2010 EXECUTIVE REPORT

How Real Are Cloud Security Concerns?

Separating Fact from Fiction for Infrastructure-as-a-Service (IaaS) Cloud Computing

HOSTING.com

ITBUSINESSEDGE
YOUR TECHNOLOGY INTELLIGENCE AGENT

How Real Are Cloud Security Concerns?

Separating Fact from Fiction for Infrastructure-as-a-Service (IaaS) Cloud Computing

Infrastructure-as-a-Service (IaaS) cloud computing has very quickly grown from an exotic concept to a known solution, with countless successful implementations ranging from small businesses to global enterprises. However, concerns remain about some aspects of IaaS clouds, and security is at the top of the list. In a recent survey by Forrester,[1] 51 percent of those queried cited security as their top cloud-related concern.

Part of this concern is a predictable reaction by naturally (and appropriately) conservative IT managers to *anything* new in technology. But the lion's share of concern stems from confusion and less-than-clear thinking and writing by journalists, commentators and industry analysts. Some of these commentators have faulted IaaS cloud security for vulnerabilities that exist in *every* IT implementation, regardless of architecture.

The fact is, when properly managed and configured, an IaaS cloud can be as safe and secure in the areas of greatest concern—data integrity, protection from theft, back-up/recovery and regulatory compliance—as any in-house solution running on dedicated servers. This briefing will address some of the sources of confusion as they apply to IaaS implementations and then outline the practices and technologies available to keep clouds safe in the areas where they do have unique vulnerabilities.

Sources of Confusion

One source of confusion about cloud security is the existence of three different models for the delivery of cloud technology:

- Software-as-a-Service (SaaS) uses cloud computing to deliver a specific application (like salesforce.com) over the Internet.
- Platform-as-a-Service (PaaS) is a cloud-based development environment (such as Google App Engine or Microsoft Azure) where customers can build their own applications that run on the provider's infrastructure and are delivered to users via the Internet.
- Infrastructure as a Service (IaaS), as its name implies, provides customers with a complete Internet-accessible infrastructure including processing, storage, network bandwidth, and other resources upon which they can run multiple operating systems and applications.

Providers in the IaaS category include Hosting.com, GoGrid and FlexiScale. A surprisingly large number of technical articles attribute issues that exist in only one delivery model to *all* delivery models, creating unnecessary confusion, particularly in the minds of nontechnical evaluators.

A second and more important source of confusion is the collection of articles, blog posts, and white papers that talk about vulnerabilities that are common to *all* IT architectures as though they were unique to clouds. In fact, the vast majority of potential cloud vulnerabilities are similar, if not identical, to those found in IT architectures across the board. Following are the key issues that fall into this category.

Threats: Real, but Not Cloud-Specific

Personnel Issues. Perhaps the most egregious example of treating generic security issues as though they were cloud-specific has to do with personnel. The complaint that with a cloud "you don't know who has access to your data" could be equally applied to literally thousands of third parties that process financial data for banks, credit card

[1] Carl Brooks, "Are Cloud Computing Vendors Ignoring IT Pros' Concerns?" SearchCloudComputing.com, http://searchcloudcomputing.techtarget.com./news/article/0,289142,sid201_gci1376086,00.html?track=NL-1329&ad=738675&asrc=EM_NLN_10219632&uid=205614

companies, retail chains and so forth on a daily basis. Companies engaging a cloud computing service will obviously want to feel they can trust the personnel handling their data. This is equally true for *any* business partner that has access to sensitive data, whether it is related to IT, purchasing contracts, HR or any other business function.

Physical Security. This is another issue that applies to any computing environment. Obviously, physical access to servers, storage units, and so on should be monitored and controlled, but the fact that the servers are part of a cloud in no way exacerbates this risk.

Privileged User Access. In a cloud, access can be controlled via passwords on an individual basis, by group, by function, or all three, just as with any application running in a dedicated server environment. Some cloud providers address the issue of privileged user access at *both* the Active Directory and VMware vCenter level, allowing administrative access on a temporary basis only and collecting login data for specific virtual machines within the cloud. These measures are actually more stringent than those in place with many dedicated solutions.

In the case of a terminated employee, an appropriate process must be in place for HR (or the employee's supervisor) to promptly notify IT so that permissions can be deleted before any harm occurs. Again, there is no difference between a cloud and a dedicated environment.

