How Does Evolving Cloud Adoption Impact Security?

Sumit Sehgal, Chief Technology Strategist, U.S., at McAfee, provides a window into what organizations need to know about security in cloud-native, hybrid and multi-cloud environments.

In response to the pandemic, organizations moved rapidly to the cloud to address urgent needs. What questions should they ask as they move forward?

First, the move to the cloud caused a massive shift in costs related to operating those cloud infrastructures. Given expected budget shortfalls, can they actually run the way they're architected today? In addition, is the workforce appropriately trained to manage that infrastructure — not only from a security perspective, but from an infrastructure operations perspective? Finally, to get things up and running quickly, some sacrifices were intentionally made in terms of security and good architecture practices. Now organizations have to ask what cost and effort is entailed in going back and addressing those sacrifices.

How does the shift to hybrid cloud introduce new security challenges?

The shift creates challenges primarily related to lack of visibility across the spectrum of security functions. Because data isn't sitting in your own environment, you can't easily access it to make security determinations. In addition, applications function differently in the cloud, so security controls may have to be re-architected. That can lead to poor visibility and discrepancies between what on-prem security controls and cloud controls are saying. Next, organizations may not have the data loss prevention, data tagging, behavioral analytics or even threat profiling controls they would have on premises. Finally, all these factors combined mean organizations must do more work manually to produce audit findings that once could be produced automatically.

Why can't organizations rely solely on traditional security solutions to secure data and workloads in hybrid or multi-cloud environments?

Traditional security controls are based on the client-server model, where the focus is on what types of machines attach to an application. In the cloud world, there's more dependence on the application architecture and how the applications themselves exchange data. Security solutions for hybrid cloud or cloud-native applications must be built in the same way, so they can run at the scale and elasticity that cloud applications can run. Traditional security controls are not designed for that. In addition, most security architectures are not built for the volume of data that security tools pull down from the cloud, so even if you deploy a cloud-native security tool, you won't see its full impact.

What approaches help improve risk posture in the cloud?

One approach is to standardize processes — think NIST or MITRE — so you have a common framework and language for measuring things like risk and attacks. That helps normalize the differences between cloud and traditional security so security teams can better understand what a risk actually means in a cloud environment. On the technology side, traditional threat profiling needs to move beyond the viruses and ransomware conversation and move toward user and entity behavior management, which looks at how users normally access and use an application. Organizations also need to articulate how separate applications securely exchange data for things like enterprise analytics. This is a nascent use case, but it has implications for critical systems where data integrity is important.

What are the benefits of cloud-native security technologies?

Because cloud-native security technology resides on cloud infrastructure, performance and resource provisioning is handled by the cloud. This enables security architecture and applications to elastically scale with the speed and type of data transfers that occur in cloud applications. It also lets them improve security capabilities and become self-learning by leveraging, at scale, innovations related to machine learning and artificial intelligence. Finally, cloud-native security technologies are built in a standardized way so they can integrate with multiple cloud types. That makes it easier for security practitioners to leverage information coming from these solutions for their operational use cases.

What workforce dynamics play into cloud security and how can organizations address them?

The newer cloud applications require a higher level of business conversation than security teams had in the past. Organizations need enough diversity — both in engineering talent and in business informatics talent — to create a well-rounded team. Significant training is also needed because skillsets are still very much geared toward the way we did things 10 years ago. It's also important to address psychological factors in security response teams. Studies show the stress levels in some agencies can be as high as those among 911 operators or air traffic controllers.

Did COVID also sacrifice your computer security?

The pandemic forced local governments to make sacrifices with their cyber security. New cloud infrastructures spun up almost overnight. Is your security architecture still supported?

Let McAfee show you how public sector agencies are economically filling the gaps in cloud security and gaining back visibility and control.

Learn more at **www.mcafee.com/publicsector**

McAfee™