Pipeline
Technology for Service Providers.
www.pipelinepub.com Volume 8, Issue 9

Safe and Sound:
Security and Reliability in the Cloud

By Tim Young

The thing about hype is that, sooner or later, it's time to put-up or shut-up. That time, it seems, has come for the cloud.

Here in the U.S., the National Institute for Standards and Technology (NIST) has published its final, official definition of cloud computing, after 15 previous iterations. This "model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources" is more than just web-apps and off-site storage. It's a definition that characterizes a baseline for cloud computing against which agencies and potential cloud adopters can judge so-called "cloud" services.

By having this standard against which to measure services, according to NIST computer scientist Peter Mell, "They are more likely to reap the promised benefits of cloud--cost savings, energy savings, rapid deployment and customer empowerment."

And if major government bodies are getting hip to the cloud, given how quickly they are known to move, it must be ready for prime time. And that's certainly the hope of the online retailers, software firms, and CSPs that have entered the cloud fray.

One CSP that has hitched its wagon to the cloud in a particularly big way is Verizon. The telecom giant picked up Miami-based cloud provider Terremark International a year ago (for a cool $1.4 billion), and doubled-down on cloud with its acquisition of cloud software supplier CloudSwitch in August, 2011.

It's no surprise that Verizon has invested so much time, money, and energy in cloud services, given their expectations for the growth of the market in years to come. Key players in the company's cloud strategy, including then-president of the company's Terremark unit (and current Verizon Enterprise Solutions CMO) Kerry Bailey, told the press late last year that they expect the market for cloud computing services to grow from $10 billion to $150 billion by 2020. Bailey told Bloomberg that $90 billion of that growth should come over the next four years, making even Verizon's multi-billion dollar cloud gamble seem like a strong bet.

Other forecasts for cloud growth have been similarly optimistic. IDC recently predicted that cloud spending would balloon to $73 billion by 2015, with half of that spend coming from U.S.-based businesses. AMI Partners pegs cloud services spending by that same year at $49 billion for U.S. small and medium businesses, alone, which could mean even larger numbers globally and across all business types.

50 billion. A hundred billion. A zillion kajillion. I'm no market forecaster and the real numbers aren't really the point. The point is that the market is growing and cloud service providers stand to make a solid profit as it does.

Doubts Persist

However, even those bullish on the cloud realize that there are serious concerns on the part of potential cloud adopters that have hampered adoption to this point, and that haven't been fully answered.

A survey conducted last summer by security software giant Symantec asked 3,700 executives from 35 countries about their plans to move business-critical initiatives into a cloud environment, and the concerns that accompany such plans.

Among other revealing questions, the survey asked respondents from enterprises that had already engaged in server virtualization if there were aspects of the process that made anyone in the organization feel less than confident in the process of placing these mission-critical applications in the cloud. An overwhelming majority reported that some at their organizations did have just such concerns.

Seventy-six percent of respondents reported that some had security concerns about the virtualization, and an equal number reported performance worries. However, it was reliability that was the number one concern, with seventy-eight percent of respondents reporting jitters about data availability and uptime.

These concerns overwhelmingly came from C-level execs who may or may not have a clear grasp on the practical realities of server virtualization. Symantec's survey found that the IT personnel at these same companies reported, for example, 78 to 85 percent completion of performance goals. It's not IT, however, that writes the checks or green-lights the virtualization process, so there's much to be done yet to reassure the higher-ups and iron out very real security, reliability, and performance concerns that persist.

Cloud providers can go a long way towards assuaging reliability fears with proper SLA management.

Down Time

After all, stories of the cloud gone awry are easy to come by and, rightly or wrongly, give all cloud a bad rap.

Amazon Web Services, the cloud's 800-pound gorilla, sports a history of reliability that's nothing to sneeze at, but its EC2 outages drew far too much press attention to be easily dismissed. Furthermore, Amazon admits that data was permanently lost in the outage. And while the amount of lost data (0.07% of the data on the company's US-East Region servers) doesn't amount to much, relatively speaking, but is certainly enough to give the already-skittish pause. After all, what if that data had been your data? It could include sales history and contacts, valuable code, or simply precious memories that were thought to be safe and secure, protected from on-site data loss.

And Amazon is certainly not alone. Microsoft has had its share of issues with its Office 365 productivity suite, leading the snarky to dub it "Office 364". In addition, Salesforce.com, often held up as one of the poster children for a cloud concept that works, has its

share of online detractors who blast the service for downtime and unscheduled maintenance.

