Growing role of security in fostering cloud adoption

Jun 11, 2020

All-pervading security will drive the next generation adoption of public, private and hybrid cloud platforms across industries

Originally published in ET CIO. By Vikas Arora, Sudeep Das and Bibhuti B Rath

'Security transcends technology' is an oft-heard phrase. This phrase perfectly describes the concerns of organisations particularly in the current scenario of constant disruption. The disruptive forces could be in the form of unprecedented events like Covid-19 or uberization of industries by start-ups introducing newer models of business. Whichever be the case, one cannot deny that the role of security is growing exponentially and it remains an obstacle in the wider adoption of the cloud, be it public, private or hybrid. In a world where remote working has become the new normal, we are witnessing a greater emphasis on the security of the cloud. This even as the foundational technologies of cloud have matured and organisations are now more aware than ever before about the many business benefits of the cloud. Therefore, here is how businesses can respond to their specialised security needs for using cloud platforms.

Automate security for DevOps

When DevOps teams within organisations build cloud-native services and work with container technologies, they need to integrate security checks within an increasingly automated pipeline. Organisations should ask their cloud vendors to provide solutions to detect and manage vulnerabilities in container images. Further, security should be a joint responsibility between organizations and their cloud providers. To achieve DevSecOps environment, organizations need to make security as part of their DevOps and Culture.

Safeguard data with encryption and BYOK

Organisations can use encryption to control access to data. They can also control access to encryption keys by using the bring-your-own-keys (BYOK) model. With BYOK, they can manage keys across all data storage and services. The added benefit of BYOK is that while it does not give access to the cloud service provider, it gives organisations the visibility and control of information needed for internal security compliance audits. BYOK also allows organisations to maintain control of their data, whether it is stored on-premises or in the private or public cloud. By design, the cloud should protect an organization's proprietary content and data and should follow the data privacy laws defined by the country in which they operate. Further, organisations can seek physically and geo-fence restricted workloads from their cloud providers to ensure they protect data at rest, in transit, and in-use.

Redefine network protection

Basic network security technologies like network segmentation, virtual isolated networks besides denial-of-

service mitigation and protection technologies such as web application firewalls and virtual private network are table stakes for establishing trust in a cloud platform. Organisations should check if their cloud platform offers security groups and options for creating and controlling micro-segmentation based on workload and trusted compute hosts.

Foil security threats with intelligent monitoring

Organisations often contend with low visibility into cloud-based workloads, application programming interfaces (APIs) and microservices among others. To combat the emerging security scenarios, they need visibility tools and a single pane of glass view that integrates in-house and managed security services. Enterprises can leverage tools such as cloud activity trackers, which provide a framework to view, manage and audit cloud activity, to comply with corporate policies and industry regulations. Such trackers can create a trail of all access to the cloud platform and services, web and the mobile. They should also make sure they have the option of integrating all logs and events into their on-premises security information and event management system.

Control access to the cloud

Strong identity and access management (IAM) practices prevent unauthorized users from accessing cloud systems. Security should cover APIs, cloud functions and back-end resources hosted on the cloud. When availing IAM solutions on the cloud from providers, organisations should check if these services are stronger than the existing tools that they are using for their on-premises workloads. Companies that have existing IAM solutions should use these solutions to govern access. If the existing IAM solutions are not designed with cloud in mind, then organisations should upgrade them to cater to cloud security.

Embrace a security culture and enhance employees' skills

With COVID-19 opening doors to newer threats owing to different silos of security capabilities from across product categories and vendors that are cloud-enabled technologies, organizations must realize the fundamental changes this new norm is bringing in with regards to shift in culture, skills and expertise. Security experts and developers have to embrace a 'secure-by-design' starting from the concept to the production and deployment stage. This will enable the security experts to identify gaps, design security and fix issues promptly. Security needs to be a forethought and employees need to be skilled in managing the cloud environment of their vendor along with leveraging their expertise to stay safe 24X7.

To summarize, the first generation of cloud computing began in 2005 and now we are at the dawn of the fourth generation of the cloud. In this generation, security technologies have evolved and address every aspect of cloud platforms, be it public, private or hybrid. Organisations no longer need to be worried about the lack or choice of technologies. It is about deploying the right-fit technologies so they can gain from the many benefits that the cloud offers. The role of security in fostering the adoption of cloud is growing and undeniable.

This blog is authored by -

Vikas Arora - VP, Cloud and Cognitive Software & Services, IBM India/South Asia
Sudeep Das - Technical Sales Leader, IBM Security Systems, IBM India/South Asia
Bibhuti B Rath - Technical Architect, IBM Cloud, IBM India/South Asia.

Blog Categories

Secure