Combat the Latest Cloud Security Challenges and Risk
Introduction

Even though the benefits of cloud computing are clear to most enterprise IT teams, security remains a top make-or-break issue, often influencing organizations' decisions around cloud. A primary fear is losing control over IT infrastructure and applications, once they're in a public cloud provider's hands.

But security technologies are evolving, and enterprises have more access to cloud security tools that provide the control and visibility they crave. New environments, such as hybrid and multicloud, can create additional gaps and vulnerabilities, but tools, such as cloud access security brokers, now target those unique attack surfaces. By forming a comprehensive strategy, enterprises can take a proactive approach against cloud security challenges and risks.
Uncover Common Cloud Threats

Understand top cloud security challenges

In the minds of many enterprises, cloud computing and security go hand in hand. While public cloud is a less expensive and more efficient computing environment, it can introduce new IT risks without some level of protection. Get to know the most pressing cloud security challenges and risks, such as shadow IT, compliance issues and improper encryption techniques. Consider all enterprise security needs and how to meet those requirements in every environment, including hybrid and multicloud.
The risky business of securing data in the cloud

Staff, SearchCloudComputing

When it comes to enterprise adoption of cloud computing, the numbers speak for themselves. Spending on public cloud services will exceed $127 billion in 2018, accounting for more than half of global software, server and storage spending growth, according to market analyst firm IDC.

But despite all the fuss, not all IT organizations are racing toward the cloud. And security concerns, especially surrounding public cloud and its multi-tenant nature, are a big reason why.

Many organizations' concerns about securing data in the cloud are valid. Without proper security measures in place, data stored and processed in the
cloud becomes vulnerable to leaks and, even worse, to security breaches and attacks.

Ranging from BYOD to data residency, here's a look at seven of the most common -- and perilous -- cloud security risks, along with ways to identify and overcome them.
Overlooking cloud data encryption

As an organization's data flows beyond the confines of its data center and into the public cloud, protecting that data from prying -- and unauthorized -- eyes becomes key. And one of the best ways to do that is through cloud data encryption.

Encryption converts data into another form, called ciphertext, that's unrecognizable to anyone unauthorized to see it. Without encryption, especially in an increasingly mobile and cloud-driven world, a business's data is especially vulnerable if it falls into the wrong hands.

Public cloud users should encrypt both data in transit and at rest, said Garrett Bekker, senior security analyst at 451 Research LLC.
"You need to protect data in transit to make sure it's not intercepted and you're not vulnerable to man-in-the-middle attacks," Bekker said. "You also need to protect data at rest to make sure somebody at the cloud provider you are using doesn't have inappropriate access."

Despite its benefits, encryption is not a set-it-and-forget-it cloud security approach, warned Erik Heidt, research director at Gartner. "[Organizations] cannot make the assumption that simply because data is encrypted, it is somehow protected with an amulet of security," Heidt said.
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

---

**Force-fitting traditional security methods to cloud**

Doing things the way they've always been done can backfire. And not adapting security measures to public cloud is like trying to fit a square peg into a round hole -- it doesn't fit and there are bound to be gaps.

"Our technical architectures are brittle when we try to apply them [to the cloud]," said Jim Reavis, co-founder of the Cloud Security Alliance. Traditional security methods -- relying on the firewall to monitor traffic -- don't exist in the cloud.

Data centers have firewalls that offer the first line of defense. Many IT pros use security apps and data analyzers on top of that to capture packets
going in and out. With cloud, companies don't have physical access to the system, so "there are more nuanced ways you have to apply security controls," Reavis added.

Developers also make the mistake of relying too heavily on the IaaS provider's security layers, said Justin Franks, lead cloud engineer, Lithium Technologies. Because Amazon Web Services (AWS) security groups, for example, are easy to use, developers may not take the extra steps to edit or manage additional layers of security.

Public cloud does have a security leg up over traditional data centers; cloud providers monitor data and alert customers to malicious activity. Providers also continue to roll out more security services and offer more visibility with access to log files, but those services tend to be a la carte.

"There are thousands of cloud services, so the onus is on the consumer to find out there's no uniform approach to how much visibility [the vendor] provides," Reavis cautioned.
Skipping the BYOD security policy

It's tough to deny the benefits of BYOD. Becoming untethered from corporate-owned devices grants employees greater flexibility, convenience and the ability to work at any time, from any place.

But the bring your own device (BYOD) phenomenon is not without risks -- especially when combined with the cloud. In a BYOD and cloud model, an organization's data is not only being hosted and used outside the corporate network, but non-corporate devices are also accessing data.

"That becomes a real challenge to manage because you aren't really controlling anything," said Garrett Bekker, senior security analyst at 451 Research LCC.
To mitigate risks, organizations should establish, and clearly communicate, a BYOD security policy -- guidelines for corporate data access via personal devices. Mobile device management platforms can also help secure and monitor devices accessing data in the cloud.

In some cases, the cloud can actually facilitate BYOD management, said Korey Lee, CIO of SumAll, a New York-based marketing and social media analytics firm.

"Because we operate on the cloud, to disconnect somebody if a device is lost, or to change their password or wipe their phone remotely, is relatively easy," Lee said.
Rushing your Docker container security strategy

Docker caught fire over the past year as a way to deploy Linux containers, but security concerns around multi-tenancy currently limit many Docker deployments to test and development.

"The bigger issue is enterprises having to come to terms and understand what security means [regarding] containers, because it’s different than virtual machines," said Dave Bartoletti, principal analyst with Forrester Research, Inc., in Cambridge, Mass.

Virtual machines (VMs) have a full operating system (OS), isolation, direct hardware access and a mature industry around them. Docker containers,
however, are Linux processes that run on an OS, meaning anyone with access to root privileges can start and stop containers, or perform some other nasty task, if access isn't hardened, Bartoletti said.

It's an issue that remains largely unsolved, as vendors, including Red Hat Inc. and Joyent, approach the challenge differently. But with everyone from IBM to Microsoft focusing on container security, improvements are likely over the next year.

For now, container security is as much about process and governance as it is about technology. Experts urge organizations to only use application containers with strongly guarded permissions, and to monitor the underlying OS. Private Docker image repositories kept in databases behind firewalls are another solution.
Giving away access to cloud APIs

APIs are a critical cog within the overall public cloud machine. Among other things, cloud APIs fuel app development, enable automation and streamline cloud services management.

But, without proper security measures, cloud APIs can also be a gateway to an attack.

In 2014, for example, APIs were largely to blame for a Snapchat breach that impacted 4.6 million users.

To minimize API risks, organizations should press public cloud providers about their application and API security practices, said Erik Heidt, research director at Gartner.
"If [a cloud provider's] narrative or explanation about how they handle app security ... does not reflect an ongoing investment in testing and training and in identifying and remediating problems, then I would be very suspect of that," Heidt said.

SumAll, a social media and marketing analytics firm based in New York, integrates its platform with more than 50 third-party APIs, said Korey Lee, the company's CIO. As a result, API security has become paramount.

"We have taken a lot of steps to mitigate risks by looking at our terms of service and implementing a number of security layers around that data," Lee said. "There's a general, healthy paranoia around where our cloud data is going and who is using it for what," he said.
Letting shadow IT run amok

Shadow IT, or the unsanctioned use of software and virtual machines, not only wreaks havoc on a company's budget, but also creates serious security holes.

"There are people that go off the reservation all the time," said Justin Franks, lead cloud engineer, Lithium Technologies. Shadow IT forces "traditional IT to turn from a choke point -- or centralized management or security stance -- to a watchdog stance," he added. But rogue IT installments aren't necessarily malicious in nature. Often, corporate IT doesn't provision something fast enough, so developers fire up VMs outside of sanctioned cloud providers, creating back doors for accessing internal systems.
While finding those unsanctioned VMs isn't easy, it is getting easier. The first line of defense is to create policies against spinning up unsanctioned cloud services. The next step is to prepare for users to break those policies.

To gain visibility, IT teams use third-party tools such as ThousandEyes, Sumo Logic, Datadog and CloudPassage to monitor applications and analyze outbound firewall logs, or build their own agents to give them "eyes and ears everywhere," Franks said.

But these tools aren't in place to block developers from what they're doing, said Jim Reavis, co-founder of the Cloud Security Alliance. "These are people who are innovating," he added. "It's a matter of understanding what they're trying to do and helping them do it in a more secure way."
Thinking globally, not locally, for data residency

The recent revelations around National Security Agency spying prompted many countries outside the U.S. to take stock of their data privacy laws. And cloud customers -- who are often unaware of where their data is stored -- should also be familiar with these local regulations.

"Every country is reacting to this differently, so it largely depends on where you're located and where you're doing business and what data you're storing," said Garrett Bekker, a senior security analyst with 451 Research LLC, based in New York.

Countries such as Austria, Australia, Canada and Germany are aggressive about data sovereignty and keeping sensitive data within their borders. But regulations are still in flux, so best to err on the side of caution, Bekker said.
"The challenge is it's a lot like shooting at a moving target," Bekker explained. "You don't necessarily know what remediation you need to take and whether they'll meet the letter of the law or not."

Cloud vendors are building data centers around the world, in part to comply with emerging regulations. But customers should take their own steps to ensure compliance, Bekker urged.

First, know where a provider's data centers are physically located. From there, be mindful of data collection processes to ensure compliance with local residency laws. If possible, put language in a service-level agreement that limits where that data can reside, Bekker said.

Cloud customers can encrypt, mask or tokenize sensitive data to minimize risk. Vendors including Perspecsys, CipherCloud and Vormetric also offer data residency services.
Download this comprehensive 19-page Cloud Management Report

Now that you're familiar with some of the major security concerns surrounding the public cloud, get unlimited access to an exclusive Cloud Management report that provides additional insights on managing and securing your cloud environment. Inside, explore a comprehensive list of enterprise-level cloud management vendors and review real user reviews that examine the pros, cons, use cases, features and more of today's top cloud management products. To access this complimentary download, simply participate in our brief Cloud Infrastructure Research Program by weighing in on your current/future cloud projects, challenges and priorities.

Free Download
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

Four cloud security myths debunked

Kristin Knapp, Site Editor

NEW YORK -- Despite the increased adoption of cloud computing in the enterprise, many executives are still wary about moving their data to the cloud. And while much of their reluctance stems from security and privacy concerns, those fears aren't always valid.

In fact, many organizations' cloud security fears are based largely on myth, said Paul Mazzucco, chief security officer at TierPoint LLC, a cloud and colocation services provider based in St. Louis. There are four myths, in particular, that keep executives up at night, Mazzucco said at the Cloud Computing Expo here this week.

Myth one: Data is inherently less secure in the cloud

Many executives wrongly assume their data is more vulnerable in the cloud than it is on-premises, Mazzucco said.
Meanwhile, these concerns are heightened when business executives, in the wake of recent high-level data breaches, drive more and more of the cloud security conversations within an organization.

"We have a tech committee that is basically a few of the head shareholders of our firm - [they're] not IT at all," said Jon Williams, regional support supervisor at Ogletree Deakins, a law firm based in Greenville, S.C. "All these [IT] decisions today are getting approved, and we will bring up ideas to them and vice versa. But they are the ones who are really trying to nitpick and ask questions."

Despite business leaders' concerns, data security is typically more robust in the cloud than it is on-premises, Mazzucco said. This is because the majority of cloud providers build security -- often using a multi-layered approach -- into their infrastructures from the ground-up.

Moving data to the cloud also reduces the risk of shadow IT, or users bypassing IT to access unsanctioned cloud apps. While most executives believe their business runs 50 or fewer cloud-based apps, the average enterprise uses more than 500, Mazzucco said. Deploying a formal cloud strategy gives IT more transparency and control.

**Myth two: A security strategy can wait**

Defining a cloud security strategy should be top-of-mind for both the business and IT from the get-go of any cloud deployment. Simply bolting on
security after deployment is a risk no business should be willing to take, according to Mazzucco.

"It's an action to take now," he said.

Even after an organization puts proper security measures in place -- and ensures, via a service level agreement (SLA), that its cloud provider is doing the same -- on-going monitoring and reporting should always be a priority.

**Myth three: A certified cloud provider guarantees protection**

Many organizations assess a cloud provider's security model based solely on the number of compliance or regulatory certifications that provider holds. But that shouldn't be the case, Mazzucco warned. Instead, IT should always "go to the next level" to evaluate a provider's security environment.

"Always validate the compliance claims your provider has handed to you," he said.

To do this, enterprises should conduct independent security assessments of their provider, or enlist a third party to do so. As a starting point, reference the Cloud Security Alliance's [Consensus Assessment Initiative Questionnaire](#), a list of questions cloud users and auditors should ask of potential cloud providers.
Moreover, organizations should always demand at least some transparency into their provider's security practices, and put that language in an SLA, where possible.

**Myth four: Set it and forget it**

Just as IT shouldn't cobble together a security strategy after deployment, they can't forget about that strategy when it's live, either.

A solid cloud security model is one that's constantly evolving, Mazzacco said. It should entail a multi-layered approach, on-going and advanced threat detection, real-time alerts and consistent monitoring and reporting. Continuously updating antivirus and antimalware technology should be just as much a priority in the cloud as it is in on-premises environments.

"The old 'out of sight, out of mind' mentality is dangerous when it comes to cloud security," Mazzucco said. "Of course, having a dedicated group who looks at all the layers of compute, all the logs, everything that equals a security environment is leaps and bounds [better] over the old approach."

Kristin Knapp is site editor for SearchCloudComputing. Contact her at kknapp@techtarget.com or follow @kknapp86 on Twitter.
Creepy cloud horror stories to keep IT up at night

David Linthicum, Cloud analyst

Ghost stories are playing non-stop on TV and it's almost mandatory you visit a pumpkin patch. Yes, it's that time of year again -- Halloween is right around the corner.

But scary stories are not just fodder for campfires and the big screen. Enterprise IT departments, in particular, are no stranger to nightmares -- especially when it comes to cloud computing.

