Mix, match and burst. New infrastructure-as-a-service tools make it easier to shift among multiple private and public clouds.
**Creating a View to the Cloud**

How well can you see into the cloud? For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

**Securing the Keys to the Cloud**

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.

**Mexican Hotelier Opt for Texas Data Center**

For many IT professionals, the view isn’t very clear, but new techniques and tools make visibility across multiple cloud initiatives crisper.

Cloud providers claim they can secure your company’s data, but as the software-as-a-service model is put to the test by more and more organizations, security holes and malware are coming to light. Here’s a guide to better cloud security.
Like many young data-driven companies, BuildFax decided in 2008 to host its construction data services on Amazon Web Services. But now, it’s moving some systems to Google’s new infrastructure-as-a-service (IaaS) offering, some to other cloud providers and some to its first in-house servers.

Gettin’ and burst. New infrastructure-as-a-service tools make it easier to shift among multiple private and public clouds.

By Robert L. Scheier
Some people treat the cloud as something separate — they have a separate hierarchy of users (that) doesn’t map to the hierarchy they have in-house.  

SHIRIRAM NATARAJAN, SENIOR DIRECTOR, PERSISTENT SYSTEMS

Companies with extensive data analysis needs make up a strong IaaS market, says Terremark Worldwide’s ELLEN RUBIN.

BUILDFAX’S vp of research and development, Joe Emison, says he was at first delighted with Amazon’s pay-as-you-go model. But he soon wanted a choice of public and private clouds so he’d have flexibility to use the best performance and disaster recovery options as his needs changed — and as computing technology and the capabilities of IaaS providers changed. “You can take advantage of the benefits of the cloud without losing sight of what’s on Amazon” — or any other provider, he says.

That viewpoint is slowly gaining traction as the IaaS business model grows beyond serving only smaller organizations and supporting less-critical systems such as development and testing. But becoming cloud-agnostic requires new thought during selection. “Users must design applications that can survive the unpredictability of the cloud, and they have to ensure proper security.”

Companies with extensive data analysis needs make up a strong IaaS market, says Terremark Worldwide’s ELLEN RUBIN.

The Role of IaaS

In the alphabet soup of the cloud, IaaS is the service that gives customers the greatest access to — and control over — servers, storage and networks, with options that include a choice of operating system and drivers, says Andre Pino, vice president of operations for a platform-as-a-service (PaaS) provider. But it also requires customers to do much of the “low level” work they do with in-house systems, he says, noting that users must provision physical servers and dynamically update load balancers whenever clusters are modified.

PaaS, the next level up, provides frameworks of software and processes that ease application deployment. The highest-level cloud option, software as a service (SaaS), provides a complete application over the Web. The “higher” a cloud service the customer buys, the less work its own staffers must do. On the other hand, says Pino, “if you’re going to provide a full set of services such as computing, storage, sometimes it’s milliseconds, other times hundreds of milliseconds, to get the same data,” says Ken Pepple, vice president at Cloud Technology Partners, a Boston-based cloud computing consultancy. (Amazon declined comment for this story)

Secure Enough?

Concerns about sharing servers, storage, and networks with other organizations, or buying software from many users from a single provider, are among the many fears away from IaaS. But most observers agree that, with proper care, IaaS can meet even strict security requirements, and the security picture is likely to improve as IaaS providers gain experience. For example, Sonian, a Newton Mass.-based provider of email and document services, recently completed a Federal Information Security Management Act (FISMA) audit of more than 300 controls analyzing how Sonian software operates on the Amazon cloud. “We met the highest standards out there,” says CTO Greg Arnette.

As with in-house data centers, most security problems in the cloud are caused by users who ignore the rules or operational status such as misconfigured networks, says Pino. IaaS providers such as India’s HCL Technologies offer multcloud governance frameworks that can provide granular access controls and configurable rules and policies for users across multiple clouds, said Sadagopan Singam, HCL’s global vice president of cloud computing. Before moving to the cloud, customers should decide how to organize their security groups, change default server configurations to restrict access to authorized users, and map their internal security and access control models to the cloud with tools or the services provided. “Anybody who has a cloud environment and doesn’t have a separate virtual LAN, he says, and for virtual machines to have one interconnect, doesn’t map to the hierarchy they have in-house,” says Natarajan.