End User Access. In an era where end users access corporate applications and databases from airports, cafés and other public locations via WiFi, the risk of data theft is genuine, and password protection by itself may not be adequate. However, the means for enhancing the protection of data—encryption and the use of Virtual Private Networks (VPNs)—are available to clouds just as they are to on-premises applications. On the subject of passwords, there is no reason why a single sign-on capability can't be implemented to provide users access to cloud and non-cloud applications.

Investigative Support. Twenty-first century IT organizations must be prepared for an unprecedented level of scrutiny related to litigation or potential criminal activity. Cloud technology can provide logs at the physical node level (for example, user login to a console controlling a physical cluster) or at the level of individual virtual machines (such as the modification of files or a security group). This technology has been tested and proven satisfactory in actual investigations.

Backup and Recovery. Cloud technology allows both sector and volume-based backups; these backups can be done to an off-cloud storage solution to further ensure security. Best practices demand that the cloud platform should be replicated on a Storage Area Network (SAN).

In sum, for many security issues, the problems and solutions in an IaaS cloud are similar if not identical to those found in a conventional IT implementation with dedicated servers. In many cases, cloud security is arguably stronger. However, in some instances, clouds present unique challenges. These are discussed next.

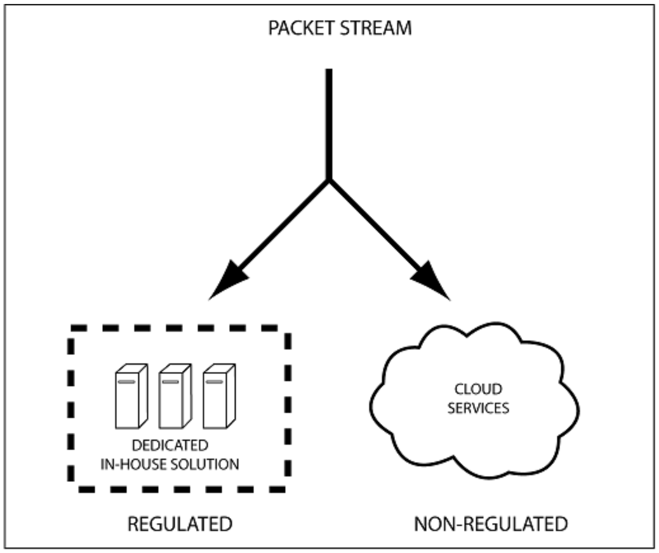
Cloud-Specific Security Challenges

Intrusion Detection. This is one of the more hotly debated issues related to cloud computing. In a conventional architecture, a firewall controls access to corporate IT assets at the front door. In a cloud implementation, security operates at a more granular level. Firewalls can be provided at the level of the individual server if desired (typically at an additional cost). In addition, a variety of security applications are available to protect against attacks such as SQL injections.

Data Location. This is another area where cloud computing presents unique challenges. Alarmists often state that with clouds, "your data could be anywhere"; and depending on the provider, this could be true. On a day-to-day basis, this fact has no importance; but it can become extremely important when situations arise that could potentially block access to your data, such as a financial dispute or bankruptcy on the part of the provider. If your data is physically located in China, for example, then your efforts to gain access to it will most likely be governed by Chinese law, a fact that is sure to make the process more expensive and time-consuming.

This challenge can be met by insisting that data be physically stored only in locations—or to be more precise, legal jurisdictions—that you approve. Many providers are willing to guarantee that data will be physically located in a specific country/legal jurisdiction, and this eliminates the primary security risk associated with data location.

Regulatory Compliance. Achieving compliance with standards such as Graham-Leach-Bliley, Sarbanes-Oxley, HIPAA and the Payment Card Industry Data Security Standard (PCI/DSS) is one of the most challenging issues related to cloud computing. The primary reason compliance is so difficult is that all these standards were written at a time when it was assumed that one-server/one-application deployments were the rule, and that servers were under the physical control of the entity running the application. This is obviously not the case with cloud computing.



When regulatory compliance is a concern, a hybrid solution that includes both dedicated servers and cloud services can be employed to achieve compliance while benefiting from the efficiency and cost benefits of cloud computing.

There are providers within the industry who argue that compliance is possible for a cloud solution with the appropriate management and configurations, and some providers have indeed achieved PCI/DSS certification. Cautious customers, however, may be wary of entering into business relationships where legal precedents are either lacking or murky.

