OPENING UP OPPORTUNITIES—AND RISKS—WITH PUBLIC-PRIVATE CLOUDS. BY **CRYSTAL BEDELL**

CLOUD COMPUTING DISCUSSIONS no longer center on whether to deploy a private or public cloud, but *when* to deploy them both in a hybrid cloud model. Amidst concerns of NSA spying, and increasingly rigorous security and regulatory compliance requirements, a hybrid cloud seemingly offers the best of both worlds. But a hybrid cloud doesn't eliminate the risk of moving to the cloud. By providing a larger attack surface, a hybrid cloud can actually increase risk. The key to mitigating that risk is understanding exactly what you're getting into.

Hello, Hybrid

IMAGE BY ©JOHN KUCZALA

RETURN TO CONTENTS

DEFINING THE HYBRID CLOUD

Let's begin by establishing what it is we're talking about when we say "hybrid cloud." For the purposes of this article, we'll use the definition established by the National Institute of Standards and Technology (NIST). According to NIST, a hybrid cloud "is a composition of two or more distinct cloud infrastructures (private, community or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability."

A hybrid cloud allows organizations to take advantage of the public cloud's benefits: namely, its elasticity, scalability, and per-usage pricing model. Non-sensitive data and processes in the private cloud burst into the public cloud, when needed, for additional computer power. When the need subsides, those processes and data are brought back on premises. A commonly used example is an e-commerce site bursting to the public cloud during the holiday season.

Meanwhile, sensitive or regulated data is stored and processed in a private cloud where the organization has more control and visibility over the infrastructure.

UNDERSTANDING THE RISKS POSED BY A HYBRID CLOUD

Even if companies are careful about keeping sensitive or private data in a private cloud, a hybrid cloud still introduces additional risk. "[Companies] are increasing their risk because, in general, these things are still new, and organizations don't tend to understand the implications of what they're doing," says Nikita Reva, CISSP, manager of Information Security and Risk Assurance, PricewaterhouseCoopers.

Randal Asay, CTO of Catbird in Scotts Valley, Calif., U.S.A., agrees. "Hybrid cloud defines an automated control point to allow you to expand your footprint and reduce it when you don't need it. That introduces security problems and a mind shift for most infrastructure teams."

Daniel Redding, CISSP-ISSEP, senior Information Systems Security engineer for Saint Security Services based in Springfield, Va., U.S.A., puts it simply: "You need to make sure that not only is your system and application configured appropriately, but that the public cloud is as well."

Companies decide to offload processing to an infrastructure-as-a-service (IaaS) provider, Reva explains, without realizing that the security controls they've put in place in their private cloud do not necessarily exist in the new environment they are bursting to. "It doesn't just take care of itself, and some of the cloud infrastructure is new and technically challenging. The traditional organization that hasn't done this may not understand what it's all about."

> "Make sure you know what security controls your provider has in place."

JD Sherry, vice president of Technology and Solutions for TrendMicro, based in Las Colinas, Texas, U.S.A., likens renting computer power from an IaaS provider to renting an apartment.

"The landlord invests in paint, the building, and the sidewalks. But they won't help you secure your assets inside your apartment. The cloud provider will secure you and give you levels of assurance up to a certain point, but once you look at securing applications on the server, that's a shared responsibility."

As the customer, you must understand where the provider's responsibility ends and yours begins.

"Make sure you know what security controls your provider has in place. You need to know that the provider has not just a risk management strategy and performs risk analysis, but that those are in line with your organization's processes and strategies and have an acceptable level of risk for your data," Redding says. "A lot of that will come from a security-minded SLA (Service Level Agreement)—making sure that in the SLA [the provider is] contractually obligated to provide a certain level of protection for your information."

IMPLEMENTING SECURITY CONTROLS IN THE PUBLIC CLOUD

Once you understand the cloud provider's responsibility, it is necessary to understand what you are doing in the private cloud to meet the security requirements of a given workload and determine how to put the appropriate controls in place in the public cloud. According

to Reva, the latter can be a challenge.

"You have to think about how am I provisioning security controls that are appropriate to what I'm trying to do," he says. "The key is how do you do that in a way that's dynamic and doesn't slow you down? It should not happen manually. It should happen automatically, in a way that ensures servers are stable and the controls you want to retain go with it.

"Tools like Chef and Puppet—automation tools that were originally created to provision cloud infrastructure—now are used more and more for provisioning security controls and applying hardening controls onto that infrastructure."

Once the workload is in the public cloud, you need tools to monitor and further assess it. Reva advises using a monitoring tool that can work across both your public and private clouds, and can provide a dashboard view of how the infrastructure is operating from a security perspective.