In fact, some observers say IaaS is so inexpensive and flexible is that many customers share a vendor’s resources, so performance isn’t guaranteed — it can rise and fall based on the demand from other customers. That could happen, if for example, “the guy sharing my server [is] streaming music and hogging the server,” says Monochel Michaluv, CEO and co-founder of data management vendor ScaleIO. If latency causes an IaaS application to fail, the system should alert an administrator and resume work when another server comes online without manual intervention or lost transactions. Emison says that BuildFax has seen “going to fail” and architect systems so that it’s easy to provision another from the “infinite pool” available in public or private clouds. Using RightScale, Emison says BuildFax can automatically create a cloud-based server that can, for example, access a file of building permit data, “extract all the data into a text file, load it up into a database and self-teardown. If it dies in the middle of the process, it spins up again.”

Using a service-oriented architecture abstracts services from the hardware, creating an asynchronous environment that less depends on specific platform choices. “Many observers stress the need to avoid a single point of failure — a need highlighted by well-publicized outages at Amazon Web Services. In a recent blog post, Todd McKinnon, CEO of Okta, said he chose IaaS for his company’s cloud-based identity management service because it forced him to avoid “supposedly ‘highly available’ components like expensive load balancers and shared state, clustered databases.” However, he says, some of the IaaS providers he has worked with can tell him whether, for example, two virtual machines share the same physical server. That’s why McKinnon says IaaS customers still “will need someone in-house” to ensure that their systems are architecturally correct.

Many IaaS providers make it difficult to avoid single points of Scale to quickly move those workloads to public clouds if needed. Sonian users IaaS to run the all-important search capability it provides to users, but it uses a Saas offering for its less critical relational database. While Amazon has a Paas search option, Arnette says he chose IaaS “because we would have more control over the design of that very critical feature.”

Robert Jenkins, CTO and co-founder of cloud vendor Cloud-Sigma, says his company has an e-commerce customer that “keeps the core database in their own infrastructure” and spins up public cloud servers when needed. He notes that “we could probably [also] move their data into our cloud efficiently,” but the company also has too many of its company data to take that step.

Moving to a multicloud world requires not only thinking through risk-benefit trade-offs, but also changing application architectures and IT processes.

Best Practices

In-house data centers include servers, storage and networks that provide certain levels of performance and reliability. One reason IaaS is less appropriate for applications with steady, predictable power for short, intensive analysis, says Ellen Rubin, vice president at Cloud Technology Partners.

In contrast, those services cost more and customers who use them today can at least have a separate virtual LAN, he says, and for virtual machines to have one interconnect, doesn’t map to the hierarchy they have in-house.”

The Power of Admiral Technologies is here.

Let’s call you “Cloud Master.”

Discover how
Security Questions for Your IaaS Provider

Here are eight tough questions to ask when vetting prospective IaaS providers, courtesy of security professionals Eric Chiu, founder and president of HyTrust, and Gerhard Eschelbeck, CTO of Sophos.

1. Is each customer’s data encrypted with a unique key?

2. Does each server have a unique encryption key?

3. Can you provide audit log details of all changes to the virtual infrastructure and virtual machines? And can you integrate that data with your security information and event management software?

4. How do you authenticate users in the public cloud back to my enterprise directory?

5. How do you ensure that potentially dangerous root and local accounts aren’t being used? If they are, can you provide detailed audit trails of who used those accounts and what they did?

6. What strong authentication products do you enable in your service offerings?

7. How do you ensure your administrators can’t make unauthorized configuration changes such as connecting one of your virtual machines to another company’s network?

8. Can you provide a report from a qualified security assessor proving that you comply with regulations such as those of the Health Insurance Portability and Accessibility Act, the Federal Information Security Management Act and the Payment Card Industry Data Security Standard?

---

provisioning, migration and management of workloads, he says.

Embotics, a provider of private cloud management systems, targets midsize companies with what it calls “a comprehensive set of virtualization and private cloud management capabilities in a single, integrated software package that can be implemented within one hour.”

Another IaaS vendor, TransLattice, uses a protocol that splits the database and associated components such as queuing systems across a network of commodity servers, says CTO Mike Lyle. That protocol, he says, ensures that all the tasks are completed in the proper order, and even handles the locking of transactions of distributed databases.

The Red Hat Hybrid IaaS Solution blurs the boundaries between IaaS and PaaS offerings with cloud-orchestration tools, a self-service portal for users, a virtualization manager, a hypervisor and a guest operating system, as well as the option to add prepaid compute hours from major public cloud providers. Its recently announced Red Hat Storage Server 2.0 will use Red Hat’s Gluster file system to replicate and distribute data among multiple public and private data centers, says Bryan Che, senior director for product management and marketing.

Last summer, Verizon acquired CloudSwitch, whose software, running either in the customer’s data center or in the cloud, is designed to ease the synchronization of data and workloads among public and private clouds, says Terremark’s Rubin. Cloud management software vendor RightScale recently acquired a cloud cost-forecasting website called ShopforCloud to make it easier for customers to calculate the costs of a variety of cloud options.