Here are three cloud horror stories to send chills down IT's spine.

Invasion of the data snatchers

We've all heard about the data breach horror stories at Home Depot, Target and Sony, but what about the attacks that go unreported? Enterprises experience ongoing attacks and have to be proactive to keep up their defenses. This includes constantly patching firewalls and updating encryption, as well as disallowing access from a growing list of IP addresses.

Of all the cloud horror stories IT has to deal with, data breaches are the most terrifying. They are also the reason many enterprises illogically push back on public cloud. But, on the other hand, organizations can't take cloud security lightly. In one recent cloud horror story, an enterprise had its data
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

hacked by a file sharing provider, who took customer lists and credit card data. The incident had to be reported and, while the damage was minor, it took the wind out of the company’s cloud computing sails.

If enough planning and technology go into the mix, the cloud can be more secure than any on-premises system. But without taking proper measures, this cloud horror story will become all too real.

A case of the compliance chills

In another spooky tale, IT realizes that business departments have taken matters into their own hands and placed data in the cloud. Through compliance research, IT then discovers the data was not allowed to leave the enterprise firewall. The company is audited, fined and has to launch a million-dollar PR campaign to restore customer confidence.

While you don't need a huge team of lawyers to determine data compliance requirements for your industry or region, you do need to pay attention. IT should inform everyone who uses public cloud to consider compliance -- or risk hefty fines and a PR mess.

Ghost clouds lurking in the shadows

One enterprise IT shop that thought it had things under control found that about 10% of its data was in the cloud. Turns out, business departments had provisioned and accessed cloud resources without IT’s knowledge or
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

In this e-guide, IT did not understand the issue until it scanned the network for the presence of these "ghost clouds."

As a result, IT had to seek leadership's support to restrict the use of rogue clouds for data storage or other purposes. The business departments then argued that the reason they spun up the cloud services was that IT was too slow to respond to their needs.

IT pros need to understand that this chilling tale is not about control; it's about speed-to-solution. IT should use cloud, or any other technology, to provide the business with answers, not excuses. And until that happens, cloud horror stories will persist.

We all need to be proactive to keep the horror in Hollywood. Now is a good time to take a closer look at compliance issues, the state of your security and ghosts in the cloud.

Next article
Prepare for these multicloud security snags

Stephen Bigelow, Senior Technology Editor

Public clouds are a viable platform for many enterprise applications, but security concerns remain. And, as organizations move to embrace multiple clouds for better versatility and availability, they often overlook emerging security issues, potentially causing data loss, compliance violations and more.

Evaluate the top multicloud security issues, along with ways to mitigate them in your organization.

The evolution of multicloud computing

In many cases, an enterprise's use of multiple cloud providers is cursory; for instance, an organization might duplicate a data store from AWS Simple Storage Service to a Google Cloud Storage bucket. In other cases, users might restart a virtual machine on an AWS Elastic Compute Cloud instance in Google Compute Engine. These use cases help improve data and application availability.

In an ideal multicloud scenario, multiple clouds are tightly integrated, and users load balance and failover applications between different cloud providers and platforms. However, because cloud providers don't use...
standard service suites and application programming interfaces (API), this level of integration is not yet possible. For example, an application deployed on AWS might use AWS Lambda for event-driven computing. But if other cloud providers don't have a corresponding service, that application might not be able to run on another provider's platform.

A closer look at multicloud security issues

One limitation associated with multicloud computing is the lack of similarities between clouds. Each public cloud provider uses different technologies, interfaces and even terminology to describe services or behaviors. There is no standardization of methodologies, services, instance sizes, performance or other attributes between public cloud vendors.

As a result, users often face interoperability issues between vendors, and need workarounds or APIs to operate an application that's deployed on different services. Otherwise, they could expose a potential attack surface. Tools like Oracle's Ravello use nested virtualization to encapsulate VMs and allow users to deploy apps on multiple clouds without making changes -- but that technology is still evolving.

There are other multicloud security issues to consider. The network, for example, remains a perennial security vulnerability because data needs to travel across the Internet, which can be insecure and pose its own configuration and security flaws. In addition, social engineering presents a risk, and hacked cloud accounts can expose a corporation's public cloud
resources. If you use public clouds, educate administrators, employees and end users about proper security policies and confidentiality.

What's next for multicloud security?

There are additional security considerations that will impact multicloud computing in the future. For example, true integration -- including the ability to load balance and failover -- between multiple clouds requires a common way to establish and maintain trust between providers. This includes a common way to approach identity management between clouds. In addition, there must be a common way to handle policies, automation and monitoring so that organizations can detect and mitigate threats, regardless of which cloud is impacted.

Someday, it may be possible to distribute data storage across multiple clouds in a RAID-like manner. Today’s data duplication between clouds is reminiscent of data mirroring -- or RAID 1 -- where data is duplicated between cloud storage instances. Eventually, the integration of multiple clouds might allow organizations to distribute data across multiple storage instances, more closely resembling RAID 5. In addition to improving storage performance, this could support the distribution of error-correcting codes, and potentially allow one cloud provider to rebuild data that another provider may lose or corrupt.

Similarly, there is emerging interest in the concept of distributed trust -- or sharing key security elements, such as identity, across multiple cloud providers rather than duplicate trust separately with each provider.
Distributing things like identity and authentication will boost multicloud security and help prevent attacks.

Shadow IT risks heightened in hybrid cloud

Tom Nolle, President

While there are many advantages to cloud computing, there are also drawbacks, including shadow IT. Driven by cloud’s low-cost, as a service model, shadow IT shifts traditional IT and CIO functions to a business’s line departments. And while shadow IT risks have been discussed before, a new risk is emerging, specifically within hybrid clouds.

To many companies, shadow IT is a way of decoupling a business’s response to a problem or opportunity from a high-inertia IT world. A line department buys compute services from a cloud provider, and adjusts the services to fit business needs. The shadow IT model may not work for every application, but it works well for at least some applications in every enterprise -- and it’s only going to expand as cloud adoption grows.

However, shadow IT risks are heightened when combined with hybrid cloud. Most companies have data security and compliance practices to protect not only their own information, but that of their customers and suppliers. These practices and policies assume that data is contained within a controlled
environment. But if users create a hybrid cloud workflow that connects shadow IT software as a service (SaaS) applications to highly structured applications, they can violate security and governance requirements—a risk known as bandit hybridization.

The dangers of bandit hybridization are growing for two reasons. First, SaaS adoption is increasing, and line departments can easily adopt SaaS applications without IT support.

Second, SaaS providers are offering more applications, making it more likely that data from at least one of those applications will be combined with an organization’s internal or other cloud data. This combination is especially subject to security and governance concerns.

A few bandit hybridization problems have come to light. Most issues develop after cloud application deployment, when management tries to integrate information to support worker productivity. For example, an organization could look at a CRM application and determine that adding customer order status would help the sales force. The SaaS provider then facilitates a link between the CRM application and the organization’s order status information. But if the organization does not consider security and governance requirements, it can create an insecure link between its data center and the cloud. In some cases, operations security and internal governance teams may not even know about it.

The biggest problem in bandit hybridization occurs with the link between one cloud-hosted application and another. The industry is filled with examples of data combinations that violate security and governance policies.
when the individual data elements would not. And because two or more shadow IT cloud applications can be connected without internal IT knowledge, some of these violations never come to light -- until it's too late.

**Three ways to minimize shadow IT risks with hybrid cloud**

So how do you retain the agility created through shadow IT, while protecting your data and applications? There are focused and broad-brush approaches, but companies should pick one that matches their shadow IT use.

The broadest and most intrusive way to prevent bandit hybridization is to require IT operations, security and compliance reviews for all SaaS contracts, services and interfaces. This alerts IT to the way cloud computing is evolving within their company, and helps them prepare for a hybrid model. But while effective, these reviews can cause delays in SaaS deployment.

The second option is to allow line departments to adopt SaaS applications, as long as there is no data exchange or workflow connection with other applications. When a data exchange is needed, organizations should conduct the operations review mentioned above. It’s also important to develop and certify any data exchange processes. This approach, however, has been met with mixed success; some companies report that operations personnel still bypass IT, while others say time is wasted reviewing what should be a simple process of application interconnection.
Another emerging approach is compliance contagion. Hybrid cloud components such as applications, data and workflows carry their own regulatory, security and governance requirements. In the contagion approach, the requirements of these hybrid cloud elements -- whether from the data center or from another cloud environment -- are published. Any time a hybrid connection is created between one cloud application and another, each application will "catch" the other's requirements. As a result, IT must ensure both applications are compliant and secure.

But even this approach doesn't fully address the challenge of securing multiple shadow IT cloud applications in a hybrid environment, particularly if both applications come from the same cloud provider. The only alternative to doing a professional IT review of all hybrid applications and workflows, even within a single SaaS provider, is to educate line department managers about security and governance issues as a condition for cloud service contract approval.

As appealing as shadow IT is to many companies, and nearly all line departments, the risks of bandit hybridization are difficult to control without formal IT involvement. As SaaS providers expand their markets, there will be more SaaS applications that require connections to existing data center applications. With that in mind, it may be impossible to detect the subtle signs of bandit hybridization, making security and compliance reviews on every cloud project critical. While that won't put an end to shadow IT, it will at least bring more light to the issue.
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

About the author:
Tom Nolle is president of CIMI Corp, a strategic consulting firm specializing in telecommunications and data communications since 1982.

Form a Cloud Security Strategy

What to consider when building a cloud security plan

After deciding to migrate to the cloud -- and getting the business on board -- reevaluate your IT strategy to address any cloud security challenges and risks. Start by researching cloud providers’ capabilities to determine if their certifications and tools fit your security requirements. Don't assume your provider will handle all your security needs; sometimes, adding third-party tools is necessary to address vulnerabilities. Finally, when securing your cloud, remember there are internal cloud security threats as well as external. There is no one-size-fits-all security strategy, so be sure to craft your plan around the enterprise's individual needs.

Prove the security of cloud computing in your organization

Dan Sullivan, Contributor

Many cloud administrators have to make the case that cloud is just as secure, or more secure, than on-premises IT environments. And while there are still cloud security skeptics in the enterprise, they can ultimately play a key role in identifying pertinent cloud security issues. Ultimately, to win a
cloud security argument, administrators should treat any concerns about the security of cloud computing as legitimate, and address them accordingly.

The first step to ease your organization's security concerns with cloud computing is to assess the security backbone of potential or current cloud providers. The simplest way to do this is by verifying a provider's major security certifications. Some important certifications to look for include the ISO 9001:2008 certification, ISO 27017:2015 certification, Multi-Tier Cloud Security Standard Level-3 certification and OC-3. Assessing the certifications of a cloud service vendor provides a good jumping off point for other assessment factors.

For instance, regulation compliance is also a good indicator of the overall security of cloud computing services or providers. If you work in highly regulated industries, such as finance or healthcare, regulation compliance is a must. Part of assessing a vendor's security level is recognizing the regulations -- such as the Health Insurance Portability and Accountability Act (HIPPA), Payment Card Industry Data Security Standard and Federal Risk and Authorization Management Program -- to which your organization needs to comply.

To properly address your compliance needs, look in-depth at the cloud service in question. Remember only some cloud services may be compliant with a particular regulation. For example, Amazon Web Services' EC2 instances may be used with applications subject to HIPPA regulations, but the SMS messaging service cannot.
Another hurdle administrators face when addressing concerns about the security of cloud computing is dealing with a dynamic infrastructure. Environments configured for flexibility and scalability rely on code to properly maintain the required level of security. Luckily, there are tools available for such a task. Tools such as Chef and Puppet, for example, enable the writing, testing and configuration of scripts, which minimizes the risk of configuration errors. Similarly, there are tools available for monitoring and configuring servers.

Tackling security concerns with cloud computing through shared responsibility

It is important to remember that cloud providers employ a shared security model. Generally, the cloud provider is responsible for securing its own network, the physical security of its facilities and the security of services up to and including hypervisors. On the other hand, customers are responsible for system and application security. These are the same responsibilities one would have with on-premises IT environments.

To hold up the customer end of a shared security model, there are some best practices to keep in mind. These include using hardened machine images, routinely performing vulnerability scans, using encryption for both data in motion and at rest, and using identity management services for access controls.
But, even with these best practices in place, security concerns with cloud computing still persist in many organizations. And one question, in particular, still lingers: can the cloud provide improved security over an on-premises environment? In short, yes. There are two main advantages to using a cloud vendor. First, cloud providers benefit from economies of scale. Because they can recover costs from their wide customer base, cloud vendors invest in security procedures that can be applied to a large number of users. Second, as a customer, working with a cloud provider frees up the IT security resources that would normally need to go into physical or hypervisor security.

Cloud providers offer an opportunity for users to take advantage of their security technologies and procedures. This allows customers to focus on delivering functionality and services that meet the specific needs of business users, while still protecting the confidentiality, integrity and availability of systems. This may be the most effective argument for addressing security concerns with cloud computing: cloud providers have demonstrated a commitment to security, have the ability to meet demanding standards and relieve customers of some of the overhead of IT security implementation and administration. If you opt to not take advantage of these benefits while competitors do, consider whether that puts your company at a competitive disadvantage.
Read between the lines of providers' cloud security assessments

Paul Korzeniowski, Freelance Writer

Cloud security assessments and certifications are designed to help businesses understand what steps a provider takes to protect confidential information. But while security certifications may provide users with some level of comfort, they're not always enough to guarantee that their information will be safe.

Data security continues to be a major bugaboo with public cloud. "After price, what level of security a provider offers is one of the first questions a business asks when examining a public cloud service," said Dan Blum, managing partner and principal consultant at Security Architects LLC, a consulting firm based in Washington, D.C.