Organizations should also consider vulnerability management for servers residing in the public cloud, Reva warns. Of particular concern is how those servers will be scanned to ensure that they meet security requirements. In many cases this requires getting permission from the public cloud provider to perform the vulnerability scan, and then coordinating the scan with the provider, which can be a challenge, he explains.

Another option is to use a tool that has been preapproved by the cloud provider. For example, Reva says customers of Amazon Web Services can use Core Security's Core CloudInspect to scan their cloud infrastructure without having to get special permission from Amazon. Core Security has already done the legwork with Amazon and has built the tool specifically for Amazon's infrastructure. ●

CRYSTAL BEDELL *is a freelance technology writer and regular contributor to* InfoSecurity Professional *magazine.*

FACT VS. FICTION

Busting the Myths about Hybrid Cloud Security

THERE'S NO SHORTAGE of cloud myths, and they can easily lead organizations and their security professionals astray. The danger in these myths is that organizations fail to properly secure their hybrid cloud deployments or—maybe worse—fail to deploy a hybrid cloud at all.

Perhaps the biggest cloud myth is that public clouds are less secure than private clouds or on-premises data centers. The experts we spoke with unequivocally agreed that this is not true. "There's no evidence that [the public] cloud is less secure," says Nikita Reva, CISSP, manager of Information Security and Risk Assurance for PricewaterhouseCoopers. "The large cloud providers have a lot of vested interest in keeping you secure."

Chris Richter, vice president of Managed Security Products and Services of CenturyLink Technology Solutions, based in Monroe, La., U.S.A., adds, "Most public clouds are run by reasonably sound cloud service providers. They provide better security than customers can do on their own, partly because there's been so much scrutiny and so much at stake that they have to be proficient around it."

Consider, for example, a financial services organization that runs its data

CONTINUED ON PAGE 16

RETURN TO CONTENTS

 CONTINUED FROM PAGE 15

centers internally and doesn't have the capital expenditures to keep the infrastructure up to date, explains JD Sherry, vice president, Technology and Solutions for TrendMicro, based in Las Colinas, Texas, U.S.A. "The risk there of not refreshing the infrastructure is very real, and we're seeing a lot of organizations see their risk internally elevate because they haven't invested in technology."

"If done appropriately and you exercise due diligence and you look at where you need to bring security best practices to reduce that gap, going to the cloud can reduce risk."

—JD SHERRY, vice president, Technology and Solutions, TrendMicro

When that same organization moves to a cloud provider, the multi-year capital expenditure becomes an operations expenditure, and the cloud services provider is taking care of keeping its infrastructure up to date. "[Moving to the public cloud] saves a ton of money and time, and reduces risk because if you look at SLAs, you're relying on [the cloud services provider] to take care of a lot of the risk, which you used to absorb internally," Sherry explains.

This is not to say that public cloud services present no risk. But the risks companies face by operating in the public cloud are different from those they face internally, explains Reva, referring to Alert Logic's State of Cloud Security Report.

"On the cloud, people are trying to slow you down, perform a DDoS attack to disable an application or brute force to bring something down," he says. "In traditional environments, [attackers] know what they're after. They use more targeted attacks in terms of intellectual property and the crown jewels, what's most meaningful to the organization."

This is because, in the cloud, the entire infrastructure is registered to the cloud services provider, so it becomes more difficult to determine what company is using which part of the infrastructure. Bottom line, according to Reva: "[Attackers] concentrate on traditional infrastructure with more targeted types of attacks."

This is where due diligence comes in. "If done appropriately and you exercise due diligence and you look at where you need to bring security best practices to reduce that gap, going to the cloud can reduce risk," says Sherry.

This means taking responsibility and doing your part to ensure that the public cloud infrastructure meets your security requirements. Sherry warns that, after dispelling the "no cloud is secure" myth, many organizations wrongly believe that moving to the cloud means offloading all responsibility for security.

"People think that when they go to Amazon Web Services or Rackspace that they'll be fine and everything will be perfect. That's a false sense of reality. [The providers] will tell you that you have security up to a certain point, but after that you have to layer security on top of it."

Finally, when it comes to hybrid cloud security, companies should be vigilant in protecting governance. "Given the highly dynamic nature of using these services, many companies think it's not practical, but it is important," says Reva. "If you're bursting into the public cloud as part of a hybrid cloud and you're not thinking about security, you should be. Otherwise, it may leave you exposed."

Reva encourages the involvement of stakeholders who are looking over IT governance. "Internal audit will want to understand...how are we governing ourselves to avoid ending up in the *Wall Street Journal*." ●

—Crystal Bedell