What’s Next?

As IaaS becomes more commonly accepted, providers are looking for ways to differentiate their offerings for specific workloads, regulatory requirements, vertical industries or even geographies.

Cloud marketing firm Preview Networks in Copenhagen, Denmark, chose IaaS vendor CloudSigma in part because it has a European data center, enabling Preview Networks to comply with European Union rules dictating where customer data can be stored, says CTO Patrick Rodies.

Healthcare data analysis firm Wound Vision pays 79% more to IaaS provider BluLock than it paid to Amazon in part because BluLock provides more insights into the operation of its infrastructure and the location of sensitive medical data, says IT director Andy Hoover. “When you go into hospitals, with all the [data privacy] concerns, they want to know where [their] data is” and may even ask to tour the data center.

“That obviously wasn’t going to happen with Amazon Web Services,” but it’s possible with BluLock, he says.

Cloud Sigma has created a cloud-based network of partners providing services such as video editing, so customers in the entertainment industry can store and process their data without moving it from the cloud.

Other observers predict the emergence of combined offerings, such as the OnApp cloud management and content delivery network, Kosten Metreweli, chief marketing officer at OnApps, says such a combined approach provides more reliable data access, accessing servers to buy and sell excess capacity in a real-time marketplace.

Gartner analyst Lydia Leong predicts the major differentiating IaaS providers from one another will be the performance guarantees they offer. “Instead of just a best effort,” she says, customers will demand consistent and predictable service from vendors.”

Pino of CloudBees predicts that IaaS will be seen as too complex to use within five to 10 years and will be replaced by Paas and SaaS offerings. People even predicts a merger of IaaS and SaaS as the “lower levels of the technology stack” become more standardized.

However IaaS evolves, the day is rapidly approaching when the question won’t be which cloud to move to, but which combination of services to move to which mix of clouds as technology and business needs change.

Scheier is a veteran technology writer. He can be reached at bob@scheierassociates.com.
ONE MILLISECOND might not seem like a lot of time. But when you’re a software-as-a-service provider with thousands of databases running 2 billion SQL queries and pushing out 10 terabytes of SQL data each day, every millisecond adds up. Performance and visibility are crucial — especially when your systems are tied to those of other vendors that also operate in the cloud.

New techniques and tools are making visibility across multiple cloud initiatives clearer. By Stacy Collett
That’s the case at Concur Technologies, which each year processes more than $50 billion in travel and expense reports in the cloud. About four years ago, the Redmond, Wash.-based company started experiencing database call lags between its middle tier and the database tier. “It’s a problem that comes in once every million calls, and it could come from any one of 30 servers in one tier to 30 in another tier,” explains John Thrapp, lead software configuration engineer at Concur. “Getting visibility into that required three different layers of people — network DBAs, network engineers, application engineers — working together” is a time-consuming process. Last year, the company found a performance management tool with a monitoring focus that now helps the IT team identify issues quickly, and that’s critical to keeping Concur competitive.

“Speed of rollout, deployment and the innovation that’s required these days to compete require tools that will keep watch in real time, spin up resources as needed and diagnose problems right off the bat,” Thrapp says.

Performance and visibility in the cloud have become major concerns among users. Large enterprises have been moving well-understood workloads to the cloud for years. But as more mission-critical systems get sent to the cloud, and as the number of cloud applications run by a single company multiplies, it will become more important for visibility and performance management tools to follow your applications to the cloud.

Spending on public and private cloud services, and on building those services, will reach $66 billion this year, according to IDC, and the strategic focus in the cloud will shift from infrastructure to application platforms. So it makes sense that demand for tools that improve visibility in the cloud is growing. Spending on cloud management software will increase 62% this year, according to IDC.

“More visibility you have into what you can see, the better you can optimize your decision to use the cloud,” says Dennis Droegeth, a vice president at IT consultancy Enterprise Management Associates.

Deciding the best environment in which to run an application at peak performance is one of the biggest pain points facing cloud-adopting enterprises today, says Dennis Callaghan, an analyst at 451 Research. “They don’t really have good visibility into what the impact is going to be on their business if they move a particular application to the cloud,” he adds. “There’s no go-to set of objective criteria on how to pick a performance management tool in a hybrid cloud environment.”

Here are some guidelines for choosing tools that will improve your ability to see and manage systems in the cloud.

**CHOOSING A PROVIDER WISELY**

When building new applications in the cloud, it’s important to choose a cloud provider that has what you need — “one that gives you as much visibility as possible and can meet the metrics you’ve established,” says Dave Bartoletti, an analyst at Forrester Research.