Organizations often feel uncomfortable moving sensitive information from their own data center to that of a third-party provider. To assuage that feeling, businesses like to confirm that a provider has completed certain cloud security assessments, or holds certifications. Those cloud security certifications often consist of two elements. First, an ad hoc group develops a framework that outlines what checks should be put in place to safeguard data. Then, third parties develop processes to ensure that those checks are implemented.
Baseline IT security certifications

IT security is complex, so, through the years, frameworks emerged from many different groups. When evaluating a cloud provider's security, business often begin with Statement on Standards for Attestation Engagements 16, according to Pete Lindstrom, VP of security research at IDC, an analyst firm based in Framingham, Mass.

The American Institute of Certified Public Accountants crafted the specification, which defines how service providers deploy security controls. The program produces three reports: Service Organization Controls (SOC) 1 focuses on financial reporting; the SOC 2 report evaluates the security, availability, processing integrity, confidentiality and privacy of a vendor's internal systems; and the SOC 3 reports the same information as SOC 2, but is designed for a general audience, rather than specific parties.

Two groups -- the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) -- worked together to craft a second set of standards. The ISO 27001 specification focuses on information security management systems and ISO 27002 describes system controls.
Cloud security assessments and certifications

The previous guidelines do not differentiate between cloud and traditional on-premises system security, but, more recently, cloud security assessments and certifications arose. For example, the National Institute of Standards and Technology Special Publication-500 specification outlines the role of cloud computing in the U.S. federal government. The document addresses cloud operations, management and security issues.

Vertical standards take shape

In addition to the horizontal standards, there are industry-specific certifications to look for when assessing cloud providers:

- **Health Insurance Portability and Accountability Act** is used to protect personal medical information, principally in the USA.
- **PCI-DSS** safeguards consumer payment card credit information.
- **FedRAMP** monitors government data and offers a standardized approach to security assessment, authorization and continuous monitoring of cloud services.
- **Information Assurance Framework** was developed by the European Network Information and Security Agency, and aims to close network and information security holes.
Formed in December 2008, the Cloud Security Alliance (CSA) is a coalition that provides guidance for enterprises adopting cloud computing. The group's Cloud Controls Matrix consists of principles that help prospective cloud users assess a cloud provider's overall security risk. The group's Security, Trust and Assurance Registry (STAR) assessment and certification process features three cloud security certifications: Level 1 is a self-assessment by the provider; Level 2 is an assessment of the provider done by a third party; and Level 3 checks security on an ongoing basis rather than only one time.

**Buyer beware**

The various standards and certifications that a cloud provider can hold come with caveats. First, they fall short of the ironclad guarantee that some companies desire; a certification provides only a high-level overview of a provider's security checks.

Second, the specifications themselves work at a high level. For instance, a certification may require that a business deploy a **strong authentication system**, but may not require that organization to use biometrics.

Third, the standards often overlap. Part of the CSA STAR Level 1 certification, for example, is based on the **SOC 2 requirements**, and the CSA's Level 2 certification uses pieces of the ISO/IEC 27001 standard.

Finally, the certification process is time-consuming and expensive. Consequently, the older certifications are more widely adopted among cloud...
providers. "Many of the large cloud service providers have passed the popular certifications," Lindstrom said.

**Small numbers in some cases**

The numbers are small for the new cloud security certifications; about 20 cloud suppliers have publically stated that they completed the CSA STAR self-assessment and 30 third parties offer Level 2 certification, according to Jim Reavis, co-founder and CEO at CSA.

Small, niche or startup cloud providers may lack certifications. "The customer has to determine if the need for the service offered outweighs any potential security risk," Blum said.

Remember that cloud security assessments and certifications aren't a perfect reflection of a provider's security posture. To fully understand how your provider implements security processes -- and whether those processes are adequate -- a business needs to examine various reports, according to Blum. The reports usually are not published on a cloud provider's website, so the user has to do some digging to find that information.
Build a shadow IT strategy all departments will love

Alan Earls, Contributor

It's a phenomenon that's at least as old as the PC: business departments and end users deciding to bust loose from the constraints of corporate IT to do their own thing. Today, thanks in part to the wide range of offerings available through the cloud, that phenomenon -- now called shadow IT -- is experiencing a major comeback.

And while building a shadow IT strategy can be as challenging now as it was 35 years ago, one increasingly common approach is for organizations to accept it, rather than fight it.

"If you can't beat 'em, join 'em," said Joe Fuller, vice president and CIO of Dominion Enterprises, a marketing company based in Norfolk, VA. His company, which produces print advertising magazines such as Auto Trader, now operates 26 listings sites, including Homes.com and Boattrader.com. That, in turn, means operating two data centers where most of those sites are hosted.

"We don't try to battle shadow IT; we try to embrace it," Fuller said. His department provides direct connections to Amazon Web Services (AWS) and Microsoft Azure from its data center in nearby Ashburn, VA. Dominion's internal hosting rates mimic AWS rates. "When we send our bill for hosting to our internal business customers, we include a recap of their cloud billing,
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

too, so the business leaders can see what they are spending inside and outside the company," Fuller said.

Fuller is also training the company's systems and network engineers on AWS and Azure so they can be a resource to the development teams that use those services outside IT's hosting environment.

**Four key steps to building a shadow IT strategy**

Shadow IT was a constant problem for about a decade at the University of Michigan in Ann Arbor, said Tim Rolston, a former IT director there. So his group eventually became adept at managing and integrating shadow IT with official IT offerings. Based on that experience, Rolston recommends a four-step approach to building a shadow IT strategy.

1. **Create an adoption path.** Most users deploy shadow IT systems to fill a need that official IT systems have not addressed. Rolston calls such shadow IT systems "gap solutions."

   "When you identify a successful gap solution running in your environment, embrace it, fund it and absorb it into your service catalog if it provides sufficient value," Rolston said.

2. **Consider making adjustments to existing services.** Sometimes, shadow apps simply work better for users than the equivalent offering in your IT service catalog. Therefore, "you should consider altering your [own] service
to specifically address the concern prompting the shadow service," Rolston said. If you can, include the shadow IT end users to make them feel like a part of this process, and encourage adoption of the adjusted IT offerings.

Next, communicate to the entire user base that you're making a change to your service -- and why. "Give full credit to the folks who made the shadow system," he said. "This will encourage other folks to approach you with their needs, as opposed to creating [more] shadow systems."

3. Don't "squish" shadow IT if you can't provide a better service for end users. It's possible that you simply aren't able to provide a better offering than what a small-scale shadow IT system can provide. If that's the case, let the shadow apps continue to run, and offer whatever support or funding you can afford to give.

If you can't afford to support it, be upfront about it, Rolston said. "This will prevent the shadow IT offerings in your organization from going deeper underground and making their identification almost impossible," Rolston said.

4. Give "homegrown IT" awards. Organizations should give an award or recognition to end users with the best homegrown IT systems, or those with the best suggestions for improving existing IT services. "This will encourage folks to approach you with their homegrown systems or concerns before they go 'shadow,'" he said.

While the four steps above may not be appropriate for every organization, they "helped our users see that we were on the same team, as opposed to adopting an 'us versus them' mentality," Rolston added.
Improve to eradicate shadow IT risks

The presence of shadow IT can be a good indicator that the IT organization isn’t meeting the objectives of the business. So, the focus shouldn’t be on managing shadow IT or getting rid of it, but on making it unnecessary, said Ben Piper, an author and IT consultant at Ben Piper Consulting in Atlanta, GA.

When creating a shadow IT strategy, IT teams should seek out the business objective behind every request. When they get a request to install a new piece of software, ask, "Why?" to uncover the true business need. "Too often, IT thinks of itself as a service provider and neglects its consulting role in the business. An IT manager should be able to explain every item of IT spend in terms of business objectives met -- not services provided," Piper said.

Finally, remember that shadow IT risks have always existed, and will continue to exist, said Andrew Storms, VP of security services for New Context, a security consultancy in San Francisco. That means one of the best things IT can do when building a shadow IT strategy is communicate. "Get out of the cubes and go and speak with your users; creating and fostering that human bond goes a long way to understanding your users' needs and challenges," he said.

Next article
Cloud security requires shared responsibility model

Kristin Knapp, Site Editor

NEW YORK -- When enterprises move data to the cloud, they surrender at least some control to their cloud service provider. But when they brush their hands of all responsibility -- especially when it comes to data security in the cloud -- it's a risky move.

To fully secure their data in the cloud, enterprise IT teams should never solely rely on their cloud provider. Instead, that responsibility should always be shared, said Vinay Patel, director and global head of information security at Citi Technology Infrastructure, the technology arm of New York-based banking and financial services firm Citigroup, Inc.

"Relinquishing control does not equate to relinquishing accountability or responsibility," Patel said at the Cloud Security Alliance (CSA) Summit 2015 here this week. "If you think about some of the expectations of your business' management [team], your regulators and your auditors â€“ they expect you to be accountable."

To ensure a shared responsibility model for cloud -- or an approach by which both the cloud provider and its customers are accountable for certain aspects of security -- enterprises must clearly define their own responsibilities, along with those of the cloud provider. A distinct line should be drawn that indicates which party is accountable not only for certain
aspects of data security, but the security of applications, virtual machines, interfaces, service configurations and more in the cloud.

Most major cloud providers, such as Amazon Web Services (AWS), detail their shared responsibility models on their websites. AWS, for its part, says its customers are responsible for "security 'in' the cloud," which includes the security of data, applications, operating systems, and network and firewall configurations.

On the other hand, AWS assumes responsibility for the "security 'of' the cloud," meaning compute and storage resources, as well as databases, networking and other components of the AWS global infrastructure.

Still, the lines can easily become blurred -- especially with a provider who has a cloud services footprint the size of AWS' -- which means enterprises must clearly define security roles with their provider upfront, ideally before signing a contract.

"You have to be able to articulate [your expectations] when you are negotiating that agreement with them," Patel said.

Because the dividing line between a cloud provider's security responsibilities and those of an enterprise isn't always clear, it's crucial to have that conversation before signing on with a provider, said Peter Keenan, chief information security officer at Lazard, a financial advisory and asset management firm in New York.

"[It's] going to be contract-dependent, but it's on us, as the enterprise, to make sure that it's very clearly spelled out in the contract where that line is,"
Keenan said. "I think it's going to be a case-by-case, service-by-service basis."

**Know what makes your cloud provider's security strategy tick**

To create a successful shared responsibility model, enterprises need visibility into their cloud provider’s security controls, Patel said. And IT organizations can gain that visibility in a number of ways. For example, they can review independent assessments of their cloud provider's security model, such as attestations from the [CSA's Security, Trust and Assurance Registry (STAR)](https://cloudsecurityalliance.org/). They may also want to check that their provider holds certain cloud security certifications, such as [ISO 27001](https://www.iso.org/iso-27001-information-security-code-of-practice.html).

But because they only reflect the state of a provider's security environment during a given period of time, certifications shouldn't be the only way an enterprise assesses a potential provider, according to Patel.

"[A provider], generally speaking, brought in an independent body that said, 'We are going to follow a certain script, look for certain things, ask certain questions and make sure you meet certain requirements,'" Patel said. "But then they walk away, and the next day, you don't necessarily have the assurance that everything is fine."

To gain full and ongoing visibility into your provider's security controls, it's crucial to ask your provider for that capability, while explaining your unique security requirements, during the negotiation phase. For some organizations,
and particularly those in highly regulated industries like financial services, it might also be necessary to ensure you have continuous monitoring of your provider's environment.

"There is a lot of information out there now, but there's nothing more important than meeting with the vendor that you plan on using and having those in-depth discussions to figure that out, because things change on a daily basis," said Dustin VanWinkle, manager of converged security architecture at ADP, a payroll and HR management services provider based in Roseland, N.J.

In addition to having a face-to-face conversation with your provider, call on another powerful resource to gain insight into your provider's security controls: other customers.

"Some of it is just kind of sitting across the table from [a provider], looking him in the eye, and asking him these questions and seeing if he blinks," Lazard's Keenan said. "But look around you -- [there are] folks in the room here that you can call and say, 'Are you using this guy? How's it been?' That's probably more valuable than anything else I've seen."

Kristin Knapp is site editor for SearchCloudComputing. Contact her at kknapp@techtarget.com or follow @kknapp86 on Twitter.

Next article
Achieving zero trust security in the cloud

Keith Townsend, Founder

In physical implementations of zero trust security -- a security model in which no user, interface or application is automatically “trusted” -- traffic flows through a centralized security device. But because a single device has to filter all traffic, it's difficult for a zero trust security policy to scale. Environments can scale, however, when the workloads and network are virtual or cloud-based.

In the data center, micro-segmentation, a byproduct of hypervisor-based network overlays, allows zero trust security to be applied at scale. And with cloud services, micro-segmentation is often inherent, according to a podcast with Adrian Cockcroft, a technology fellow at venture capitalist firm Battery Ventures and former cloud architect at Netflix. Here's a look at the micro-segmentation and zero trust security capabilities within various virtualization and cloud platforms.

VMware NSX

VMware's network virtualization platform NSX filters any traffic that travels to and from the hypervisor. This capability creates zero trust security. VMware uses the scalability of NSX's distributed firewall to create zero trust security between virtual machines (VMs) on separate hosts. A security policy can also be created between hosts on the same logical Layer 2 broadcast network.
VMware’s approach is to abstract physical zero trust security, while using the distributed attributes of hypervisor-based network overlays. Administrators create rules in a centralized management system that are enforced across a distributed firewall appliance. The result is a centrally-managed solution that can scale to double-digit Gpbs per hypervisor.

Amazon Web Services

In cloud platforms, customers and third-party products don’t have direct access to the underlying hypervisor. This means customers must rely on services made available via cloud APIs to achieve zero trust security.

