Securing Hybrid Cloud Applications

The cloud is here to stay. Companies small and large, all across the globe, are investing in cloud technology. The ability to deploy and scale applications in the cloud in minutes instead of weeks is game changing in terms of speed to market, flexible growth strategies and cost management. Many companies are moving to Software as a Service (SaaS) models, which fuel cloud adoption at multiple levels. No company wants to watch its competition reap these benefits while it lags behind.

Public Infrastructure as a Service (IaaS) providers, such as Amazon, Rackspace, GoGrid and Terremark, are enjoying rapid adoption, as are hybrid-oriented cloud infrastructure technologies, such as Eucalyptus and OpenStack. Hybrid cloud hosting offers several key advantages over public or private cloud hosting:

• **Convenience**—Organizations can delay or avoid purchasing, installing and maintaining hardware. Hybrid allows a company's virtual servers to be deployed from its private cloud environment to public IaaS easily and quickly.
• **Agility**—New servers can be up and down within minutes, either in the public cloud environment or the public IaaS environment. Use cases, such as temporary growth for product testing or rapid customer deployment, become faster and easier, and include more controlled costs.
• **Economics**—Companies no longer need to build the largest-needed server farms to handle peak capacity just to have large percentages of their server capacities idling. Using the hybrid combination of private cloud and public IaaS, capacity can scale up and down dynamically to match business needs and recover costs wasted on idle servers.

The hybrid model enables companies to cover their day-to-day computing needs using their private clouds, bursting into public cloud resources for peak workloads, transient computing needs and rapid-deployment scenarios. The benefits of this model are driving rapid growth, although the model does come with concerns.

**SERVER SECURITY AND COMPLIANCE**

Security and compliance are two of the biggest obstructions to hybrid cloud adoption. While organizations such as the Cloud Security Alliance have made great strides toward education and guidance regarding cloud security, a range of technical challenges and misunderstandings still places companies at risk.

The technology community recognizes that servers hosted in multitenant clouds are at increased risk without layers of in-depth perimeter controls, typically found in the data center. CloudPassage recently conducted a nationwide survey among 164 technology professionals and found that:

• 45 percent of respondents cited a lack of perimeter and/or network controls as their primary cloud security concern, making perimeter defenses their chief cloud security issue
• 39 percent were uncomfortable with the concept of multitenancy, where a number of companies share the same infrastructure
• 21 percent understood that their traditional enterprise security tools no longer work in the cloud
• 31 percent of respondents believe that their cloud provider will take care of securing their cloud servers

For information security and compliance professionals, the last statistic on the list should be of great concern. A large percentage of cloud users are under the misguided belief that they have no responsibility for cloud server security.

In reality, cloud providers place the responsibility for virtual server security squarely on their customers. They will, of course, secure the shared network, hardware and hypervisor environments that support the guest virtual machines, but the customers are directly responsible for protecting their own virtual cloud servers, starting with the operating system and moving up the stack to include network, application and database services in use.

Carson Sweet is cofounder and chief executive officer of CloudPassage. His information security career has spanned nearly two decades and includes a broad range of entrepreneurial, management and hands-on technology experience. Prior to founding CloudPassage, Sweet served as RSA’s principal solutions architect for the financial services sector, chief security officer for GlobalNetXchange and chief technology officer for the Investor Responsibility Research Center.
Almost all providers spell this out clearly in their service level agreements (SLAs) and advise their customers to implement firewalls, intrusion detection systems and other security controls. While most providers are transparent, some providers do leave customers in the dark on this critical issue. The security SLA is one of the first areas to examine as businesses consider the risk implications of allowing servers and data into public cloud environments, a critical component to achieving the benefits of hybrid server hosting.

CLOUD SECURITY IS DIFFERENT
Data centers have long relied on strong perimeter controls to prevent server weaknesses from being exploited. Servers were safe behind the corporate firewall, and that belief in safety could lead to relatively lax enforcement of security standards at the server level. Unfortunately, weak server protection makes its way easily into private cloud hosting, making it one cloudburst from severe exposure of servers moved onto public resources.

Securing cloud servers requires a new approach. Dynamic cloud environments, especially public IaaS clouds, have greatly reduced the network and hardware control needed to create defined perimeters or security choke points. The technical nature of cloud-hosting environments also makes them more difficult to secure. Cloud server security mechanisms need to dynamically scale up and scale down with the servers themselves, and organizations need to be flexible in the ability to operate in either the private or public sides of a hybrid cloud.

The elastic nature of cloud-hosting environments can also lead to dramatic increases in exploitable server vulnerabilities. Cloud servers are easily replicated or cloned within seconds, typically to increase available computing power. If a server is vulnerable to exploit, cloning that server multiplies the vulnerable surface area available to attackers. Every single server has to be rigorously hardened before it can be exposed to public cloud threats; the speed and scale of cloud deployments coupled with deteriorating change management makes automation absolutely critical.

AVATAR NEW YORK’S HYBRID SECURITY APPROACH
One of CloudPassage’s customers is New York-based digital agency Avatar New York. Avatar was founded in 2003 and combines art and technology to deliver consistent branding and solid e-business solutions that are deployed on a combination of public and private cloud infrastructures.

Patrick Tully, Avatar’s chief technology officer, had the vision of leveraging the agility and scalability of the cloud to match the increasing pace of his customer’s demands. “Our Internet solutions must be delivered fast and with maximum flexibility for the future. We engineer technology requirements on a real-time basis as business models are changing in conjunction with new technologies,” Tully says. His team needed to ramp up its number of Rackspace servers frequently, using automated tools such as Puppet to meet the computing demands of the organization’s customers.

Since the organization manages valuable customer information, it has rigorous security requirements. Initially the Avatar New York team used traditional security products, but soon found that these tools were not designed to work in dynamic cloud environments. “They took hours to configure and did not have an [application programming interface (API)] for automation,” Tully recalls.

Tully had read about CloudPassage on a blog and went to its web site, where he learned more about Halo. “I was impressed when I asked a question on the community site and got my answer in less than 24 hours,” remembers Tully. He signed up for the free Halo Basic platform, and in only a few minutes Halo was installed on Avatar’s cloud servers. Avatar’s main goal was to use the configuration management and software vulnerability
scanning capabilities of Halo to harden its servers. The organization found that Halo included a number of standard security policies that allowed it to get up and running quickly. Avatar soon added its own very specific policies.

Today, Avatar New York has all of its public cloud servers protected by Halo around the clock. The IT team can automatically spin up new servers within minutes, and ensure that all of them are secure. “We wrote Puppet scripts so that every new server is automatically protected by Halo right from the start, without any manual intervention,” Tully explains.

One of the challenges of relying on third-party infrastructure for Avatar New York is a lack of visibility. Some of Avatar’s customers have very specific questions regarding compliance, policies and security. “When you are running more than 50 servers in the cloud, it is hard to do it without an automated system,” Tully says. “Halo helps us make sure that nothing gets overlooked. It is our way to constantly monitor and audit our systems and policies.”

Avatar is interested in rolling out an API integration with Halo Professional as the next step. The API will play a major role in Avatar New York’s infrastructure going forward.

CONCLUSION
In summary, it is critical that companies understand their responsibility when it comes to securing their public or hybrid cloud environments. They need to review the related risks and implement security controls that are well adapted to the dynamics of the cloud. Once IT management has addressed these security issues, public IaaS will become a standard component for implementing agile and scalable computing with hybrid cloud-hosting models.

“It is critical that companies understand their responsibility when it comes to securing their public or hybrid cloud environments.”