“Maybe it’s compute performance. You’re building a big analytics application that requires a lot of computing horsepower and you want to confirm you’re getting all those CPU cycles that you’re paying for,” he says. “Or maybe it’s an application on the Web. Your performance metric might be whether he scales right away to meet load.”

When it comes to performance requirements and visibility, the “educated consumer” model prevails. Cloud users need to know what they want and convey their needs to the cloud provider.

“You, as the consumer, have to own it,” says Bartoletti.

---

**Building in a Hybrid World**

Companies that will run some of their applications on-site and some in the cloud require a higher degree of visibility from the cloud provider. “In this case, you want to look at what kind of APIs they provide to their performance management tools,” Bartoletti says. “You may want to download to their performance management information into your own existing system for that part of the app that you’re running on the site,” says Bartoletti.

Many cloud providers offer visibility and monitoring of their own performance, but industry watchers say it’s best to also deploy a third-party tool for accuracy. If the vendor has an in-house system for monitoring performance, says Bartoletti, “it might be hard to validate metrics.” You’re not going to get visibility into data upload and download performance, he adds. “But you should be able to validate performance spikes and see how your application is performing at different times of the day.”

A third-party tool will help validate the kind of load the cloud provider says it is seeing. It’s really about trying to match what the cloud provider offers to what you already do. That’s part of the buying process.

When parts of an application reside in-house and other parts sit in the cloud, it’s important to match key metrics both on the ground and in the air. “If you already are using a performance management tool in-house, what are the key metrics they’re tracking? That’s what you take to the cloud provider and say, ‘You’re going to have to give me at least this visibility into my load patterns throughout the day, my traffic spikes, my storage consumption, and I need to see that on a particular level of granularity — whether you’re tracking it in five-minute intervals or 30-minute intervals,’” says Bartoletti.

---

You’re not going to get visibility into data upload and download performance. But you should be able to validate performance spikes and see how your application is performing at different times of the day.

**Dave Bartoletti, Analyst, Forrester Research**
Speed of rollout, deployment and the innovation that’s required these days to compete require tools that will keep watch in real time, spin up volume as needed and [diagnose problems] right off the bat.”

John Tharp, lead software configuration engineer, Concur Technologies

“Even though this market has been around for a long time, it’s surprisingly immature,” says Jesse Rothstein, co-founder and CEO of ExtraHop. “People haven’t agreed yet on what solves the problem. That’s why this is a market that is ripe for innovation.”

The market is unbelievably crowded,” says ExtraHop co-founder and CEO Jesse Rothstein. “Even though this market has been around for a long time, it’s surprisingly immature. People haven’t agreed yet on what solves the problem. That’s why this is a market that is ripe for innovation.”

Rothstein says there are several key issues to keep in mind when choosing a performance management application. First, it must work in a dynamic environment. “Mimicking a cloud environment means a solution must have some type of auto-discovery and auto-classification of all resources — VMs, servers, databases, virtual appliances and storage — and must adapt to changing environments automatically,” he explains.

A performance management application should also have the ability to monitor the complete stack to get holistic visibility. And it must measure all aspects of application response time, not just resource utilization like CPU and memory. “Resource utilization does not equal response time,” says Rothstein. The system must also be easy to install and capable of being up and running in an extremely short amount of time, he adds, noting that “cloud and virtualization are all about speed and agility.”

Concur deployed a performance management tool from ExtraHop and can now track real-time performance of more than 2 billion SQL queries and 500 million memcache transactions each day — that represents a 20% improvement over the performance of its previous system.

Experts also caution against “cloud washing,” or rebranding existing performance management tools that are not intended for the cloud. “You don’t want to be trying to repurpose your existing management tools and running it on a cloud server,” Callaghan says. “It can weigh down performance. Go with something more lightweight and designed for these new environments.”

Ask for What You Want

It’s important to ask the cloud provider for the performance and service levels that you need in terms of throughput, response times and downtime, “and insist on it in many cases,” Drogerth says. If a cloud provider says that its standard service-level agreement meets your organization’s performance demands, you should validate that claim by running a test application. The challenge is to generate a realistic load, but that should be possible if the cloud provider offers load simulation tools.

Once the baseline for performance has been established, you should establish service-level agreements that define your organization’s performance expectations. “You should establish up front what the remediation process is if actual performance doesn’t equate what’s been promised,” he adds, “Is there a penalty system in place? Is there a set of refund or an extension of your services promised, he says, adding, “Is there a penalty system in place?”