In the case of Amazon Web Services (AWS), it’s important to understand the connectivity between the public cloud and an internal network. There are three ways to access instances running in AWS: the public Internet, IPsec-based Amazon Virtual Private Cloud (VPC) and AWS Direct Connect -- a dedicated Layer 3 circuit into Amazon facilities. All connectivity options require customer-side IP termination, which should be through a firewall. Amazon does not allow users’ Layer 2 traffic to be extended over Direct Connect or VPC.

Based on the AWS connectivity design, there is inherently zero trust between AWS hosted instances and on-premises nodes. The question then becomes what happens to instance-to-instance traffic within AWS?

AWS uses security groups to control network access to instances. Security groups can be very broad or narrowly defined. An instance can have one or
several security groups applied to it. While the focus is typically on IP traffic, it's important to know that VPC networking doesn't support broadcast or multicast traffic. So, there is no need to filter for non-IP traffic.

Developers can create or assign rules using either the AWS Management Console or the AWS API. They can also apply the rules to both inbound and outbound traffic. By default, all outbound traffic is allowed, while inbound traffic is denied. This granular capability can make it difficult to troubleshoot connectivity, as single instances can belong to multiple security groups. In addition, separate security groups exist for both Windows and Linux, which could result in conflicting or overlapping security policies. However, this can be the case with any zero trust security offering.

**Google Compute Engine**

*Google Compute Engine* networking is more similar to traditional networking. Each instance is assigned to a default network, which allows instance-to-instance traffic within the same network. Google provides a logical firewall that blocks traffic between networks. To achieve zero trust security, each instance must use a local firewall or *iptables*, or place each instance in a separate network. However, using local firewalls and *iptables* can be extremely difficult to manage and, because CPU cycles will be used to enforce the rules, it may impact VM performance.
Microsoft Azure

Microsoft Azure's networking is similar to Google Compute Engine's networking. VMs are grouped in logical private networks. Azure allows for endpoint access control lists (ACLs), which are applied at the host level. Processing rules at the host level helps maintain local VM performance. Similar to Google, you can't apply rules for instances from groups in Azure. Therefore, keeping track of rules in a large environment can be a challenge.

Cloud providers have robust models for zero trust security and micro-segmentation. In the case of Microsoft Azure and AWS, developers can choose to integrate micro-segmentation security from within an application. This allows developers to create applications that scale and react to rapidly changing security.
How do I establish network security groups for public cloud?

Jim O'Reilly, Cloud consultant

Network security groups allow organizations to shield parts of their public cloud from direct outside access — similar to a firewall. At the same time, these groups ensure the data flowing between cloud instances is contained only within relevant instances. While some organizations will require additional public cloud security tools, network security groups are a good start.

Network security groups help cloud admins establish access controls for networks in a public cloud configuration. For instance, admins can set up a subnet of instances as a demilitarized zone (DMZ) with Internet access, while ensuring tiers of back-end cloud instances only talk to each other, and to specific ports or instances, within the DMZ.

The process for setting up network security groups differs between clouds. With Microsoft Azure, for example, admins create network security groups either through the Azure Resource Manager portal, which has a GUI setup, or through scripts. Cloud admins for Amazon Web Services (AWS) can use AWS' Virtual Private Cloud console.

All cloud instances need to belong to network security groups, and there is a default group in both that blocks inbound traffic from the Internet. However, it's generally bad practice to rely only on defaults. Cloud services need to
communicate with other applications and services, but some instances, such as databases, should never be accessed directly by the Internet.

To address this, cloud admins can create a three-tier cloud security model that consists of:

1. A top tier that is Internet-aware for Web servers.
2. A middle tier that acts as an application layer and talks to the top tier and the bottom tier.
3. A bottom tier that supports the database. Because only the middle layer can communicate with the bottom tier, the database has greater isolation.

There are other similarities and differences between network security groups for public cloud security in Azure and AWS. Both are rules-based systems and admins can apply these rules to cloud instances, as well as subnets. In AWS, rules have no priority over each other; this makes it easier for admins to write them, since exceptions to a prior rule don’t need to be stated. Azure maintains a priority system, which more closely resembles traditional firewall setups, and can increase complexity.

Google takes a more traditional approach to public cloud security. Google Cloud Platform uses features such as firewalls and routing that are more familiar to network admins with a background in on-premises operations. While experienced admins may feel more comfortable with Google’s cloud security approach, it could also create more work, since there are more elements to manage.
How can I minimize cloud API security risks?

Stephen Bigelow, Senior Technology Editor

Cloud application programming interfaces allow software developers to create code that interfaces with a cloud provider's services. But while critical to cloud applications, APIs also have an attack surface that can potentially compromise sensitive business data. This means providers and software developers need to prioritize cloud API security.

**Sessionless security practices enable better scalability in the cloud**

First, tactics like including a username and password in the body of data or in **simple object access protocol** headers is not secure. Instead, developers should use sessionless security practices such as **HTTP authentication**, **token-based authentication** or **Web Services Security**. Sessionless security also enables better scalability for the cloud service because any server can handle user requests without sharing sessions between them.

Developers should determine whether an API performs secondary security checks, such as verifying the user has appropriate permission to view, edit
or delete services and data. Once initial authentication is cleared, developers often overlook secondary security strategies.

Cloud providers and developers should test cloud API security against common threats, such as injection attacks and cross-site forgery. For the cloud service providers creating the APIs, testing is especially critical. However, users should independently verify cloud API security, as it’s critical for auditing and compliance.

If encryption keys are part of the access and authentication methodology for API calls, store the keys securely and never code them into a file or script.

**Perform API change reporting**

While security is a key part of cloud API construction and use, it’s also important to consider change logging and reporting features. These features help track user access to cloud resources, as well as data and configuration changes.

A software developer invokes one or more cloud API calls to change cloud-hosted data, launch new compute instances and alter the resources provisioned to a cloud instance. Each of these activities should produce a log trail that developers can conveniently access. Comprehensive logging can be critical for auditing, legal discovery and other compliance issues.
Overcome the most pressing OpenStack security challenges

Jim O'Reilly, Cloud consultant

OpenStack adoption continues to grow, with major companies including PayPal, Walmart, eBay and AT&T now using the open source cloud platform. But like any new technology, committing to OpenStack can introduce potential security risks, such as the recently discovered Secure Socket Layer vulnerability. And while OpenStack has created a Vulnerability Management Team, along with a 200-page guide to OpenStack security, to protect against these risks, it's still important for users to build their own OpenStack security strategy.

Building a cloud is not the same as creating a traditional IT cluster. For instance, the number of sockets needed to support the scalability of a large cloud deployment can introduce certificate management issues that slow down operations. And with OpenStack, the range of cloud services is broad, including messaging queues, access and configuration policies, logging services and various other modules.

In many ways, the world of cloud security is different than traditional firewall management, switch and router control and load balancers. The cloud flattens the network topology, and almost everything is virtual. In addition, the number of security tokens can be staggering, authentication certificates can run into the many thousands and the number of sessions being generated in Secure Socket Layer is much higher. Any one of these components can create a vulnerability point.
Exploring the top OpenStack security challenges

With OpenStack, the cloud security challenge is compounded because the technology is a work in progress. Some of the tools have deficiencies that need to be addressed. For instance, Horizon, the OpenStack dashboard, is missing two-factor authentication. Horizon is a Web-based solution that is both admin- and tenant-facing. It’s a powerful tool for managing cloud resources, but any vulnerability could impact a large number of users, making this a hot target for hackers. Keystone, the OpenStack authentication service, is pluggable for multiple forms of authentication, so an admin setting up this module should aim for the most robust system possible.

There are other OpenStack security factors to consider. For example, because of OpenStack’s modularity, log structures vary, which makes it difficult to prove compliance and secure operations during an audit. While the audit process for any cloud can be a challenge, it should be done regularly. For OpenStack, an audit should involve validating Keystone’s integrity, and looking at patching and levels for code and policies. Log mining using Splunk or other tools makes it easier to audit log activities, though monitoring capabilities, such as those provided by a dashboard like CERN’s Lemon, are also useful. Tools like Puppet can also help simplify deployments.
Best practices for OpenStack security

When deploying an OpenStack-based cloud, there are general best practices organizations can follow to protect their environment from threats.

For instance, because there are many OpenStack authentication certificates, it's tempting to give them long lifespans, but with a flattened system like OpenStack, it is dangerous to do so; a single security failure can lead to wide exploits. It's a best practice to keep certificate lifespans as short as possible.

In addition, most OpenStack operations are driven by policies. At low and medium scale, this is easy to manage, but at a larger scale, it's difficult to maintain consistent policy levels across all instances. The rapid pace of evolution within the OpenStack module family makes manual management difficult, so use a protocol management tool to avoid errors. Exploits that attack clusters by looking for down-level services are common, and as future policies start to control software-defined infrastructures as well as instance management, we can expect this to become even more fertile ground for hackers.

Organizations should ensure that access to the OpenStack control plane is restricted and well protected. The data plane is another matter; encrypt all data at the source and maintain that encryption at rest.

Despite potential risks, an OpenStack private cloud can have security advantages over the public cloud. Generally, access to the private cloud is
much more restricted, and organizations can deploy detection tools, such as those for file and deep packet inspection, data loss prevention and intruder detection, to improve security.

Still, given all the challenges of multi-tenancy, most public cloud providers have developed an aggressive security approach that can lend best practices and tools to the OpenStack community. The maturity of public cloud providers like Amazon Web Services (AWS) and Azure means they've already fought, and won, many hacker attacks.

OpenStack security is maturing fast. It should end up at the same level as all three major public clouds -- AWS, Azure and Google -- and benefit from being deployed in private environments, where additional tools can restrict data access.

Next article
Assess Cloud Security tools

Build a wall around your cloud with security tools

Cloud is always evolving, which means cloud security technologies need to evolve alongside it. Hybrid and multicloud environments present new cloud security challenges and risks as data moves between on premises and the cloud. To address this vulnerable gap, cloud access security brokers (CASBs) focus on protecting that in-between area. Cloud security tools are also becoming more specialized, targeting certain areas such as data, through encryption, or user authorization, through IAM management. Explore provider and third-party tools to reduce cloud security threats.

Cloud access security brokers fill critical enterprise void

Paul Korzeniowski, Freelance Writer

As security tops management concerns in 2016, cloud access security brokers are gaining attention from enterprises. Data security is paramount when enterprises move data center systems from their own premises to the cloud, and cloud access security brokers act as "gatekeepers" to protect their network traffic.
Traditionally, enterprises used firewalls to create a boundary between internal and external communications -- but cloud has blurred those lines. As organizations span their applications between their on-premises computing infrastructure and an off-site location, security tools that will protect data as it moves across both environments are in high demand. Cloud access security brokers, or tools that users place between internal systems and cloud service providers, help do this. They also allow enterprises to see who is using cloud services and what data is being stored and transmitted.

**Weighing the pros, cons of cloud access security brokers**

Cloud access security brokers offer a number of benefits. First, they establish barriers that reduce risk and security threats by tracking the movement of authorized users, internal threats and potential hackers. The
systems are also flexible; in addition to identifying potential threats, they provide varying degrees of policy enforcement.

For instance, an organization might use a cloud access security broker to discover that 30% of its employees are designated as system administrators with privileged access -- and such a high percentage could expose them to potential risks. A cloud access security broker also offers retroactive analysis, allowing enterprises to back date system activity and locate the origin of suspicious behavior.

Despite their benefits, cloud access security brokers pose some challenges. For example, to optimize their cloud security strategy, organizations should integrate cloud access security brokers with existing security products. However, the integration process can be time-consuming and difficult. Since cloud access security brokers are relatively new, the application program interfaces to connect to other security products may not be developed, so the customer has to take on that work itself.
Another challenge is that the cloud access security broker market changes often via mergers and acquisitions. The process of folding a startup into an established firm requires time, money and patience. Sometimes, the melding does not go well because of issues, like corporate culture conflicts, so customers become saddled with dead-end products.

What's to come in the cloud access security broker market

While cloud access security brokers are still new, they are poised for growth. In 2015, fewer than 5% of large businesses had installed them, but 85% of these firms will do so by 2020, according to analyst firm Gartner. The predicted growth is attracting various startups, including Bitglass, CloudLock, Elastica, ManagedMethods, Netskope, Palerra and Skyhigh Networks. Additionally, established vendors have entered the market through acquisition, such as Microsoft, which acquired Adallom, and Palo Alto Networks, which acquired CirroSecure.
Will a cloud access security broker impact users' experience?

Stephen Bigelow, Senior Technology Editor

A cloud access security broker is a tool that intercepts and manages traffic between cloud applications and users. While it can help secure a cloud environment, the tool may also impact users in undesirable ways, potentially decreasing productivity and leading to shadow IT. When evaluating a cloud access security broker, business and IT leaders need to consider the effects on user privacy, application usability and endpoint mobility.

A cloud access security broker tool deals with private employee traffic, meaning employees may be resistant to using applications that they feel puts personal traffic under a security microscope. Cloud access security brokers must be able to use policies or processes that accommodate a company's written acceptable use standards that every employee agrees to.

If adding a cloud access security broker tool slows cloud application performance or makes the application more difficult to use, users may shy away from that application. Instead, they might seek an alternative cloud application that is not constrained by the cloud access security broker -- which could increase shadow IT risks. IT teams should test and evaluate application performance both with and without the cloud access security broker to gauge the tool's impact on application performance. Then, they
E-guide

In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

should use the results of that evaluation to optimize the application, adjust the infrastructure or select an alternate CASB tool.

A cloud access security broker also accommodates various endpoint devices, since users expect to log in to cloud applications from an increasingly diverse array of products. This kind of endpoint flexibility and cloud application persistence have been important factors in cloud adoption, and cloud access security broker tools should not inhibit that flexibility to any noticeable degree. Otherwise, users may resist using the cloud application in favor of other applications that a cloud access security broker does not protect. However, with cloud access security brokers gaining popularity, vendors will likely address this problem moving forward.

