Brought to you by: CIO FROM IDG

BRINGING MULTI-CLOUD OUT OF THE SHADOWS

OK, so you've made the commitment to a multi-cloud strategy. What's your next step?

First, make sure you have a full understanding of how cloud services are currently being used – you could be in for a surprise.

Then try to figure out a strategy to best manage what is likely a multi-headed hydra. Be honest about how prepared and equipped you are to manage all the elements in your cloud profile.

WHAT'S HIDING IN THE CORNERS?

More than likely, you're already utilizing multiple cloud solutions (even if you don't know exactly how many). The typical enterprise is using a half-dozen clouds in some fashion, the 2016 RightScale *State of the Cloud Report* reveals. "Cloud users are running applications in an average of 1.5 public clouds and 1.7 private clouds. They are experimenting with an additional 1.5 public clouds and 1.3 private clouds," says RightScale.

But that half-dozen may be just the tip of the iceberg. A report by the consulting firm PwC finds that among European companies the average number of cloud services in use is 987! That's because business departments and individual users throughout the enterprise are so easily able to sign up for cloud services without the knowledge of IT.

"Shadow Cloud – the unsanctioned and uncontrolled use of cloud services – has emerged as today's equivalent of the Shadow IT problem, creating both risks and opportunities for business," says PwC.

DON'T OVERREACT

A word of caution: Those data points should not be cause for IT management to go on an abrupt rampage trying to stamp out shadow cloud usage altogether. That could cause more problems than it solves.

Noted cloud commentator David Linthicum writes that "CIOs can embrace, rather than fight, the rise of shadow IT for their own benefit."

Linthicum cites three business benefits of shadow cloud: Existing business users won't have to be convinced of the benefits of doing things in a new way; it can cut through lengthy requirements cycles for departmental needs; and "third, these shadow cloud deployments give you the green light to put more stuff on the cloud, including applications and data," he says.

BALANCING CONTROL ISSUES

Still, says Brad Schulte, senior architect and Amazon Web Services domain specialist for Rackspace, that leaves CIOs walking a tenuous line:

"They are still charged with protecting the information of the organizations they serve. They must continue to provide oversight and control of IT while simultaneously relinquishing control. And, they must act in the financial best interests of the organization, which means imparting fiscal governance over the IT budget while once-fixed expenses become variable and are now often directly controlled by the lowest levels of the organization."

Schulte says that IT chiefs faced with demands from different areas of the company, such as DevOps, for ready access to Amazon Web Services typically either "throw up their arms in defeat" and allow unfettered access, or place onerous restrictions on its use.

The end result: "IT is either being blamed by the rest of the organization for legitimately failing to provide any oversight or control, or being blamed for stifling innovation and inhibiting progress." Schulte argues that IT leaders should modify legacy governance processes to account for and embrace the changes these cloud services bring.

"If the IT shop beats down shadow IT, it's missing an opportunity," Linthicum says. "If the IT shop ignores shadow IT, it's not doing its job. Instead, IT shops should engage constructively with shadow IT, treating it as a resource and opportunity."

So, the issue is not whether shadow cloud is going to be used – users will always find a way around onerous policies or vote with their feet – but rather how it can be managed to the benefit of the enterprise. And that likely means embracing multi-cloud wholeheartedly, and figuring out how to best manage it.

EMBRACING MULTI-CLOUD

A multi-cloud strategy offers many benefits to the forward-looking enterprise, but it also entails new management challenges.

Foremost on the benefits front, multi-cloud provides the opportunity to choose the best-suited cloud solution for individual workloads. It also reduces the risk for vendor lock-in and increases leverage over vendors.

Further, multi-cloud also can be an asset in disaster recovery strategies, and makes it easier to deal with compliance with regulations restricting the migration of data across national or regional boundaries.

Now to the challenge, which primarily revolves around the issue of managing multiple vendors: tracking costs and managing billing, different admin interfaces, varying skills needed for different cloud solutions, and integration across cloud solutions.

"While some service providers will develop intercloud features and tools, users must navigate this increasingly complicated cloud space and make it work at the business level," writes Tom Nolle, president and founder of CIMI Corporation and the firm's principal consultant/analyst.

Just the process of selecting different vendors for different cloud services can be overwhelming. Fixating on relatively minor variances in pricing between similar service providers can be self-defeating says Nolle: "Integration and management costs can cancel out price differences among providers, and in some cases, these costs could even outweigh the cloud services' benefits."

THREE APPROACHES TO MULTI-CLOUD MANAGEMENT

One solution is to opt for a cloud broker to gather the data needed to make decisions on which cloud providers to use. But, as Linthicum argues in another article, "using cloud service brokers may cost you more in the long run because you'll need the in-house expertise for each service that the broker might allocate."

An alternative is to utilize a cloud management platform (CMP). But, as Gartner observes in a CMP guide, that market is fragmented and rapidly changing.

"Enterprises that are successful in implementing CMPs for [multi-cloud] management and policy enforcement are early technology adopters, with technical expertise, mature processes, and centralized governance, and have been successful in combining CMPs with other tooling (often homegrown)," says Gartner. That is a pretty narrow slice. Plus, Gartner adds, enterprises need to weigh the value gained against being locked-in to the CMP provider.

For many, the third alternative may be most practical: turning the management aspect over to a managed service provider that can administer not only the customers' computing, storage, networks, and operating systems, but also the complex tools and application stacks that run atop that infrastructure. If multi-cloud is just the means to an end, why invest in tools and skills to run it when you can apply those precious resources more directly to supporting business goals.