While software-as-a-service providers have rigid service levels in the past, “SaaS in the cloud are still evolving,” according to Bartoletti. Amazon, for instance, has recently “taken great strides” in making its performance more visible through APIs and tools, he says. At the end of the day, the real benefit of tracking perfor-

performance with whatever tools the cloud provider can give you is that you can “right-size” your cloud investment, Bartoletti says. “You can get them right over time.”

Stacy Collett is a Computerworld contributing writer. You can contact her at stacy@zcoal.com.
As the cloud model is put to the test at more organizations, security holes and malware are coming to light. Here's how to cope.

By Bob Violino

business networking
site LinkedIn suffered a security breach in June that resulted in the theft of more than 6 million user account passwords, which were subsequently published online. Although the company says there were no reports of compromised accounts, the incident garnered headlines about the risks of the cloud.

And in April 2011, a server breach at email marketing company Epsilon Interactive exposed the names and email addresses of millions of people. The company said unknown intruders broke into one of its email servers and accessed the names and email accounts of some of its 2,500 corporate customers.

As these incidents show, the cloud is still very much a work in progress when it comes to security. Although many cloud service providers claim they can secure their customers’ data, security problems are surfacing as the technology takes hold at more organizations.

“More and more businesses are pushing information and services out to the cloud every day. Many are doing so without the slightest knowledge of what risks are lying in wait for them once they leave the sanctity of the existing data center,” says Mark Gilmore, president and co-founder of Wired Integrations, a technology consulting firm in San Jose.

There are several areas in which the cloud has security issues, says Dave Shackleford, a cloud security expert and certified instructor at the SANS Institute, a cooperative research and education organization in Bethesda, Md. “Most fundamentally come down to either application security or virtualization-specific issues,” he says.

Threats to cloud-based systems include so-called hypervisor escape, or “virtual machine escape” exploits. “There have been several recent vulnerabilities announced that could potentially lead to attackers executing code from a malicious VM and affecting the underlying virtualization platform at a cloud provider,” Shackleford says.

One in particular affects a number of 64-bit platforms, as outlined by the U.S. Computer Emergency Readiness Team. In June 2012, US-CERT reported that some 64-bit operating systems and virtualization programs running on Intel CPU hardware are vulnerable to a local privilege escalation attack. Privilege escalation involves exploiting a design flaw or configuration oversight in an operating system or application to gain elevated access to information resources that are normally protected from an application or user.

An attacker might exploit the vulnerability for operating system privilege escalation or for a guest-to-host virtual machine escape, the report says. The solution is to apply vendor-specific patches for the operating system or virtualization software.

The Risks Examined Another category of vulnerabilities relates to data storage and access failures, Shackleford says. Cloud providers will invariably leverage large-scale shared storage environments such as a storage area network or network-attached storage, he says.

“There are many configuration issues that could lead to illicit storage access, but new research into VMware virtual disks shows that an attacker could potentially create a virtual machine with a crafted virtual disk file that grants access to other parts of the storage environment,” Shackleford says.

Other examples of new threats that cloud environments face, he says, include denial-of-service attacks from systems in the cloud and cloud providers that are inadvertently hosting malicious botnet controllers.

Gilmore says he sees cloud security risk breaking down into two...
major categories: malicious attacks and malicious content. “Malicious attacks would be in the form of the cloud. “I didn’t really focus on vendors’ assurances as much as I did on my own research to verify the security of cloud providers,” says CIO Yousuf Khan. “The key thing is asking, What’s the criticality of the application, and have I done my homework when considering moving it to the cloud?”

The company uses Amazon.com’s Amazon Web Services across four geographic zones throughout North America for extra availability and security. It has used cloud services for several years for payroll processing, collaboration, customer relationship management and other applications. Other steps Alpine has taken include deploying a “firewall sandwich” to protect Web application servers and back-end systems. “This configuration is particularly important in the cloud, where back-to-back firewalls often exist at the boundaries of the service provider and enterprise network infrastructures,” Sadowski says. He says on- and off-the-shelf security technologies include multi-factor authentication and context-based authentication, which uses contextual information to help confirm a user’s identity.

Hult International Business School in Boston runs multiple applications in public and private clouds, including a learning management system, email, file storage and social media tools. The school’s IT department works with cloud providers and assessed its own security needs before moving apps to the cloud. “I didn’t really focus on vendors’ assurances as much as I did on my own research to verify the security of cloud providers,” says CIO Yousuf Khan. “The key thing is asking, What’s the criticality of the application, and have I done my homework when considering moving it to the cloud?”