Next article
Four ways to streamline cloud access security broker adoption

Stephen Bigelow, Senior Technology Editor

Security remains problematic for enterprise IT. The struggle to ensure application availability while protecting corporate data is even tougher when the business integrates public cloud services.

One emerging tool to end the struggle is a cloud access security broker. With a cloud access security broker, IT teams can enforce a multitude of cloud security policies. But these tools are not created equal, so it’s important for organizations to consider potential issues and assess each offering carefully.

Here are four tips to more effectively choose and deploy a cloud access security broker.

Define your goals

One of the recurring problems with enterprise tools is that organizations lack a clear goal for deploying them. A cloud access security broker can't do everything, so start with a clear understanding of why you're deploying one.

A cloud access security broker -- such as those from Palerra, Elastica, Skyhigh Networks and Netskope -- usually imposes an independent set of security policies between the enterprise and the cloud service provider,
such as Amazon Web Services (AWS) and Google Cloud Platform. But sometimes, the goal might be to discover and restrict shadow IT operations, or identify weak or liberal security policies. In other cases, the cloud access security broker might play more of monitoring and management role, allowing business units to see how cloud services are used -- an advantage for cloud budgeting.

**Review the feature set**

Cloud access security brokers offer a range of features. They might give administrators insight into utilization of cloud services; use packaged templates, custom policies and machine learning to monitor behaviors and spot risky activities; generate logs, send alerts and create detailed reports for administrators; and even take some remedial actions to enforce established security policies. A cloud access security broker can also integrate with existing IT platforms, such as Lightweight Directory Access Protocol, identity and access management tools, ticket and helpdesk systems, single sign-on and other security tools.

Review the cloud access security broker feature set thoroughly to ensure it fits your needs -- or identify feature gaps that may demand additional security investments. The role of a cloud access security broker is still relatively new so careful testing and evaluation is vital.
Evaluate the scope

Organizations can tailor a cloud access security broker to suit specific cloud services or platforms. These service-specific tools can perform reliably, but only for the intended service. For example, if the business develops cloud software that runs on AWS, it may need one tool for AWS and another for the cloud software repository, such as GitHub. Also, if a business changes cloud platforms, it may need to invest in another cloud access security broker. Be sure to budget for multiple tools, if necessary.

Locally hosted cloud access security brokers require updates, but, in some cases, the updates can be disruptive. Businesses that deploy a cloud access security broker in-house will need to integrate the platform with existing patch and change management tools.

When cloud access security brokers are delivered as a third-party service, users face the same possibility of service outages or disruptions that can occur with any other software as a service offering. The provider must stand behind a suitable service level agreement (SLA) that meets the business' security and compliance requirements.

Assess the operational models

Organizations can deploy a cloud access security broker in multiple locations. Each location can offer unique benefits and capabilities, so it's important to understand where the tool will operate most effectively.
Deploying cloud access security brokers locally is often the preferred model, allowing the tool to see all network traffic, manage identities and access control to the group, device or geographical level and employ local encryption to prevent unauthorized access. However, a local deployment requires IT to manage and support another system.

Cloud-based security brokers can be easy to adopt, but establishing encryption control may affect cloud applications' ability to process data. For example, if a cloud access security broker encrypts financial data, the financial cloud app intended to use that encrypted data may not be able to decrypt it. These products also experience the same availability issues that any other cloud application faces, so if the tool becomes unavailable, the cloud applications it protects may also become unavailable.

Some cloud access security brokers may also touch endpoint devices through endpoint encryption. This requires a policy link between the tool and the endpoints that enforces central security policies, drives encryption and allows a selective wipe of data if the employee leaves the company or the endpoint device is compromised.
The cloud IAM market evolves to meet old and new IT challenges

**Alan Earls**, Contributor

Access controls continue to play a key role in many companies' cloud security strategies. As a result, the identity and access management market is poised to grow significantly over the next few years.

In general, cloud-based functionality moves costs from a Capex to an Opex model, while offering greater agility and faster time-to-value. The cloud identity and access management (IAM) market is estimated to be about $600 million, and projected to grow to $1 billion in 2017, said Gregg Kreizman, research VP at analyst firm Gartner. Much of that revenue will be divided between newer players, such as Okta, OneLogin, Ping Identity and Centrify, and more established companies, such as IBM, SailPoint and Salesforce.

One driver for the cloud IAM market, beyond the simple lure of cloud, is that some organizations have trouble finding the necessary skills to support on-premises IAM products, Kreizman said.

"The cloud market really got started with small- and medium-sized businesses with challenges delivering access to needed resources for their workforce using on-premises IAM," he said.

But now, cloud identity and access management tools are finding their way into larger companies, as well.
"Initially, we typically got inquiries about cloud IAM from companies with 300-600 users, but now it is often inquiries about 2,500 seats and even 10,000 seats or more," Kreizman added.

Growth in the cloud IAM market will likely continue over the next few years, especially since the market has sort of "congealed around the two vendor types," said Merritt Maxim, senior analyst at Forrester Research. Like Kreizman, he sees two camps of cloud IAM vendors: the "born in the cloud," software as a service (SaaS) players, such as OneLogin and Centrify, and incumbent companies, like IBM, CA, Oracle or Microsoft.

The latter group is established companies that have also launched their own SaaS offerings, usually based on their on-premises IAM products.

"There is a healthy ecosystem now with a variety of architectures," Maxim said.

So, which vendors lead the cloud IAM market? It's not clear, according to Maxim. "Our surveys show that the market penetration of IAM is still fairly low -- between 40% and 50% -- so there is still a lot of whitespace out there for growth," he said

**Single sign-on a big driver of cloud IAM market**

Across the board, the killer user case for cloud IAM is still single sign-on -- the most in-demand model for user login. With single sign-on, a user can log
In this e-guide

Introduction

Uncover Common Cloud Threats

Form a Cloud Security Strategy

Assess Cloud Security Tools

Test Your Cloud for Weakness

Cloud Security in the News

Cloud Security Terminology

In, typically through a portal, and from there access all the cloud apps she needs, such as Salesforce or Office 365.

"That is not so much a security play as a convenience play," Maxim said. "There is a security benefit, but that may not be how it comes in to the organization," he said.

In many cases, the cloud IAM market closely parallels the on-premises market of 15 years ago. Then, the driver for IAM was also single sign-on. Once organizations got that capability, they started looking into deeper features for ID management, account provisioning and verifying who has access to what.

A similar trend is playing out now in the SaaS world; users are first focused on single sign-on, with more user management and ID management features added over time. The main difference is the delivery model.

"From the end-user perspective, it all looks similar," Maxim said. "The end users might not even know if an application is on-premises or in the cloud, but they want single sign-on convenience."

Data security in the cloud

How much do you know about protecting enterprise data in the cloud? Take this quiz and find out.
Mobility, shadow IT create new cloud IAM challenges

However, single sign-on now presents more of a challenge than it did in the past, noted Garrett Bekker, senior analyst, information security at 451 Research. While IAM has evolved from an on-premises application to a cloud-based service, the world has changed, and users increasingly access corporate resources from mobile devices—many of which come from the BYOD trend.

"With mobile use cases, the idea of a corporate perimeter and inside versus outside are gone; your main control is now authentication and access controls to verify that the user is the user they claim to be," he said.

That problem is spawning a related category of offerings, according to Bekker—namely, cloud application control or cloud access security brokers (CASBs). "Those approaches also address the shadow IT problem and can help you determine if employees or others are using unsanctioned SaaS applications that have not been vetted for security risks," said Bekker. Offerings with this kind of capability can "say 'yes' to single sign-on and 'yes' to accessing Salesforce, but 'no' with regard to certain pages that might have sensitive data," he explained.

"The starting point for the CASB [tools] is that you can't secure what you don't know about," Bekker said. "Discovering what your employees are using is a starting point."
Data encryption, for both data at rest and in motion, should be a standard practice in cloud computing. But despite the nearly ubiquitous availability of encryption within the enterprise and through cloud providers, common encryption technologies are not always enough for some organizations.

Some businesses, for example, are subject to strict compliance regulations, such as the Health Insurance Portability and Accountability Act, which require formal agreements between healthcare businesses and their partners, including cloud providers. And while cloud providers may meet some of a business’s encryption needs, many enterprises are turning to cloud security providers to help fill in the gaps.

**The benefits of centralized cloud data encryption**

Centralized cloud data encryption providers such as Vaultive and CipherCloud offer enterprise-grade technology that enables businesses to encrypt their data while it is still on the trusted corporate network. This
ensures that all data sent to and stored on the cloud is encrypted. Only the highest-level administrator of the cloud service can access encrypted data. And if the cloud provider is hacked or required to release data for legal reasons, only encrypted data is released.

CipherCloud for Amazon Web Services (AWS) is an encryption service specifically designed for the AWS cloud with support for Relational Database Service and Redshift. The service uses AES 256-bit encryption paired with centralized key storage and management, and stores the encryption keys on CipherCloud servers. CipherCloud encryption is implanted on the application driver where it encrypts data locally before moving it between points.

CipherCloud allows admins to encrypt data on a per-field basis. For example, an online sales system might encrypt only payment information using the fine-grained CipherCloud tools, while leaving other data, such as a shipping address, in plain text.

An advanced feature of CipherCloud allows administrators to generate encrypted data that uses the same data type and size of the unencrypted data. This is especially important when businesses want the protection of encryption, but do not want to modify their database schemas.

Sometimes, a business will want to use a separation of duties when handling encryption. CipherCloud's key management functions mitigate the risk of an insider having unacceptable access to keys and, therefore, encrypted data.

Similar to CloudCipher, Vaultive has a specialized service for a single cloud provider -- Microsoft. Vaultive offers encryption for a range of Microsoft
services, including Office 365, Yammer, OneDrive and Dynamics CRM Online.

Vaultive operates as a stateless layer that serves as a door between a cloud service and user endpoints. For example, Vaultive, along with partner BitTitan, encrypts data for Office 365 as it enters the cloud. From that point on, the data remains encrypted until it returns to an end user with the authority to view it. Data traveling to and from the Office 365 cloud always passes through a network encryption layer managed by BitTitan.

Prepare for centralized encryption risks

Despite the benefits of centralized encryption services, they can also introduce a potential point of failure in an organization's infrastructure. If a gateway is down or an encryption software as a service (SaaS) is unavailable, you can't send new encrypted data to the cloud. In addition, your encrypted data in the cloud will be inaccessible until the problem is resolved.

One option when deploying an on-premises gateway is to use its high availability and scalability. To do this, run multiple gateways and either load balance between them or keep one on standby. Alternatively, if you can tolerate a longer time to recovery, you could bring up a new gateway manually when the primary gateway fails.

When using encryption SaaS, be sure the SLAs meet your expectations for scalability and availability. The SLA should also specify compensation for failures to meet agreed service levels.
Centralized **cloud data encryption services** are an important part of the cloud ecosystem and will be especially helpful to companies with demanding compliance regulations. However, always anticipate the risk of temporary failures in the process and plan accordingly.

**About the author:**
*Dan Sullivan holds a master of science degree and is an author, systems architect and consultant with more than 20 years of IT experience. He has had engagements in advanced analytics, systems architecture, database design, enterprise security and business intelligence. He has worked in a broad range of industries, including financial services, manufacturing, pharmaceuticals, software development, government, retail and education. Sullivan has written extensively about topics that range from data warehousing, cloud computing and advanced analytics to security management, collaboration and text mining.*
Climb into a hacker's mind with cloud security testing

One of the best ways to find cloud security is to attack like a hacker would. Testing your cloud is a critical part of a cloud security strategy. Not all environments have the same weak spots and there is no standard test that will discover all issues. In addition, don't assume that certain workloads don't need to be tested, just because they're inaccessible from the internet. When it comes to cloud security challenges and risks, don't overlook internal threats. Testing your cloud is the only way to know where your cloud needs some extra security attention, whether external or internal.

Penetration testing is an IT security practice designed to identify -- and address -- any vulnerabilities a hacker could exploit. And just as they would with a traditional data center, many IT shops perform penetration tests on their public cloud environments. Whether testing for AWS, Google or Microsoft Azure clouds, here are some best practices to formulate a penetration testing plan for public cloud.

First, since penetration testing looks a lot like an attack, it is important to coordinate with cloud providers before performing such tests.
Next, create an inventory of what to test, including servers, endpoints, applications, Web services and persistent data stores. You can conduct penetration tests using a tool like Metasploit or a third-party service such as Tinfoil Security’s security scanning tool. But in either case, you need a well-defined list of components to test.

Then, determine which security tests to perform. The Open Web Application Security Project (OWASP) maintains a list of their top 10 security vulnerabilities in Web applications. This is a good starting point, and is considered the minimal set of vulnerabilities for which organizations should test. The list includes injection attacks, broken session management and authentication, cross site scripting and security misconfiguration.

Be sure to test all points of potential attack. You might expect customers to always use the Web interface you have provided, but attackers can exploit Web services or database servers directly. Test all public-facing access points in your application stack, including API functions and application interfaces.

If you have the time and resources, also test services that should not be accessible from the Internet. For example, you might configure your database server to accept connections only from your application server. Someone might think the database is inaccessible from the Web, and therefore protected, but that is not necessarily true.

Security controls can fail. If the application server has access to the database server and is compromised, attackers can use the application server as a host for an attack on the database server. Without compromising
needed functionality, harden the security of your database server as much as possible. Follow defense in depth practices and put multiple controls in place to protect data and system resources. Database server security shouldn't depend on a well-secured application server.

Lastly, remember that not all attacks will originate from outside your organization. An insider may have legitimate access to a number of systems that can be exploited for malicious purposes. Review logs to determine if you are capturing sufficient information to respond to an actual attack. Also, test the capabilities of security information and event management software. Make sure alerts are generated as expected, and present security testing data in a way that allows experts to quickly determine the cause of the alerts.
Minimize threats through public cloud security testing

David Linthicum, Cloud analyst

Due to public cloud's multi-tenant environment and shared resources, many organizations are skeptical about a public cloud provider's ability to secure their data.

