

Security In The Cloud

Ensuring The Security Of Applications & Data Can Be A Roadblock To Widespread Cloud Adoption



There seems to be no stopping the move to the cloud. But as many enterprises begin to consider the move to cloud computing, the biggest concern is security, and many data center managers

are not yet willing to pass near-complete control of a process over to someone else. So what are the biggest security-related problems when it comes to cloud computing? How do data center and IT managers overcome those problems? How safe is your company's data?

■ The Real Issues

Scott Morrison, CTO and chief architect at Layer 7 Technologies (www.layer7tech.com), says the biggest security-related issue is not understanding the real ramifications of transfer of control over to a provider. "Basically, you are handing over all management of low-level networking to another party to realize the benefit of commoditization of infrastructure and the human resources who run it," he says. "The problem is that, too often, people in enterprise IT don't recognize the degree to which their security model relies on local control, visibility, and perimeter defense."

Cloud challenges these assumptions and reveals the shortcomings of the current model, says Morrison. "At best, cloud is an important wake-up call about the need for comprehensive application security. At worst, enterprises moving into the cloud ignore the issues and deploy vulnerable applications into the cloud," he says. "The latter is the single biggest risk that cloud represents—that is, not rethinking how security must be done differently in the cloud and naively assuming that you can simply move existing applications and/or security models into the cloud unchanged. The cloud isn't a private data annex waiting for you and only you. It's a multitenant environment with a number of new risks and unique challenges."

Dean Trumbull, vice president and chief operating officer for Global DataGuard (www.globaldataguard.com), says security is by far the biggest issue that enterprises face when deciding to move to the cloud. Trumbull says the outsourcing of an infrastructure to cloud computing providers, though financially compelling, does not obviate the need for customers to secure their applications, content, and data and

Key Points

- Enterprises considering a move to the cloud need to remember that they are transferring control of their applications to a third party and plan their security accordingly.
- The process of moving applications to the cloud may have a side benefit of shining a light on current inefficiencies or shortcomings in an enterprise's security policy.
- Cloud security concerns will eventually lead to improved security applications and processes that help SMEs better secure data, address compliance, and work with best practices.

meet regulatory compliance. “When you look at the absence of robust SaaS (software as a service) security services such as intrusion detection and prevention, vulnerability management, threat management, log management, and access control, there is an obvious gap that must be closed before enterprises are able to move forward,” he says.

Morrison agrees. “This is born out in nearly every survey done looking at what are the inhibitors to cloud adoption by the enterprise,” he says. “The trust model for the cloud is significantly different from a classic hosting provider and requires careful consideration of the issues and technology involved.”

■ It’s All About Control

As for managers and their willingness to pass the control, Trumbull says there appears to be a bit of a disconnect between the cloud providers claiming that their networks are safer and more secure than most CPE (customer premises equipment) environments and the companies needing to secure their content and data with more than just virtual firewalls. He says most IT managers understand the requirements to secure deployed applications and meet regulatory compliance. “Truth be told, the security industry is behind the curve with respect to SaaS security services,” Trumbull says. “This absence of mature SaaS security applications is creating a potential overhang in terms of broad cloud computing adoption.”

As far as Morrison is concerned, passing control makes IT and data center managers realize the limitations of their existing security models, which rely so much on local control, existing processes, physical security, and perimeter firewalls. “This is completely at odds with cloud, where all of this is delegated to another party who cannot guarantee the same degree of physical isolation,” he says. “Cloud forces you to approach security differently from the ground up, and this scares people. Security is complex and the price of failure is high.”

■ Overcoming Obstacles

Morrison says that in order to overcome security-related issues, it is critical to understand where you can—and cannot—assert control in a cloud environment. He says you need to claim ownership and assert control where it is practical. “These opportunities for control in the cloud are few, but they do exist,” he says. “However, you may need to think differently about what it means to secure and control applications and data in the cloud.”

Morrison adds, “A cloud-deployed instance must be hardened both at the OS level and the application itself because you must assume it will be under continuous attack. Then you need to assert control over your hardened application instances by controlling all communications in or out of the image. This is the key new control point that is crucial in the cloud but was often overlooked in the on-premises enterprise network.”

According to Trumbull, the limitations and restrictions placed on cloud computing customers are leading to a new breed of SaaS security applications that are required to

address the full complement of security requirements imposed by regulatory compliance security standards and commonly adopted best practices. “Specifically, traditional network security products will need to transition from CPE appliances to SaaS security services designed to operate within each customer’s cloud account,” Trumbull says. “In this manner, SaaS security services will complement and overlay security services offered by cloud providers while offering customers the ability to mix and match security services to address unique regulatory compliance requirements.”

To be successful in the cloud, Morrison says you need to rethink many traditional aspects of application architecture. He says you can’t just use a classic castle wall-like perimeter defense model; you need to take an approach where the focus is on securing services, not networks. “The former you can still do in the cloud; the latter has been surrendered to your provider,” he says. “Understand the new boundaries of control in the cloud and how you can use these to your advantage, and you will be successful in the cloud.” ■

by Chris A. MacKinnon