Hult also uses security tools such as an identity and access management application from OneLogin, which enables users to go to a portal to be authenticated for access to applications in the cloud. Organizations that rely on the cloud need to build in expecta-

Violino is a freelance writer in Massapequa Park, N.Y. You can reach him at bviolino@optonline.net.

Tips for Better Cloud Security

1. Know your own infrastructure and that of your cloud provider.
   The less you know about the vendor’s setup, the more vulnerable you are.

2. Ask your security and legal teams to review contracts with cloud providers. Verify that security assurances are legally binding.

3. Study your provider’s service-level agreements so you understand all contractual obligations you and the vendor’s. Make sure that you can monitor your apps, and that the vendor will notify you in the event of a security breach.

4. When negotiating a contract, ask tough questions about the vendor’s hiring policies and employee monitoring practices, because malicious insiders represent security risks.

5. Research security controls and make sure cloud providers have those controls in place. Also understand how vendors will handle breaches.

6. Understand that your company is most likely responsible for the confidentiality and integrity of its systems. Identify vulnerabilities by conducting regular penetration tests of your cloud-based systems— with the provider’s help, if possible.

7. Implement your own security tools, such as complex passwords, data encryption and data access management software that integrates with your infrastructure.

8. Ask your security and legal teams to review cloud providers’ setup, the more

9. Critical business systems or confidential information such as financial data and intellectual property might be too sensitive for systems that are publicly accessible in the cloud, Irvine says. Your contract with a cloud service provider should include “a clause requiring complete declaration of all outsourcing or third-party service providers being used by your cloud partners,” Irvine says. “These service providers need to be held to the same service-level agreements. However, the cloud partner needs to be held responsible for any actions, deficiencies or negligence of their service providers.”

Cloud providers, for their part, “need to be more diligent about recognizing the shortcoming of the existing architecture,” Gilmore says. “While I can relate to the need for deploying solutions in a rapid fashion, I also believe the providers owe their customers the due diligence in ensuring [that] data and resources are safe and secure.”

It’s vital to audit and update the cloud infrastructure on a regular basis. Users of cloud services should ensure that they completely understand the security architecture of their providers and act accordingly to bolster their own security where needed, Gilmore says. “Doing things such as implementing an internal Web security system is really a no-brainer, but you’d be surprised at how many enterprises fail to do this,” Gilmore says.

Layered Approach

Some experts recommend a layered security model when using the cloud. “As is the case with most security controls, defense-in-depth is especially important when dealing with cloud computing,” says Rob Boren, a partner at consulting firm PricewaterhouseCoopers in New York. “While there is no silver bullet that can completely secure an application hosted in the cloud, risks can be mitigated by applying proper security controls at each layer of the architecture.”

Many cloud providers incorporate security measures such as static code analysis tools at the platform-as-a-service layer to remedy the gaps in a layered security approach, Boren says. Access control is also very important. “If the organization cannot implement or enforce its enterprise identity management solution in the cloud, it must make sure that access control policies in place in the cloud are — at a minimum — at the level of the organization’s policies,” he says.

Companies using cloud services are proactively addressing security.com. Alpine Access, a Denver company that operates a virtual call center for clients, “is always looking to tighten security in light of emerging threats,” says Rich Sadowski, vice president of solutions engineering. “We are continually updating our hardware and software, as well as patches.”

The company uses Amazon.com’s Amazon Web Services across four geographic zones throughout North America for extra availability and security. It has used cloud services for several years for payroll processing, collaboration, customer relationship management and other applications. Other steps Alpine has taken include deploying a “firewall sandwich” to protect Web application servers and back-end systems. “This configuration is particularly important in the cloud, where back-to-back firewalls often exist at the boundaries of the service provider and enterprise network infrastructures,” Sadowski says. He says on- and off-the-shelf security technologies include multi-factor authentication and context-based authentication, which uses contextual information to help confirm a user’s identity.

Hult International Business School in Boston runs multiple applications in public and private clouds, including a learning management system, email, file storage and social media tools. The school’s IT department works with cloud providers and assessed its own security needs before moving apps to the cloud. “I didn’t really focus on vendors’ assurances as much as I did on my own research to verify the security of cloud providers,” says CIO Yousuf Khan. “The key thing is asking, What’s the criticality of the application, and have I done my homework when considering moving it to the cloud?”

Hult also uses security tools such as an identity and access management application from OneLogin, which enables users to go to a portal to be authenticated for access to applications in the cloud. Organizations that rely on the cloud need to build in expecta-

Violino is a freelance writer in Massapequa Park, N.Y. You can reach him at bviolino@optonline.net.

Tips for Better Cloud Security

1. Know your own infrastructure and that of your cloud provider.
   The less you know about the vendor’s setup, the more vulnerable you are.