According to a 2014 study from analyst firm Current Analysis, which polled over 600 IT decision makers worldwide, 58% of respondents deployed private cloud because of public cloud "security" and "data privacy" concerns.

But, in reality, public cloud providers are not responsible for securing your data -- you are. Providers are, however, responsible for supplying the necessary mechanisms to meet your security requirements.

There is no one-size-fits-all approach to public cloud security. Organizations must determine their specific security requirements, and map those to the appropriate technology. In some cases, the cloud providers offer that technology. But in other cases, organizations will require third-party services.

However, there are ways to identify and fix holes in public cloud security. The most effective way is to test.
Strategies for public cloud security testing

Public cloud security testing begins with selecting a portion of the cloud environment to test. Anything that can be isolated, such as a single database, container cluster or application instance, will work.

From there, create a cloud security testing strategy. One method is to try to penetrate the part of the system being tested with any exposed access mechanism -- such as a user interface, set of APIs, or primitive access points that lead directly to the infrastructure.

To simulate attacks, use automated security testing tools, such as Core Security Technologies' CloudInspect or Trustwave's Managed Security Testing. Many of these tools can also gather information on response times and defense methods. While these tools vary greatly, they're typically designed to test specific cloud security components. As a result, organizations are likely to use between three and five different tools.

Beware of side-channel attacks

One threat to guard against is a side-channel attack, a method that one virtual machine can use against another within the cloud to comprise the target VM's encryption key.

Public cloud providers pay special attention to side-channel attacks, which makes it unlikely to experience one. However, as public cloud providers
In this e-guide

Introduction

Uncover Common Cloud Threats

Form a Cloud Security Strategy

Assess Cloud Security Tools

Test Your Cloud for Weakness

Cloud Security in the News

Cloud Security Terminology

constantly release new versions of their cloud services, it's important to check whether a new vulnerability is introduced.

Finally, determine which employee will perform cloud security testing. As a rule of thumb, never let developers take on that role. Because they're so close to the cloud, developers are unlikely to spot issues. Instead, use a separate group that is dedicated to security and security testing. These people could be in your company, or third-party consulting firms that focus exclusively on cloud security and penetration testing.

Despite many users' concerns, public cloud security is solid if approached and tested carefully. Security testing validates whether an organization has chosen the right security technology, as well as identifies and fixes vulnerabilities before they become real issues.

About the author:

David “Dave” S. Linthicum is senior vice president of Cloud Technology Partners and an internationally recognized cloud industry expert and thought leader. He is the author or co-author of 13 books on computing, including the best-selling Enterprise Application Integration. Linthicum keynotes at many leading technology conferences on cloud computing, SOA, enterprise application integration and enterprise architecture.

His latest book is Cloud Computing and SOA Convergence in Your Enterprise: A Step-by-Step Guide. His industry experience includes tenures as chief technology officer and CEO of several successful software companies and upper-level management positions in Fortune 100 companies. In addition, he was an associate professor of computer science for eight
years and continues to lecture at major technical colleges and universities, including the University of Virginia, Arizona State University and the University of Wisconsin.
Spot cloud security strategy flaws before it's too late

David Linthicum, Cloud analyst

There are certain public cloud benefits that seem undeniable. Organizations that embrace cloud platforms often see a number of advantages -- both from a business and technical standpoint. These range from reduced capital expenses to increased flexibility and scale. But, in the realm of IT security, the public cloud still gets a bad rap.

While perceptions are starting to change, many enterprises are still wary of the public cloud when it comes to application and data security. For some IT pros, the thought of relinquishing control to a third-party cloud provider seems like the stuff of nightmares. But, with the right security strategy in place, the public cloud can be just as, if not more, secure than traditional on-premises environments.

Of course, you can't create a solid public cloud security strategy overnight. There are a number of critical decisions to make and steps to take before you can ensure your cloud data is safe.

Compliance standards, for starters, are a big one. Organizations in vertical markets, such as healthcare, need to make sure their cloud environments -- and cloud service providers -- comply with regulations such as the Health Insurance Portability and Accountability Act. Other industries, such as financial services, need to pay particular attention to Personally Identifiable Information guidelines.
Beyond compliance, IT security teams need to identify their unique application security requirements and determine whether traditional security approaches -- such as user IDs and passwords -- are enough to keep data safe. In many cases, more advanced security practices, such as proactive monitoring and identity and access management, will be a must -- especially for new applications.

To meet these needs, organizations should consider using the cloud-native security systems each public cloud platform provides, such as Amazon Web Services' Identify and Access Management service. Third-party security products can also help meet these needs, but integration could be a challenge.

Organizations that don't think they need to meet compliance regulations, or that are comfortable with their security strategies, should review their cloud security framework to ensure 100% confidence in that stance. When the integrity of enterprise data is on the line, it's always worth a second look.

Even after crafting a cloud security strategy, the work doesn't stop there. Ongoing and automated security testing, and integrating security into your day-to-day IT operations, will be critical to keep the bad guys at bay.

Consult the decision flow chart above to steer your organization toward a public cloud security strategy that works best.

Next article
Test your ability to avoid cloud security risks

Nicholas Rando, News Production Editor

For some organizations, cloud computing is a perfect fit. For others, cloud security risks are tough pills to swallow. Scalability, agility and a pay-per-use model are attractive features that entice many businesses to consider cloud deployment. But despite its benefits, some organizations believe the cloud is risky business.

Security is a common question mark that hovers over cloud, and 2014 certainly didn't help. Major security breaches at retail giants Home Depot and Target, as well as the iCloud and Sony hacks, drudged up significant cloud security concerns. However, cloud computing wasn't directly responsible for any of these security bugaboos. Nonetheless, many questioned cloud's ability to lock down sensitive information.

While there is inherent risk in storing information in a multi-tenant public cloud, encryption and other methods can help enterprises avoid many issues. Test your degree of knowledge on cloud security risks and how to avoid them.

Next article
Cloud Security in the News

Stay up to date on cloud security

Cloud security has been stealing tech headlines with data breaches, new technologies and improved compliance agreements. These stories reveal new cloud security challenges and risks, as well as the improvements being made to answer those concerns. Top cloud providers, such as Amazon Web Services, Azure and Google, continue to compete with each other to provide the best security services possible, with each new update bringing more protection to the cloud. Providers are also keeping a close eye on the transfer of personal data between the U.S. and Europe.

Cloud vendors saw end of Safe Harbor agreement coming

Trevor Jones, News Writer

The dissolution of a trade agreement for the transfer of data between the U.S. and Europe shouldn't dramatically impact cloud vendors or customers in the near term, but does highlight how a lack of clarity around data privacy will hang over the industry in the long-term.

Safe Harbor, a legal framework for data transfers based on an agreement in 2000 between the European Union (EU) and the U.S., was struck down this week by the European Court of Justice. Roughly 4,500 companies used the
agreement, but the decision is something cloud vendors are prepared for with contractual language and a glut of new data centers across Europe.

"This is really a formal nail in the coffin that's already been filled," said Adrian Sanabria, senior security analyst with 451 Research LLC in New York. "It's not a surprise to anyone and I'm not sure how much it changes."

Seen as a victory for privacy groups, the ruling does leave some uncertainty about data transfers. Tech advocacy groups on both sides of the Atlantic have called for interim guidance from the pertinent governing bodies, as well the implementation of a new Safe Harbor agreement and long-term legal changes around surveillance regulations in the U.S.

Smaller companies are expected to be most impacted as they lack the financial and legal means to get around the ruling. There are still mechanisms, however, that companies can use to transfer data, including binding corporate rules and a presence in the EU to keep and store sensitive data.

Microsoft and Amazon each put out statements saying the ruling will not affect their customers' data, citing approval from EU data protection authorities for their specific agreements and compliance with EU Model Clauses.

Google, considered the other hyper-scale public cloud vendor, declined to comment, but pointed to a statement from the Internet Association, which represents Google, Amazon, Facebook and other tech giants. The statement called for reforms while acknowledging that larger companies can continue data transfers.
The decision doesn't mean companies have to discontinue their data transfers immediately, but it does provide authorities in the EU to investigate those transfers and shut down those communications if they aren't within the data privacy laws of the nation in which the information lies. Companies were essentially self-reporting on their compliance under the Safe Harbor agreement.

Many of the Silicon Valley tech giants have been in the crosshairs of the EU for some time. And while they may use this to go after them, don't expect anything overnight, because of the influence these companies hold with the public, said Renee Murphy, senior analyst for Forrester Research Inc., in Cambridge, Mass.

"If you shut off Google [in Europe] tomorrow there would be a riot," Murphy said.

For a typical cloud customer, there should be nothing to worry about, as the onus is on the vendor to ensure the data resides where it's supposed, Murphy said. It also shouldn't come as a surprise that these large cloud vendors can continue to operate business as usual.

"Of course Amazon is well positioned," Murphy said, "The reason they were so well positioned is they knew this was a problem in the first place."

In fact, some see this ruling as an opening for public cloud vendors and third-party security providers.

"It makes a big case for companies getting into both security more and adopting the cloud," Sanabria said. "The one thing about the cloud is it
makes you agile enough that you could move your data center from one fiscal center to another."

It's also hard to look at some of these giant companies solely as U.S.-based, as they have subsidiaries and huge presences abroad and have to take the legal ramifications of those nations' data laws just as seriously as they do those in the U.S., he said.

There's also the opportunity for non-residency related solutions to the problem, including tokenization that allows the data to remain in its country of origin, analysts said.

**Safe Harbor questions remain**

Web-scale vendors aside, European companies remain troubled by the lack of certainty that this ruling has created.

"We're operating a bit in a vacuum as organizations," said Christoph Luykx, EMEA government relations director for CA Technologies. "We want to respect the court case, but at the same time, there's only so fast we can go for finding solutions."

CA, a global software company headquartered in New York, has mechanisms in place to move around data and is preparing internal guidance so services aren't disrupted. But discussion have to be worked out up and down the entire supply chain.
"The impact on smaller customers that would also like to use cloud services or have offerings, for them they are finding these legal discussions very complicated," Luykx said.

And regardless of what happened to the Safe Harbor agreement or what type of civil agreements have been reached, the biggest concerns about criminal inquiries and data privacy remain unanswered, said Daniel Arthursson, CEO of CloudMe, a Swedish sync and storage provider.

"The single person designated as data controller in the European Union company will be liable," Arthursson said. "It doesn't really matter what you have signed; if there is a breach you are liable."

If anything, this week's ruling only made it clearer to European companies that the Safe Harbor agreement didn't protect them, he added.

"Something needs to be done between the European governments and the U.S.," Arthursson said. "The implications for both sides will be huge. It's a crazy situation."

The ruling sprang from an Austrian citizen's challenge to Facebook's transfer of his data outside the EU in light of the National Security Agency surveillance revelations. So while the final decision came as no surprise, how it came about is telling, analysts said. It's striking how one individual was able to bring down such a massive agreement and it will likely take civil suits and other legal action in the U.S. before the full extent of data privacy is established.
"We're going to have to have one person suing Google and winning some weird class action lawsuit," Murphy said. "It's going to take us going to the Supreme Court in order to find the true limits."

---

### Data privacy in the spotlight with Privacy Shield, Microsoft

**Trevor Jones**, News Writer

Two long-simmering questions about data residency requirements have been answered, but neither resolution will fully quell cloud providers' lingering uncertainty around international data transfers.

Last week, the European Commission formally adopted the U.S.-EU Privacy Shield to provide legal cover for transatlantic data transfers. Meanwhile, a federal court overturned an order for Microsoft to provide access to a customer's emails in Ireland. Both moves provide a degree of clarity to cloud providers and customers that rely on these global networks of data centers to conduct business around the world, though more challenges lie ahead.

Privacy Shield fills the void left by the dissolution of the Safe Harbor agreement last October and is seen as an improvement for privacy and transparency, though some advocacy groups feel it still doesn't go far enough. It replaces the self-reporting model that 4,500 companies relied on through Safe Harbor with a higher bar for approval and regular reviews of participants' practices by the U.S. Department of Commerce.
The initial agreement on the Privacy Shield framework was reached in February, though there have been several adjustments since, including restrictions on bulk data collection and surveillance by the U.S. government.

CA Technologies, a global software company headquartered in New York, relied on corporate binding rules and worked with customers to update contracts with new clauses to respond to the "legal vacuum" caused by the dissolution of Safe Harbor, said Christoph Luykx, the company's EMEA government relations director.

Questions from CA customers following the end of Safe Harbor have been infrequent or low on the priority list, and mostly came up during specific contract negotiations or renewals. CA didn't have a set of stipulations it wanted to see in the new deal, as long as the framework would reflect the EU Court of Justice's concerns and provide businesses with stability and legal certainty, Luykx said.

Companies can start signing up on Aug. 1, and CA likely will sign up for Privacy Shield after its legal team reviews the full, final text. "We're in safer waters, but it's not smooth sailing, because we do have some more challenges ahead," Luykx said.

Safe Harbor was in place for almost 15 years before it was struck down last fall by the European Court of Justice. The court's ruling was based on an appeal by Max Schrems, an Austrian privacy activist who raised concerns about Facebook's use of customer data. Schrems reportedly plans to appeal Privacy Shield, as well -- but even if he doesn't, industry observers expect some form of legal challenge to crop up in the next couple of months.
Privacy Shield is an improvement from Safe Harbor, but there’s still plenty of gray area, and the pending legal fights only add to the uncertainty for cloud service providers and customers, said Duncan Brown, research director for European security practices at IDC.

Some companies won’t care about the effect on data transfers, but for those dealing with sensitive data, it’s important to understand Privacy Shield isn’t the only option, he added. Cloud service providers can use binding corporate rules or insert model contract clauses into contracts with EU customers.

