Brought to you by: CIO FROM IDG

MANAGING SECURITY IN THE MULTI-CLOUD ENVIRONMENT

TIME TO LOOK OUTSIDE THE BOX?

It's tough enough these days to place the right staffer to deal with security on a single platform, but finding or training personnel who are skilled across multiple platforms is even more challenging. If you can find the right people, chances are they'll be recruited away as they gain experience and expertise.

Since RightScale began its State of the Cloud survey in 2013, security was always cited as the top challenge in cloud. That changed in 2016, when lack of resources and expertise moved into the number one spot.

As enterprises struggle with the challenge of finding resources and expertise, some may be overly reliant on their cloud service provider. In fact, security is a shared responsibility: While the cloud service provider is responsible for platform security, the customer must still ensure that apps and data running in the cloud are secure.

Gartner argues that enterprises may be too focused on the security capabilities of their service providers, rather than taking care of business internally.

"Concerns about cloud service provider security have become counterproductive, and are distracting CIOs and CISOs from establishing the organizational, security, and governance processes that prevent cloud security and compliance mistakes," says Jay Heiser, research vice president at Gartner. "In fact, Gartner predicts that, through 2020, 95 percent of cloud security failures will be the customer's fault."

Consider that it takes on average 205 days for an enterprise to detect a cyberbreach. The reality of security budgets is that corners get cut, mistakes go undetected, and vulnerabilities are just lying there waiting for some hacker to find them.

MORE SECURE

In most cases, Gartner asserts, public cloud services are a more secure starting point than traditional in-house implementations.

As companies increasingly adopt multi-cloud environments that encompass different platforms and core technologies, IT and security teams should be focusing on how to overlay an easily managed layer of security over diverse cloud services.

"Top challenges for cloud security includes the ability to provision security controls, assessing the security status, monitoring workloads, and maintaining regulatory compliance across clouds," Dan Conde, an analyst with ESG Research, said in assessing Rackspace's announcement last fall that it is extending its managed security offering to Microsoft Azure.

With that development, Rackspace Managed Security can detect and respond to security threats across leading cloud platforms, including Microsoft and Amazon Web Services (AWS), Rackspace Dedicated Hosting, and Rackspace Managed VMware Cloud.

EVERY PROVIDER IS DIFFERENT

While multi-cloud represents freedom of choice for enterprises to match workloads to different cloud services and platforms from different vendors, it will be a challenge for any one enterprise to have the skills and expertise across such a broad environment.

“Each public cloud provider uses different technologies, interfaces, and even terminology to describe services or behaviors,” observes Stephen J. Bigelow, senior technology editor with *SearchCloudComputing*. “There is no standardization of methodologies, services, instance sizes, performance, or other attributes between public cloud vendors.”

Of course, it is possible to go it alone within a multi-cloud environment, but security fears can be greatly relieved when you can leverage external expert services.