Cloud providers can go a long way towards assuaging reliability fears with proper SLA management. Typical service level agreements for cloud providers offer guarantees of 99+ percent uptime, with partial service credits available if those benchmarks aren't met. In Microsoft's case, their outage in the UK brought their uptime below their touted guarantee (marketed at 99.9 percent), leading the Advertising Standards Agency (ASA) to investigate complaints from customers who called the software behemoth's marketing misleading. So these claims are taken seriously and bolster customers' intrepidation to move to a cloud environment or entrust a third party provider to manage their cloud infrastructure.

However, it's worth remembering that no on-premise server is immune to crashes or downtime, either, and the redundancy offered by cloud storage or other cloud computing and virtualization offerings may help to avoid many types of permanent data-loss or frequent server downtime. At least, in theory.

Keeping Clouds Within Reach

However, one of the problems with clouds is that you have to be able to reach them and they are only as good as the (third-party) connectivity upon which they rely. This places a great deal of faith in the last mile, which is not always up to the task of allowing access to mission-critical applications. As a recent Ovum report points out, a crowded hotel full of business travelers all attempting to use wifi to access a key application or bit of sensitive data creates the sort of bottleneck that stymies cloud efforts, even if the servers are working at a tremendous clip.

And this is an area in which the CSPs can leverage their network know-how to create a reliable cloud offering that may be beyond the abilities of some of the other major cloud players. Ovum notes that Portugal Telecom is among the providers who view the cloud-motivated ongoing need for bandwidth on the access network as a business opportunity that stems directly from the cloud push. And for CSPs who have been particularly active in marketing their cloud services, from BT to Tata, the ability to offer both the reliable access network and the cloud services to which that network allows access is a considerable advantage.

The Security Concern

Then, of course, there's the security question. Despite reminders that even on-premise databases aren't immune to fraud or malice, there's something disconcerting about putting sensitive data and critical applications out in the ether, where they seem all-too-susceptible to wrongdoing. Of course, that doesn't stop major enterprises from leveraging the low capex and high redundancy of the virtual environment.

There's something disconcerting about putting sensitive data and critical applications out in the ether...

Gartner estimates that by the end of 2016, more than half of Global 1000 companies will have placed customer-sensitive data in the public cloud. Furthermore, there are a number of enterprises who may think they have side-stepped this frightening world of public clouds by opting for a "private cloud." But as Gartner's Lydia Leong points out on her blog, many customers think they've gotten their hands on a private cloud, even when they have done no such thing. A number of supposed private clouds actually use a multi-tenant shared resource pool model, and a number of "public cloud" resources have what amounts to private connectivity, rendering the separation far less clear than some providers would have their customers believe. The fact is, unless it's a closed network, it's a public network.

Public or private, there are a number of paths to increasing the security of a cloud environment, of course.

There are a number of handy tips available for virtualization security available through the Cloud Security Alliance, of which companies from AT&T to HP to Oracle to Telecom Italia are members. Hypervisor introspection can detect even tricky bugs like kernel level rootkits. Host-based security, meanwhile, secures each virtual machine. Data can be encrypted at the file level before it enters the wider network. The code for boot OS and hypervisor can be kept as small as possible to create a tiny attack surface for malware. In these and many other ways, security can be baked into the process. In addition, tools like hash value verification can ensure that data remains uncorrupted and complete throughout the process of virtualization.

In addition, Gartner estimates that by 2016, 40 percent of enterprises will make independent security testing certification mandatory for any type of cloud service.

Opportunity Knocks

Therefore, just as service providers are presented

with an opportunity for facilitating and offering cloud services, backed by a level of network visibility that many other cloud providers can't match, there is also an opportunity to make this cloud access as secure and resilient as possible as a competitive differentiator.

Vendors are clearly aware of the opportunity to help CSPs accomplish these goals. In fact, as I was writing this article I received a news alert that cloud software company Joyent just raised $85 million to pursue global growth, with the tackling of those three top concerns among executives I stated earlier (performance, security, and reliability) mentioned as their main missions.

Likewise, any number of OSS and BSS providers have extended their solutions for service assurance, SLA management, billing, and other key applications to cover the emerging cloud services market. Heck, many have even begun offering their software platforms as a managed service through the cloud.

There is also an opportunity to make this cloud access as secure and resilient as possible.

In short, vendors and providers, alike, are putting up, and the struggle to provide a reliable, secure cloud continues. Like any nascent technology, the road to the cloud is fraught with challenges, but as end-users are, increasingly, able to see the benefits of the cloud's possibilities and, more importantly, cloud providers are able to prove that they are capable of realizing those possibilities, gains are made. After all, dangers exist for all centralized computing and storage solutions. But where there is danger, so too is there opportunity.