"We’re recommending vendors and end-user clients seriously investigate one or both of those mechanisms as a backup, and possibly as a long-term answer, to Privacy Shield," Brown said.

Cloud data center propagation not a panacea

Microsoft has said it will implement Privacy Shield, but it’s unclear if other major cloud vendors will follow suit. Amazon, Google, IBM and Oracle, among others, offer EU model contract clauses for their customers.

Part of their strategy to get around data sovereignty and privacy concerns is to build data centers inside Europe, opening a crowd of new facilities in recent years, with more planned or now under construction. The vendors have built their networks to allow users to restrict the flow of data, so it
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

stays inside Europe, or even inside a specific data center, in case the information is restricted from leaving that country.

CA is not a cloud infrastructure provider, but it does deliver software as a service hosted in multiple locations. Everyone is looking at where to put data centers based on a wide range of criteria, including cost to run and proximity to users, Luykx said. The legal ramifications are important, but these safeguards may not be sufficient for a company outside of Europe servicing a customer on the continent and needing access to databases in the EU, he added.

"A lot of the focus is on keeping the data in one data center, but it doesn't work like that," Luykx said. "Data still needs to flow."

Microsoft's win ripples through the clouds

The Privacy Shield adoption was followed just days later by a court ruling in the U.S. that signaled a further push to protect data sovereignty and quash an effort that could have deeply affected how cloud providers operate.

The Microsoft case pertained to a December 2013 warrant issued under the Stored Communications Act that required the company to turn over the contents of a customer's emails stored outside the U.S. Federal prosecutors believed the account was being used for drug trafficking, but the warrant was overturned last week by the U.S. Court of Appeals for the Second Circuit.
In the earliest days of cloud computing, the pitch was it didn't matter where your data resided, but it turns out that thinking was wrong, Brown said. This ruling is important because it essentially prevents U.S. law enforcement agencies from being able to reach into any U.S.-based companies' data centers around the world to extract information, he added.

"The fact that they won is not only good news for them, but good news for everybody, because it reasserts that residency is important," Brown said.

More than two dozen media and technology companies filed amicus briefs in support of Microsoft, including cloud vendors, such as Amazon, Salesforce and Rackspace. The ruling "paves the way for better solutions to address both privacy and law enforcement needs," said Brad Smith, Microsoft president and chief legal officer, in a blog post.

Smith called for replacement of the decades-old laws governing data protection with a new International Communications Privacy Act, and he praised the work by the U.S. Justice Department to pursue a bilateral treaty with the United Kingdom on this particular issue.

All of these issues likely will be revisited when the General Data Protection Regulation goes into effect in the EU in 2018. Europe is leading the way on this issue and the new agreement "raises the bar" for data protection and privacy, including extraterritorial clause that covers data about EU citizens irrespective of where that data is physically processed, Brown said.

So, despite the lingering uncertainty around international data transfers, the Microsoft case and Privacy Shield have, at very least, served as a wake-up call.
"What [these events] have done is shed a light on the whole area of data transfers and data residency," Brown said. "There is a much better understanding of the issue, and understanding by U.S.-based cloud providers that it genuinely is an issue for some EU-based companies."

Trevor Jones is a news writer with TechTarget's data center and virtualization media group. Contact him at tjones@techtarget.com.
Google cloud security plays catch-up with AWS, Azure

Trevor Jones, News Writer

Google has added security compliance standards to its cloud platform, a critical step toward greater inroads with the enterprise market.

Google last week added International Organization for Standardization (ISO) 27017 certification for cloud security and ISO 27018 certification for personally identifiable information stored in the cloud, in addition to its existing ISO 27001 certificate that’s been renewed for the fourth year. The standards basically serve as an assurance to customers that Google has taken specific internal measures to secure its users’ data.

The certifications already had been received by Amazon Web Services (AWS), Microsoft Azure and IBM SoftLayer, among others.

A few years ago, security was a primary concern for enterprises, but cloud adoption continued at a rapid pace, mostly around testing the platforms. That’s changed, as enterprises are more comfortable with the idea of workloads in public clouds and the benefits of asset management on those platforms, said Adrian Sanabria, senior security analyst at 451 Research.

"It’s being seen as a foregone conclusion," Sanabria said. "Everybody is using cloud, and the only question is, how much are they going to use it and what are they going to use it for?"
Still, enterprises need to see certain regulations and standards before they can put anything in the cloud. "You can't even talk with a business if they're required to have those certifications and you don't have them," Sanabria said.

ISO 27017, which first became available late last year, centers on Google cloud security roles and ensuring networking is in place so that unauthorized parties can't access customers' data. It also requires the vendor to provide customers with adequate monitoring tools.

ISO 27018 focuses on privacy practices for customer data and compliance. It prevents the vendor from using data for advertising and provides protection from third-party requests.

Third-party scrutiny and protection of data sets is a hot-button issue, and customers will need these kinds of assurances before adopting big data services, said Renee Murphy, principal analyst with Forrester Research. It's a positive step for Google, which is usually the last to comply with security certifications.

"If you want to get into the cloud space and want to do enterprise cloud, you should at least be able to prove you're compliant," Murphy said.

Typically, Google doesn't act until it reaches a critical mass of customer demand, she added. It's also far from being ready to take on deeper compliance structures, such as FedRAMP -- Google Cloud Platform is not FedRAMP-compliant, but Google App Engine is.
"They definitely let demand push them in that direction," Murphy said. "They don't go out there to create demand the way AWS does."

Not including the limited FedRAMP compliance, Google now lists nine different privacy and security standards it meets for its platform -- far fewer than either AWS or Azure.

Google Cloud Platform services covered by these certifications include Cloud Dataflow, Cloud Bigtable, Container Engine, Cloud Dataproc and Container Registry. Compute Engine, App Engine, Cloud SQL, Cloud Storage, Cloud Datastore, BigQuery and Genomics, which were previously audited as part of ISO 27001 compliance, will be part of the additional certifications as well.

Though it's important to businesses, ISO standards can't truly be certified in the same way some others are, Sanabria pointed out. There is no certification body to assess against those standards, so it doesn't go beyond the third-party audit.

Trevor Jones is a news writer with TechTarget's data center and virtualization media group. Contact him at tjones@techtarget.com.

Next article
Linode cloud security response draws praise, raises concerns

Trevor Jones, News Writer

Cloud hosting provider Linode is receiving praise for its handling of a string of recent security attacks, but some customers are concerned enough to consider other options.

Linode Manager passwords expired last week and users were prompted to set new passwords after an investigation found unauthorized logins into three accounts. The reset came on top of ongoing distributed denial-of-service (DDoS) attacks the cloud provider faced in its data centers. Linode also faced downtime earlier in 2015 when it had to do a reboot to address security issues around Xen.

The vast majority of Linode cloud customers have been supportive, according to the company, but two users said the string of attacks has them looking elsewhere.

The series of attacks was "quite a big deal" for Dallas-based consulting firm and Linode cloud customer etc.io, which suffered several outages as a result of the attacks, said chief advocate E.T. Cook. Etc.io uses a variety of cloud providers but Linode has been its go-to platform.

"We've been transparent, and although we sympathize with the Linode DDoS situation and won't be abandoning them, we're starting to look at diversifying
and having failovers outside of Linode for all of our primary properties," Cook said.

Making such a move will create challenges, particularly around database replication, but he's convinced it needs to be done.

Munzee Inc., a McKinney, Texas-based scavenger hunt game with workloads hosted in Linode's Atlanta facility, said in a blog post that the attacks lasted 10 days before finally stopping on Jan. 3. The worst of it came the weekend prior, with intermittent uptime resulting in its apps, websites and stores down the majority of that time period.

The post also said Munzee was taking steps to prevent similar downtimes in the future, including hosting servers in multiple data centers or with multiple companies, and possibly changing providers. In an email to SearchCloudComputing, Scott Foster, vice president of technology at Munzee, said the company was making the move from Linode to Amazon Web Services.

An investigation found unauthorized logins into three accounts in the Linode cloud. Two Linode.com user credentials were used on an external machine - meaning they could have been read from Linode's database, either offline or on, Linode said.

There was no indication that any customers' information was accessed, but it's possible that usernames, email addresses, securely hashed passwords and encrypted two-factor seeds could have been read from the user table of its database, according to Linode.
Users of the three potentially affected customer accounts were immediately notified, and no additional evidence was found of access to the vendor’s infrastructure. An unnamed third-party security firm has been brought on to assist in the investigation.

Linode has handled the situation well, based on the information the company has been made available, with an appropriate level of transparency regarding what occurred and the steps taken, said Adrian Sanabria, senior security analyst at 451 Research. Linode also has been smart not to disclose information that customers don't need to know, such as the name of the firm they've engaged to help with the investigation, he added.

"It's nice to see that they're not running all over social media waving a Mandiant-branded flag, or denying responsibility because the attacker was 'super advanced' or 'sophisticated,'" Sanabria said.

The DDoS attacks started on Dec. 25, and over the next week the Linode cloud faced more than 30 attacks of what the firm called "significant duration and impact."

Linode claims to have no information about who is behind the attacks or if the attacks are connected. The company is working with law enforcement officials and plans to have a full technical explanation of the incidents once the attacks stop.

Past examples of DDoS attacks have run concurrent with fraud. Investigators will explore any possible connections but that will be difficult to prove, said Robert Westervelt, research manager at IDC Research.
"Identifying a threat actor is very difficult, and connecting them to multiple incidents further complicates the issue," Westervelt said.

While acknowledging that unauthorized login of three customer accounts is troubling, Westervelt agreed that Linode appears to be responding appropriately. Users are known to adopt poor password practices, but the company used accepted best practices around securely hashing passwords and encrypting two-factor seeds.

Stolen passwords are one of the top risks for cloud services providers, according to Westervelt. One good way [to address this] is to add multi-factor authentication, he said. "Most providers provide it as an optional capability if customers desire that level of protection."

Another common method for attackers to gain access is through chinks in the Web-based management system software, which could have vulnerable components, Westervelt said.

"For Linode, providing transparency about its actions to contain the threat and any remediation steps it has taken, is important for it to maintain the trust of its customer base," Westervelt said.

Trevor Jones is a news writer with TechTarget's data center and virtualization media group. Contact him at tjones@techtarget.com.
Cloud encryption key management becomes table stakes

Trevor Jones, News Writer

The ability to bring your own encryption keys is fast becoming ubiquitous in public cloud, but that doesn’t mean IT pros should retain control.

Security concerns and data center oversight are two primary hang-ups for IT shops averse to adopting public cloud. Amazon became the first major infrastructure as a service (IaaS) vendor to offer bring your own key encryption in 2014 as an answer to some of those critiques. Over the past few weeks, Microsoft and Google have also advanced their cloud encryption key management capabilities.

Vendors at every layer of the cloud stack have added encryption capabilities, and, eventually, all cloud vendors will offer some form of encryption and key management, said Garrett Bekker, senior security analyst with 451 Research LLC, based in New York. Some vendors will opt to do it natively, while others will pass the control to customers so they can check off that box on their list of capabilities, Bekker said.

"It comes down to how important it is for customers to control the keys," Bekker said. "My guess is a lot of customers will be OK with letting service providers control the keys, but it depends on what the data is, what you’re using it for, and what industry and regulatory compliance you face."
And business considerations will affect vendor services, too, with a company such as Google that lags in the market offering key management for free. Other companies like Salesforce.com that need to generate new revenue streams offer native encryption as a premium service.

To key or not to key?

Encryption is considered central to data protection in the cloud, but who should retain its control?

SunGard Financial Systems, which partners with Google to build a big data processing prototype for the U.S. Securities and Exchange Commission, uses Customer-Supplied Encryption Keys for compute resources on Google Compute Engine. The free tool for bringing your own keys became available in beta last week, and it's essential from a risk and regulatory control perspective for this project, said Neil Palmer, CTO at SunGard Consulting Services, based in Wayne, Pa.

All data in the cloud should be encrypted anyway, but the ability to bring your own keys is one of those additions that should help enterprise adoption and increase the ways those customers use public cloud, Palmer said. Still, SunGard doesn't bring its own keys to every project, so it's a matter of weighing if and when key management is the best fit.

"It's just a question from a perspective of effort, time, integration, etc.," Palmer said. "There's a return on investment around key management
required, so if you're BuzzFeed or one of the big media Internet sites, maybe not so much. But if you're healthcare or government work, you may need it."

**Microsoft Azure Key Vault**, which became generally available last month, can be used as a standalone service and allows customers to import keys from their own hardware security modules (HSMs). Microsoft charges $0.03 per 10,000 operations for software-protected keys and an additional $1 per month per key for HSM protected keys.

Similarly, **Amazon Web Services (AWS) Key Management Services** charges $0.03 per 10,000 requests and $1 per month per each key that is created and active. Amazon also has **CloudHSM**, a dedicated HSM appliance that costs $5,000 for each instance, in addition to an hourly fee of $1.88 for as long as the instance is running.

Cloud encryption key management is difficult, and bringing your own keys to a service someone else owns is a non-trivial endeavor that goes against one of the cloud's main advantages of not having to worry about these sorts of things, said Adrian Sanabria, senior security analyst at 451 Research.

"You've got to somehow own the keys and manage to inject them into workloads without exposing them to the cloud provider," Sanabria said. "It is a compromise, where you can't be 100% cloud if you want to manage your own keys."

Public perception about cloud security and regulatory environments with antiquated requirements both play a role for the need for key management, but the point could be moot in five years' time, as customers start to trust
large public cloud providers as good stewards of keys, said Leonard Law, a product manager for Google Cloud Platform.

"As people are transitioning from on-premises to the cloud, there's this notion of control. So by managing your own custom keys that gives customers a lot of peace of mind, but ultimately, it's just less necessary," Law said.

Trevor Jones is a news writer for TechTarget's Data Center and Virtualization Media Group. Contact him at tjones@techtarget.com.

