. Using security-driven development, SMEs should continually assess themselves against sanctioned best practices frameworks, permitting the use of services and functionalities on a roll-out basis, and only after threat modelling is carried out and compensating controls are implemented. Additionally, capitalising on cloud service providers' well-architected frameworks as part of a systematic approach in evaluating architectures for each workload can help proactively identify and address potential risks with one's cloud environment.

Principles such as deny-by-default, where deployment on the platform will not be allowed until a series of security opinions, threat models and controls are executed, and the implementation of a preventative build-and-release pipeline where appropriate, coupled with detective controls, should form one's basic security benchmarks.

Apply a continuous learning mindset

Cloud security presents ever-evolving challenges as new information comes to light, necessitating a continuous education cycle. For example, the recent and widespread adoption of public Application Programming Interfaces (APIs) have brought about new security challenges, owing to its vast potential in allowing anyone with valid credentials to interact with almost every part of your cloud environment, managing and updating business critical workflows. This has led to the rise in the theft - or "harvesting" - of credentials.

The impact of these breaches can be quite monumental since credentials, once obtained, may be used anonymously by anyone, anywhere. Keeping up to date with the moving parts of your Cloud at Scale journey plays a formidable role in making or breaking the business.

Identify your normal

Understanding what "normal" looks like within the realm of your cloud environment is just as important as implementing a double-layered defence against the myriad of potential threats, wherein a company not only detects failures in one's control processes, but also performs root cause analysis and threat remediation. Only then will organisations develop their capabilities to identify these "abnormal" events, remedy them and update organisational knowledge to prevent future occurrences.

The ever-increasing pace of new cloud feature releases and service updates could result in the inconsistent and unsecure enrolment of these capabilities into an organisation. Taking the necessary time to evaluate these services' security profile, undertake comprehensive threat modelling and develop the organisation's understanding of possible risks associated with the use of these services would prove valuable in thwarting future threats.

Good security is hard to achieve. Having a grasp of everything happening both inside and outside of one's business environment, without falling into the trap of implementing checkbox security, is a monumental task. That is why modern-day technologies require modern-day approaches, benefiting businesses who adopt a security-led perspective as one of their forefront business priorities.

So, how are you strengthening your defences against ever-growing cloud attacks? E