NETWORKWORLD

This story appeared on Network World at http://www.networkworld.com/supp/2013/enterprise1/021113-ecs-hybrid-clouds-security-266156.html

Hybrid clouds pose new security challenges

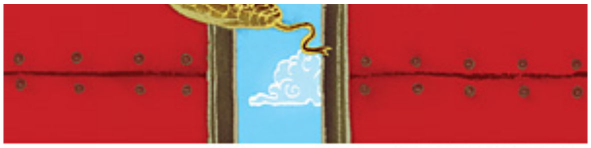
Locking up data that moves between private and public clouds can be a slippery problem

By Christine Burns Rudalevige, Network World

February 11, 2013 12:05 AM ET

Network World -

If 2013 is the year



YUKO SHIMIZU

enterprises begin implementing their hybrid cloud strategies, as the experts are predicting, then it follows that this will also be the year when hybrid cloud security takes center stage.

According to analysts, industry watchers and security practitioners the bad news is that there is no silver bullet on how to fully accomplish security in a hybrid cloud.

That's because there are so many facets to hybrid cloud security; there's the issue of how to secure on-premise data center resources, how to secure applications that burst to the public cloud, how to secure data stored with multiple cloud service providers, how to protect the virtualized underpinnings of your public and private clouds, and finally how to secure mobile devices that connect to your cloud infrastructure.

If that's not daunting enough, another reason why there isn't a one-size-fits-all solution is that the definition of hybrid cloud is open to interpretation.

[CLOUD: Cloud security to be most disruptive technology in 2013

12 hybrid security products to watch**]**

And every company has a different comfort level when it comes to security in general and cloud security in particular. One company's game plan for keeping a minimum set of operations under lock and key inside the on-premise data center or a virtual private cloud, while pushing batch processing or user front-end processes to the public cloud might be another IT department's worst nightmare.

"Every hybrid cloud implementation is unique and that makes securing them a moving target," says Dave Asprey, vice president of cloud security at security management vendor

TrendMicro. Asprey subscribes to the notion of ambient clouds, essentially the idea that enterprise customers are going to move toward a distributed cloud model where they employ multiple cloud providers - each replaceable based on use case, price and availability.

"I don't necessarily think the types of threats against the ambient cloud is up from those used against traditional data center or private cloud schemes, but the potential risks against the data running across these distributed cloud certainly is," Asprey says.

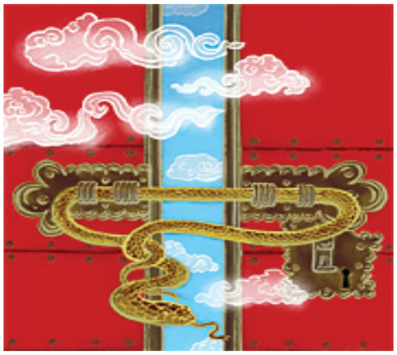
Security strategies that work

The good news is that enterprises already employing defense-in-depth practices across their existing networks can apply those same tenets within a hybrid cloud security management strategy.

The caveat here, though, is that IT management must commit to a whole lot of advanced planning and prepare their staffs for a bit of technological tweaking of its security policy and gear before the hybrid cloud goes live (see story on **hybrid cloud implementer tips and tricks**).

"Typically in this industry the adoption of any technology happens well before security considerations surrounding it are fully addressed," says Gary Loveland, a principal in PricewaterhouseCooper's advisory practice and head of the firm's global security practice.

With hybrid cloud, Loveland says, clients are being clearer about the security requirements up front and are forcing cloud



- Hybrid clouds pose new security challenges
- Cloud security tips and tricks
- 12 hybrid security products to

service providers to be more prepared to have solid answers on topics ranging from defining and ensuring multi-tenant boundaries, PCI and FISMA compliance, and auditing capabilities.

watch

- Enterprise Cloud Services archive

Industry guidelines can help

The Cloud Security Alliance in 2011 established the CSA Security, Trust & Assurance Registry, a free, publicly accessible registry that documents the security controls provided by various cloud service providers. The registry, which vendors supply the information for about their own products, is designed to help users assess the security of cloud providers they currently use or are considering contracting with in the future. To date, the registry contains information about 20 providers.

The underlying problem, Loveland says, is that enterprises have to mature enough in their use of virtual technology and cloud services management to take advantage of the higher security offerings.

Jeff Spivey, international vice president of ISACA, an association of IS professionals dedicated to the audit, control, and security of information systems, and vice president of mobile security vendor RiskIQ, concurs. He sees all too often that enterprise IT assumes that once they hand off their operations to a cloud provider, that the latter then assumes sole responsibility for security.

"Not true, it's at that point that IT needs to become even more diligent about implementing sound security across their clouds," Spivey says.

He pointed to COBIT 5.0, the newest version of ISACA's framework for governance and management of enterprise IT which outlines IT control objectives for cloud computing in general, as a strong guideline for how to implement hybrid security.

As hype surrounding cloud computing continues to grow, IT departments are being pressured by management to seize some of the cloud's promised economical benefits. But it's IT's job to make sure they are not risking the farm in order to go into the cloud to see those benefits.

In fact, computer scientists at the University of Texas in Dallas have devised an algorithm that can help companies develop a risk-aware hybrid cloud strategy.

According to one of the researchers, Dr. Murat Kantarcioglu, the scheme is an efficient and secure mechanism to partition computations across public and private machines in a hybrid cloud setting (see the paper).

Kantarcioglu and his colleagues have set up a framework for distributing data and processing in a hybrid cloud that meets the conflicting goals of performance, sensitive data disclosure risk and resource allocation costs getting weighed and balanced.

The technology is implemented as an add-on tool for a Hadoop and Hive based cloud computing infrastructure and the team's experiments demonstrate that using it can lead to a major performance gain by exploiting hybrid cloud components without violating any pre-determined public cloud usage constraints.

Having to think about how hybrid cloud operations fit into a company's overall information security management scheme could help IT departments reset the appropriate level of security for the processes across the entire enterprise, argues Pat O'Day, CTO at Bluelock, a VMware based cloud service provider in Minneapolis.

"We now get to think about how to set the right level of security on a application-specific, a process-specific or even a data-specific basis," says O'Day, a condition that gives enterprises a lot of leeway in terms of where they want to spend resources on security.

Rand Wacker, vice president of products for CloudPassage, a cloud server security vendor, suggests customers take the strictest security scenario - most likely pertaining to hybrid cloud usage because there are direct links between the public cloud and on-premise resources -- and set the most stringent security policy for that level of risk.

ISACA's Spivey advises clients that whatever security policy they establish, they must be sure that it is portable. "Don't lock your policy to your cloud provider," Spivey says. There will be a time down the road where you will want to migrate away from them for either price or performance reasons and you don't want to have to rethink your whole security policy to make the switch, he says.

Burns is a freelance writer. She can be reached at cburns1227@gmail.com.

Read more about cloud computing in Network World's Cloud Computing section.