Next article
Cloud Security Terminology

Learn important cloud security terms

To recognize and overcome cloud security challenges and risks, it's important to understand the vocabulary. No matter your knowledge level, here are some basic definitions you should know.

Cloud Computing Security

Margaret Rouse, WhatIs.com

Cloud computing security is the set of control-based technologies and policies designed to adhere to regulatory compliance rules and protect information, data applications and infrastructure associated with cloud computing use.

Because of the cloud’s very nature as a shared resource, identity management, privacy and access control are of particular concern. With more organizations using cloud computing and associated cloud providers for data operations, proper security in these and other potentially vulnerable areas have become a priority for organizations contracting with a cloud computing provider.

Cloud computing security processes should address the security controls the cloud provider will incorporate to maintain the customer's data security, privacy and compliance with necessary regulations. The processes will also
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

Likely include a **business continuity** and data **backup** plan in the case of a cloud security **breach**.

**Next article**

---

### Cloud Access Security Broker (CASB)

**Margaret Rouse**, WhatIs.com

A cloud access security broker (CASB) is a software tool or service that sits between an organization's on-premises **infrastructure** and a cloud provider's infrastructure. A CASB acts as a gatekeeper, allowing the organization to extend the reach of their **security policies** beyond their own infrastructure.

CASBs work by ensuring that network traffic between on-premises devices and the cloud provider complies with the organization's security policies. The value of cloud access security brokers stems from their ability to give insight into cloud application use across cloud platforms and identify unsanctioned use. This is especially important in regulated industries. CASBs use auto-discovery to identify cloud applications in use and identify high-risk applications, high-risk users and other key risk factors. Cloud access brokers may enforce a number of different **security access controls**, including **encryption** and device profiling. They may also provide other services such as credential mapping when **single sign-on** is not available.

CASBs are particularly useful in organizations with **shadow IT** operations or liberal security policies that allow operating units to procure and manage
their own cloud resources. The data that CASBs collect can be used for reasons other than security, such as monitoring cloud service usage for budgeting purposes. Vendors in the cloud access security space include SkyHigh Networks and Netskope.

Cloud Encryption (cloud storage encryption)

Margaret Rouse, WhatIs.com

Cloud encryption is a service offered by cloud storage providers whereby data, or text, is transformed using encryption algorithms and is then placed on a storage cloud.

Cloud encryption is the transformation of a cloud service customer's data into ciphertext. Cloud encryption is almost identical to in-house encryption with one important difference -- the cloud customer must take time to learn about the provider's policies and procedures for encryption and encryption key management. The cloud encryption capabilities of the service provider need to match the level of sensitivity of the data being hosted.

Because encryption consumes more processor overhead, many cloud providers will only offer basic encryption on a few database fields, such as passwords and account numbers. At this point in time, having the provider encrypt a customer's entire database can become so expensive that it may
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

In many ways, cloud services governance can be viewed as an extension of SOA governance, although the unique properties of a public cloud architecture -- such as multi-tenancy -- present different slightly different concerns. Ideally, cloud services governance complements or is integrated
In this e-guide

- Introduction
- Uncover Common Cloud Threats
- Form a Cloud Security Strategy
- Assess Cloud Security Tools
- Test Your Cloud for Weakness
- Cloud Security in the News
- Cloud Security Terminology

E-guide

Compliance

Margaret Rouse, WhatIs.com

Compliance is either a state of being in accordance with established guidelines or specifications, or the process of becoming so. Software, for example, may be developed in compliance with specifications created by a standards body, and then deployed by user organizations in compliance with a vendor’s licensing agreement. The definition of compliance can also encompass efforts to ensure that organizations are abiding by both industry regulations and government legislation.

Compliance is a prevalent business concern, partly because of an ever-increasing number of regulations that require companies to be vigilant about maintaining a full understanding of their regulatory compliance requirements. Some prominent regulations, standards and legislation with which organizations may need to be in compliance include:

- **Sarbanes-Oxley Act (SOX) of 2002**: SOX was enacted in response to the high-profile Enron and WorldCom financial scandals to protect
shareholders and the general public from accounting errors and fraudulent practices in the enterprise. Among other provisions, the law sets rules on storing and retaining business records in IT systems.

- **Can Spam Act of 2003**: The Can Spam Act requires businesses to label commercial emails as advertising, use legitimate return email addresses, provide recipients with opt-out options and process opt-out requests with 10 business days.
- **Health Insurance Portability and Accountability Act of 1996 (HIPAA)**: HIPAA Title II includes an administrative simplification section that mandates standardization of electronic health records systems and includes security mechanisms designed to protect data privacy and patient confidentiality.
- **Dodd-Frank Act**: Enacted in 2010, this act aims to reduce federal dependence on banks by subjecting them to regulations that enforce transparency and accountability in order to protect customers.
- **Payment Card Industry Data Security Standard (PCI DSS)**: PCI DSS is a set of policies and procedures created in 2004 by Visa, MasterCard, Discover and American Express to ensure the security of credit, debit and cash card transactions.
- **Federal Information Security Management Act (FISMA)**: Signed into law in 2002, FISMA requires federal agencies to conduct annual reviews of information security programs, in order to keep risks to data at or below specified acceptable levels.

IT compliance guidelines vary by country; SOX, for example, is a U.S. legislation. Similar legislation in other countries includes Germany's Deutscher Corporate Governance Kodex and Australia's Corporate Law Economic Reform Program Act 2004. As a result, multinational
organizations must be cognizant of the regulatory compliance requirements of each country they operate within. As regulations and other guidelines have increasingly become a concern of corporate management, companies are turning more frequently to specialized compliance software and IT compliance consultancies. Many organizations have even added compliance jobs such as a chief compliance officer (CCO).

The main responsibilities of a chief compliance officer include ensuring that an organization is able to both manage compliance risk and pass a compliance audit. The exact nature of a compliance audit will vary depending upon factors such as the organization's industry, whether it is a public or private company, and the nature of the data it creates, collects and stores.

Regular regulatory compliance training programs for both IT staff members and business users can protect the organization as a whole. Compliance training program guidelines will also vary depending on the industry a company is in and the data it generates and uses.
Identity access management (IAM) system

Margaret Rouse, WhatIs.com

An identity management access (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management.

An identity access management (IAM) system is a framework for business processes that facilitates the management of electronic identities. The framework includes the technology needed to support identity management.

IAM technology can be used to initiate, capture, record and manage user identities and their related access permissions in an automated fashion. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.

Poorly controlled IAM processes may lead to regulatory non-compliance because if the organization is audited, management will not be able to prove that company data is not at risk for being misused.
Why you need IAM

It can be difficult to get funding for IAM projects because they don't directly increase either profitability or functionality. However, a lack of effective identity and access management poses significant risks not only to compliance but also an organization's overall security. These mismanagement issues increase the risk of greater damages from both external and inside threats.

Keeping the required flow of business data going while simultaneously managing its access has always required administrative attention. The business IT environment is ever evolving and the difficulties have only become greater with recent disruptive trends like bring-your-own-device (BYOD), cloud computing, mobile apps and an increasingly mobile workforce. There are more devices and services to be managed than ever before, with diverse requirements for associated access privileges.

With so much more to keep track of as employees migrate through different roles in an organization, it becomes more difficult to manage identity and access. A common problem is that privileges are granted as needed when employee duties change but the access level escalation is not revoked when it is no longer required.

This situation and request like having access like another employee rather than specific access needs leads to an accumulation of privileges known as privilege creep. Privilege creep creates security risk in two different ways. An employee with privileges beyond what is warranted may access
applications and data in an unauthorized and potentially unsafe manner. Furthermore, if an intruder gains access to the account of a user with excessive privileges, he may automatically be able to do more harm. Data loss or theft can result from either scenario.

Typically, this accumulation of privilege is of little real use to the employee or the organization. At best, it might be a convenience in situations when the employee is asked to do unexpected tasks. On the other hand, it might make things much easier for an attacker who manages to compromise an over-privileged employee identity. Poor identity access management also often leads to individuals retaining privileges after they are no longer employees.

What should an IAM system include?

IAM solutions should automate the initiation, capturing, recording and management of user identities and their related access permissions. The products should include a centralized directory service that scales as a company grows. This central directory prevents credentials from ending up recorded haphazardly in files and sticky notes as employees try to deal with the burden of multiple passwords for different systems.

IAM systems should facilitate the process of user provisioning and account setup. The product should decrease the time required with a controlled workflow that reduces errors and the potential for abuse, while enabling automated account fulfillment. An identity and access management system should also provide administrators with the ability to instantly view and change access rights.
In this e-guide

Introduction

Uncover Common Cloud Threats

Form a Cloud Security Strategy

Assess Cloud Security Tools

Test Your Cloud for Weakness

Cloud Security in the News

Cloud Security Terminology

An access right / privilege system within the central directory should automatically match employee job title, location and business unit ID to manage access requests automatically. These bits of information help classify access requests relevant to employees existing positions. Depending on the employee, some rights might be inherent in their position and automatically provisioned, while others may be allowed upon request. In some cases, reviews may be required. Other requests may be denied except in the case of exemption or may be outright prohibited. All variations should be handled automatically and appropriately by the IAM system.

An IAM should set workflows for managing access requests, with the option of multiple stages of reviews with approval requirements for each request. This mechanism can facilitate setting different risk level-appropriate review processes for higher-level access as well as reviews of existing rights to prevent privilege creep.

IAM products

One Identity Manager from Dell combines easy installation, configuration and use. The system is compatible with Microsoft SQL and Oracle database systems. According to Dell, the self-service product is so user-friendly that employees can manage all stages in the IAM life cycle without requiring help from the IT department. The product suite also includes Cloud Access Manager, which enables single sign-on capabilities for a variety of Web application access scenarios.
F5 Networks' BIG-IP Access Policy Manager has highly-reviewed service and support. The software is part of the BIG-IP multilayer switch system, which is available in appliance and virtualized systems. The Policy Manager allows HTTPS access through all major web browsers, saving workstation configuration time.

Tools4ever's Self-Service Reset Password Management is ranked highly for ease of installation, configuration, management and service. The tool allows admins to create their own “forgot password” link for users and specify numbers of security questions. This self-service password tool has been demonstrated to reduce the need for password reset calls by as much as 90 percent.

IBM's Security Identity Manager is designed to be quick and simple to deploy and to be compatible with other products. The software supports Microsoft Windows Server, SUSE Linux Enterprise Server, Red Hat Enterprise Linux and IBM's own AIX, as well as most common operating systems, email systems, ERP systems and cloud applications such as Salesforce.com. The included toolkit simplifies the integration of custom applications. Creation and modification of user privileges are automated through a rules-based system and access rights can be automatically added or removed for individual users based on changes in business roles. Permissions can also be applied for groups.
Pen test (penetration testing)

Margaret Rouse, WhatIs.com

Penetration testing (also called pen testing) is the practice of testing a computer system, network or Web application to find vulnerabilities that an attacker could exploit.

Pen tests can be automated with software applications or they can be performed manually. Either way, the process includes gathering information about the target before the test (reconnaissance), identifying possible entry points, attempting to break in (either virtually or for real) and reporting back the findings.

The main objective of penetration testing is to determine security weaknesses. A pen test can also be used to test an organization’s security policy compliance, its employees’ security awareness and the organization’s ability to identify and respond to security incidents.

Penetration tests are sometimes called white hat attacks because in a pen test, the good guys are attempting to break in.

Pen test strategies include:

**Targeted testing**
Targeted testing is performed by the organization's IT team and the penetration testing team working together. It's sometimes referred to as a
"lights-turned-on" approach because everyone can see the test being carried out.

**External testing**
This type of pen test targets a company's externally visible servers or devices including domain name servers (DNS), e-mail servers, Web servers or firewalls. The objective is to find out if an outside attacker can get in and how far they can get in once they've gained access.

**Internal testing**
This test mimics an inside attack behind the firewall by an authorized user with standard access privileges. This kind of test is useful for estimating how much damage a disgruntled employee could cause.

**Blind testing**
A blind test strategy simulates the actions and procedures of a real attacker by severely limiting the information given to the person or team that's performing the test beforehand. Typically, they may only be given the name of the company. Because this type of test can require a considerable amount of time for reconnaissance, it can be expensive.

**Double blind testing**
Double blind testing takes the blind test and carries it a step further. In this type of pen test, only one or two people within the organization might be aware a test is being conducted. Double-blind tests can be useful for testing an organization's security monitoring and incident identification as well as its response procedures.
Shadow IT

Margaret Rouse, WhatIs.com

Shadow IT is hardware or software within an enterprise that is not supported by the organization’s central IT department. Although the label itself is neutral, the term often carries a negative connotation because it implies that the IT department has not approved the technology or doesn’t even know that employees are using it.

In the past, shadow IT was often the result of an impatient employee’s desire for immediate access to hardware, software or a specific web service without going through the necessary steps to obtain the technology through corporate channels. With the consumerization of IT and cloud computing, however, the meaning has expanded to include personal technology that employees use at work (see BYOD policy) or niche technology that meets the unique needs of a particular business division and is supported by a third-party service provider or in-house group, instead of by corporate IT.

Shadow IT can introduce security risks when unsupported hardware and software are not subject to the same security measures that are applied to supported technologies. Furthermore, technologies that operate without the IT departments’ knowledge can negatively affect the user experience of...
other employees by impacting bandwidth and creating situations in which network or software application protocols conflict. Shadow IT can also become a compliance concern when, for example, an employee stores corporate data in their personal DropBox account.

Feelings toward shadow IT are mixed; some IT administrators fear that if shadow IT is allowed, end users will create data silos and prevent information from flowing freely throughout the organization. Other administrators believe that in a fast-changing business world, the IT department must embrace shadow IT for the innovation it supplies and create policies for overseeing and monitoring its acceptable use.

Popular shadow technologies include personal smartphones, tablets and USB thumb drives. Popular shadow apps include Google Docs, instant messaging services and Skype.