The fact is, any committee of corporate lawyers is likely to veto cloud computing when sensitive data is involved. This does not necessarily mean that regulated companies cannot enjoy any of the benefits of the cloud. Some IaaS providers have dealt with the compliance issue via hybrid solutions that incorporate dedicated physical servers where they are necessary to meet compliance requirements, while utilizing cloud computing for nonregulated business processes. A private cloud can also be a component of a hybrid solution, providing seamless integration into a cloud environment.

To summarize, IaaS clouds do present unique challenges related to three important security issues—intrusion detection, data location and regulatory compliance—but these challenges can be easily met through a combination of cloud-specific technology and best practices.

Economies of Scale

With all the media focus on cloud security issues, an important point has been overlooked: For many small and medium-sized organizations, service providers using cloud computing may be able to offer security superior to what those organizations could provide for themselves. For example, in many cases, organizations with small IT departments have firewalls installed by value-added resellers (VARs) on a set-it-and-forget-it basis. When new requirements arise, such as providing selective access to VoIP services, the IT department may lack the resources or the skill set to respond. In more robust (and more expensive) environments, functions like these can be managed automatically.

Another example is approaches to intrusion. Small companies are likely to have an intrusion *prevention* system where the rules are predetermined by an administrator. But few can afford a level of monitoring that informs administrators about problems from active, targeted attempts to penetrate a firewall *as they arise*.

In an IaaS cloud, the cost of security is amortized over multiple customers just like everything else, making some security measures affordable that would otherwise be out of reach.

Conclusion

In spite of hype to the contrary, the vast majority of security issues that arise for IaaS clouds are identical to those encountered in conventional implementations. The few issues that are unique to clouds can be handled with a combination of technology and simple good management. IT organizations interested in IaaS cloud computing should of course proceed with caution, but they should definitely proceed.

This IT Business Edge Executive Report Sponsored by

HOSTING.com

Hosting.com is a global provider of enterprise-class IT infrastructure solutions, services and facilities. Hosting.com’s geographically-dispersed data centers and Cloud Super Sites coupled with the industry’s top networking and connectivity technologies provide clients with the highest levels of security, reliability and support. The most recognized names in Retail, Financial Services, Healthcare, Government, Technology and Web 2.0 rely on Hosting.com’s colocation, cloud hosting, dedicated and managed hosting solutions.

Hosting.com’s Cloud Hosting infrastructure recognizes a business’s evolving needs and reacts instantly to provide production-ready infrastructure on demand. Technology alliances with VMware, EMC, Dell, Intel, Juniper, F5 and others enable the most secure and flexible enterprise-class cloud.

For example, clients demanding high levels of application security or regulatory compliance utilize Hosting.com’s Cloud Dedicated solution (single tenant) to store sensitive applications and records and utilize Cloud Enterprise for additional compute resources for non-sensitive assets.   Hosting.com’s migration expertise and integrated platform for all solutions allow clients to create hybrid hosting solutions to meet their specific business and security needs.

Hosting.com utilizes a custom provisioning process and robust platform that allows clients to connect and use the following cloud solutions:

- Cloud Enterprise (Multi-Tenant)
- Cloud Dedicated (Single Tenant)
- Cloud VPS (VPS on Steroids)
- vCloud Express (Utility Billing, Developer Centric)

Specific businesses finding value on Hosting.com’s cloud platform include those:

- Collecting, processing and storing client transactions.
- Requiring flexible, secure infrastructure to support back-office applications.
- Seeking a scalable infrastructure to meet changing client demands.
- In need of a project-based infrastructure on a VMware platform that integrates with their internal infrastructure.

IT Business Edge

IT Business Edge delivers the information, analysis and context business technology decision makers need to maximize returns on IT investments and align IT initiatives with business objectives. As a Technology Intelligence Agent, IT Business Edge provides content different from that of a traditional IT publisher, news service or analyst firm. Our editors monitor all these sources—plus many others—for critical IT information that they translate into actionable advice for high-level IT and business managers. Subscribers access our practical content and useful decision-making tools through a rich Web site, targeted e-mail newsletters and varied RSS feeds. All these outlets feature our business-focused blogs, exclusive interviews with field experts and industry insiders, plus our database of more than 20,000 abstracts summarizing content from 2,500-plus sources. Visit our Web site at http://www.itbusinessedge.com.

About the Author

Mike Stevens began his career as a technical writer in semiconductor manufacturing and then switched to marketing. At his own Silicon Valley-based agency, he worked with an impressive list of clients, including HP, EMC, Fujitsu and Microsoft. His primary focus for the last seven years has been enterprise software.