Brought to you by: CIO FROM IDG

ENSURING SECURITY FOR CLOUD APPLICATIONS

Ceding control to outsiders is unnerving, particularly when it involves enterprise applications. But with the right tools and processes, your applications can be as secure—if not more so—in the public cloud.

There's little doubt that enterprises are overcoming long-standing fears over the security of public cloud services. RightScale's 2017 State of the Cloud Survey found that 41% of all workloads are being run in the public cloud, compared to 38% in private cloud. Meanwhile, 25% of respondents cited cloud security as a major concern, down from 29% the previous year.

Yet, for every glowing survey on security, there's another survey that offers a more qualified view. In IDG Enterprise 2016 Cloud Computing Survey, for example, 52% of respondents cited cloud security as a barrier or concern, although that was a decline from the previous year "and worry about public cloud security maintenance is becoming less extreme."

These mixed messages are not really surprising, given that cloud continues to evolve. In particular, cloud users are gaining awareness that cloud security does not rest solely on the shoulders of the provider, but is a responsibility shared with the customer.

"Since the inception of cloud, the number one inhibitor of adoption has been security," writes Network Computing contributor and F5 tech evangelist Lori MacVittie. "What's changed is that the concern is no longer about security of the cloud itself, but security of the apps being deployed in the cloud."

AVOIDING MAJOR BREACHES

There's a general recognition that cloud vendors have a vested stake in security and have a proven track record in avoiding major breaches that have plagued some enterprises.

"Organizations have had a decade now to watch with bated breath for an attack of epic proportions to justify initial fears regarding cloud security," asserts MacVittie. "That attack has not yet materialized and we've long since moved past that as a factor in whether we deploy an app in the public cloud or not."

David Linthicum, cloud commentator and senior vice president with Cloud Technology Partners, says there's a reason for that. "Indeed, the approaches and mechanisms available to developers and administrators in the public cloud are often better than the tools and methods you use within the enterprise. However, in the context of the cloud, you need to look at security as a systemic concept."

It's not enough to build fences around applications and data, Linthicum argues. "Developers who build applications to run in public clouds, or migrate and refactor applications for the cloud, should focus on a few basic security concepts, including authorization, auditing, confidentiality, and integrity," he says.

Gartner asserts that cloud providers have as good or better security posture than most enterprise data centers. "Cloud computing does reduce the overall security scope, and it does require customers to manage some of the computing stack in a shared-responsibility model," Kasey Panetta writes on the Gartner website. "This is a good opportunity for new types of approaches and new method adoption to protect information. The cloud will require a different approach to security; on-premises security habits and designs won't work well for information stored in the cloud."

PLUGGING GAPING SECURITY HOLES

It's long been argued that application development has too often approached security as an after-the-fact bolt-on feature, with developers sometimes leaving gaping holes for hackers to discover. As noted in a Rackspace primer, "Many modern application compromises come through their own administrative back doors, so maintaining a security-minded organization and proper internal security controls is increasingly important. None of this is new, though it can be challenging to adhere to many of these tried-and-true best practices in today's [bring your own device] environments."

Gartner argues for leveraging the programmatic infrastructure of public cloud IaaS and automating as much of the process as possible to "remove the potential for human error — generally responsible for successful security attacks."

Automation is crucial as DevOps practices speed up the development and deployment process. "It is normal to find development teams now practicing continuous deployment models, making changes many times a day or even many times an hour," Rackspace points out. "The rapidly changing nature by which new resources are provisioned and de-provisioned, within minutes, requires new methods of thinking."

Linthicum offers several recommendations to foster cloud application security, not least of which is the use of identity and access management technology to ensure individuals and services are properly authenticated, authorized, and audited.

"Cloud application developers must understand IAM," Linthicum asserts. "Don't just attach it to resources such as data and services, but build it right into your applications. IAM systems include APIs that you can use for such things as rechecking that the user is authorized to access the application, the platform, the services, and the data. Any of these can be de-authorized at any time, and so it's never an all-or-nothing approach."

INTEGRATING ALL THE PARTS

Cloud-based Identity-as-a-Service (IDaaS) offerings are increasingly popular as a way to create and manage user rights across an enterprise cloud environment. Still, IT leaders must recognize that their security posture is more than the sum of the systems they have implemented, asserts Steve Tout, founder and president of the Forte Advisory consultancy.

"Over the past several years, modern cloud security solutions such as user behavior analytics (UBA), cloud access security brokering (CASB), and security information and event management (SIEM) systems were born and matured alongside IDaaS solutions, but their integration and utilization has not always been demanded by IT leaders," Tout writes in a *CSO* article. He makes the case that IT must drive a risk-aware IAM agenda.

Awareness along with new methods and tools will go a long way to increasing enterprise comfort level in cloud security. But the reality is that many businesses are simply overwhelmed by security demands. According to an Intel Security survey of 2,000 IT professionals globally, "Almost half (49%) of the professionals surveyed stated that they had slowed their cloud adoption due to a lack of cybersecurity skills."

Just as they have turned to cloud providers for infrastructure and software, many of these overwhelmed enterprises are also likely to opt for managed security services to supplement their capabilities. Few organizations have the resources to be expert across the entire IT security spectrum. Click here for insights into strengthening your security posture.