2. Ask your security and legal teams to review contracts with cloud providers. Verify that security assurances are legally binding.

3. Study your provider’s service-level agreements so you understand all contractual obligations you and the vendor’s. Make sure that you can monitor your apps, and that the vendor will notify you in the event of a security breach.

4. When negotiating a contract, ask tough questions about the vendor’s hiring practices, because malicious insiders represent security risks.

5. Research security controls and make sure cloud providers have those controls in place. Also understand how vendors will handle breaches.

6. Understand that your company is most likely responsible for the confidentiality and integrity of its systems. Identify vulnerabilities by conducting regular penetration tests of your cloud-based systems— with the provider’s help, if possible.

7. Implement your own security tools, such as complex passwords, data encryption and data access management software that integrates with your infrastructure.

8. Ask your security and legal teams to review contracts with cloud providers. Verify that security assurances are legally binding.

9. Critical business systems or confidential information such as financial data and intellectual property might be too sensitive for systems that are publicly accessible in the cloud, Irvine says. Your contract with a cloud service provider should include “a clause requiring complete declaration of all outsourcing or third-party service providers being used by your cloud partners,” Irvine says. “These service providers need to be held to the same service-level agreements. However, the cloud partner needs to be held responsible for any actions, deficiencies or negligence of their service providers.”

Cloud providers, for their part, “need to be more diligent about recognizing the shortcomings of the existing architecture,” Gilmore says. “While I can relate to the need for deploying solutions in a rapid fashion, I also believe the providers owe their customers the due diligence in ensuring [that] data and resources are safe and secure.”

It’s vital to audit and update the cloud infrastructure on a regular basis. Users of cloud services should ensure that they completely understand the security architecture of their providers and act accordingly to bolster their own security where needed, Gilmore says. “Doing things such as implementing an internal Web security system is really a no-brainer, but you’d be surprised at how many enterprises fail to do this,” Gilmore says.

Layered Approach

Some experts recommend a layered security model when using the cloud. “As is the case with most security controls, defense-in-depth is especially important when dealing with cloud computing,” says Rob Boren, a partner at consulting firm PricewaterhouseCoopers in New York. “While there is no silver bullet that can completely secure an application hosted in the cloud, risks can be mitigated by applying proper security controls at each layer of the architecture.”

Many cloud providers incorporate security measures such as static code analysis tools at the platform-as-a-service layer to remedy the gaps in a layered security approach, Boren says. Access control is also very important. “If the organization cannot implement or enforce its enterprise identity management solution in the cloud, it must make sure that access control policies in place in the cloud are — at a minimum — at the level of the organization’s policies,” he says.

Companies using cloud services are proactively addressing security.com. Alpine Access, a Denver company that operates a virtual call center for clients, “is always looking to tighten security in light of emerging threats,” says Rich Sadowski, vice president of solutions engineering. “We are continually updating our hardware and software, as well as patches.”

The company uses Amazon.com’s Amazon Web Services across four geographic zones throughout North America for extra availability and security. It has used cloud services for several years for payroll processing, collaboration, customer relationship management and other applications. Other steps Alpine has taken include deploying a “firewall sandwich” to protect Web application servers and back-end systems. “This configuration is particularly important in the cloud, where back-to-back firewalls often exist at the boundaries of the service provider and enterprise network infrastructures,” Sadowski says. He says on- and off-the-shelf security technologies include multi-factor authentication and context-based authentication, which uses contextual information to help confirm a user’s identity.

Hult International Business School in Boston runs multiple applications in public and private clouds, including a learning management system, email, file storage and social media tools. The school’s IT department works with cloud providers and assessed its own security needs before moving apps to the cloud. “I didn’t really focus on vendors’ assurances as much as I did on my own research to verify the security of cloud providers,” says CIO Yousuf Khan. “The key thing is asking, What’s the criticality of the application, and have I done my homework when considering moving it to the cloud?”

Hult also uses security tools such as an identity and access management application from OneLogin, which enables users to go to a portal to be authenticated for access to applications in the cloud. Organizations that rely on the cloud need to build in expecta-

Violino is a freelance writer in Massapequa Park, N.Y. You can reach him at bviolino@optonline.net.
Experts say that the average cost of a data breach in the U.S. is $204 per individual.

**THOMAS J. TRAPPLER**

**Building a Bulletproof Contract in the Cloud**

W H AT M A K E S people hesitate to put their data in the cloud? Loss of control tops many lists of concerns. We all know how painful a data breach can be. It’s hard enough to prepare for a breach when you’re in control. How do you do it when someone else is in charge?

That’s the job of a well-negotiated contract.

Let’s face it: Data breaches can be expensive, and they can damage your reputation. According to Ponemon Institute’s “Five Countries: Cost of Data Breach” report, the average cost of a data breach in the U.S. is $204 per compromised individual. The report analyzes numerous data breaches, of those that took place in the U.S., the smallest involved 5,000 people. So even at the low end, the total price tag was over $1 million.

It’s possible to prepare for breaches in a way that enables you to avoid such costs. Here’s how.

For starters, your cloud contract should state the obvious: that the vendor won’t share your data with anybody else. Yet despite such provisions, there’s always a risk that any data stored on a provider’s infrastructure could be inappropriately or maliciously accessed, used or disclosed.

A data breach involving surveys of people’s favorite ice cream flavors might not be a big deal, but the stakes go up when the hacked systems hold sensitive data such as Social Security numbers, credit card numbers or personal health information. So it’s important to know in advance what kind of data you’re storing in the cloud. Armored with that information, you’ll know how strongly you should negotiate for certain contract clauses. Categorizing your data — even in a very simple way — can be helpful. High-sensitivity data would include information that’s regulated, proprietary or business-critical; the medium-sensitivity category would include data that’s personal but not highly sensitive; and low-sensitivity data could include information that doesn’t reveal people’s identities or is already publicly known. Next, it’s important to define who will be responsible for which follow-up actions and/or related expenses in the event of a data breach. Key issues to consider include the following:

**Notification.** The cloud provider should agree to notify you about any breach of its system, even if your data wasn’t involved. And it should do so as soon as possible, preferably immediately.

**Details.** When the vendor notifies you about a breach, it should tell you when the breach occurred, how it was perpetrated, what data was accessed, and who committed the breach. It’s possible that a series of notifications might be necessary to provide all of the details.

**Corrective actions.** The cloud provider should do the following as soon as possible: cut off the hacker’s access to your data, restore your secure access to the service, apply state-of-the-art forensics in investigating the incident, and upgrade its infrastructure to address the root causes of the breach.

**Indemnification.** Due to the high costs of breach, the cloud provider should indemnify you if the incident was its fault. A vendor will typically try to limit its liability to an amount equal to the fees that you’ve paid over the previous 12 months. Depending upon your needs, you might need to negotiate a larger sum, perhaps the amount you’ve paid over the previous 24 months or a higher fixed amount.

As with so much else related to cloud computing, the best way to deal with a data breach is to protect your interests beforehand with a properly drafted contract.

---

**opes**

**THOMAS J. TRAPPLER**

**Trapper is director of software licensing at the University of California, Los Angeles, and a nationally recognized expert, consultant and published author on the topic of cloud computing risk mitigation via contract negotiation and vendor management. For more information, please visit ThomasTrappler.com.**

---

**COMPUTERWORLD SEPTEMBER 2012**

---

**SPONSOR RESOURCES**

**Addressing Fundamental Cloud Questions for the Enterprise**

Organizations across the business spectrum are harnessing cloud services to drive agility, innovation and further positive business outcomes. But to realize that potential, you must first address the most basic cloud issues. This paper will outline the first important steps businesses must take for a successful cloud evolution. Download PDF

**Increasing Agility and Reducing Cost for Cloud Computing**

Now that the dust has settled from the initial cloud excitement, it is realizing that its main task remains unchanged: to deliver reliable services in a cost-effective way. What has changed is the way lines of business think about IT services. This paper explores implementing comprehensive, unified management that can help you handle the intricacy of large hybrid cloud environments. Download PDF

**Defining Tier-1 Storage in the Modern Data Center**

Modern data centers have evolved into a complex web of virtual machines, clouds and growing user expectations. Gain a better understanding of the modern definition of Tier-1 storage according to ESG. Find out about the attributes and categorization required for your infrastructure to operate a modern data center. Be in the know about the appropriate criteria which will enable your Tier-1 storage to cope and respond to the needs of the next-generation data center. Download PDF

**The Best Way to Build a Cloud**

Virtually every company is interested in transforming its infrastructure and applications to take advantage of the cloud and a more flexible, efficient IT infrastructure. However, implementing a private cloud can be complex and daunting. This report sponsored by HP + Intel outlines a strategy for quickly unlocking the benefits of the cloud. Learn about the solutions that can help you save time, improve storage efficiency and maintain a secure, available environment. Download PDF

**Building Cloud-Optimized Data Center Networks**

This white paper reviews the impact of cloud computing on data center networks and describes HP’s approach to building simpler, more secure and automated networks that fully meet the stringent performance, security, reliability and agility demands of the new data center in the cloud. Download PDF