InfoWorld DeepDive

Cloud Security

A NEW SECURITY MODEL FOR THE CLOUD ERA

SPONSORED BY

INTRALINKS®

Deep Dive

Staying secure in the cloud

Cloud computing depends on sharing resources that were never shared before, demanding a new set of security best practices

BY ROGER GRIMES

The good news about cloud computing is you're probably saving a lot of money on IT overhead and getting more out of the services you're paying for. The bad news is you're giving up a lot of control. This lack of control presents the biggest challenges.

Cloud computing is here to stay. But it brings with it all of the traditional computer security threats as well as a host of new ones. The cloud is making security experts' jobs harder than ever before, forcing them to step up with innovative responses. This Deep Dive will detail the unique security challenges cloud computing presents and the best practices you should implement to meet them.

Cloud computing basics

No matter what services your organization is deploying in the cloud – infrastructure, software, or platform – how you secure them depends a great deal on who's providing them. There are essentially three kinds of cloud services:

- **The public cloud.** As the name implies, public clouds are offered to the general public. They're accessible via an Internet connection and shared among multiple, often thousands, of customers. Some of the largest public cloud providers include Amazon Web Services, Microsoft Windows Azure, and Rackspace Cloud.
- **The private cloud.** Private clouds are typically created and hosted by a single organization, usually behind the corporate firewall, which provides services on request to employees. Private clouds can also be hosted by third parties, but they remain dedicated to a single customer. They can be more costly than public clouds but offer greater control over your data and better fault tolerance.
- **The hybrid cloud.** This term typically applies to organizations whose IT operations combine internal private cloud services with external public cloud services. It may also refer to service offerings used exclusively by an invited group of private customers (also called a "community cloud").

Because the public cloud offers both the least control and the least understood risks, this Deep Dive will focus primarily on securing the public cloud.

How public cloud computing is different for traditional IT

In a traditional IT scheme, all your applications and data are likely stored on servers and data you control and share with no one else.

You know where these machines and data are located. You know exactly how well they are secured, how often they're backed up, where those backups are located when you need them, and what processes will kick in if those machines fail or are compromised. If you're doing your job correctly you should have a good idea of who's accessing your network, what machines they are using to do it, and where these users are physically located. You probably use a centralized directory service to manage how employees and customers are authorized to access different parts of the network, which you can use to deprovision them at any time. Finally, when you're decommissioning servers or storage, you can make certain they are wiped clean of sensitive data before they're sent to the boneyard.

In the public cloud, many of those things are no longer true. Your IT operations are accessible via the Internet. The machines and data you're using could be located anywhere on the planet as part

Deep Dive

of a massively scalable user-configurable pool of computing resources. You are likely sharing many of those computing resources with hundreds if not thousands of users who are not in your organization. You may also be sharing a common authentication scheme with many of those other organizations. Disaster recovery and fault tolerance are the responsibility of the cloud provider, as is disposal of old machines containing your data.

The good news is you're probably saving a lot of money on IT overhead and getting more out of the services you're paying for. The bad news is you're giving up a lot of control. This lack of control presents the biggest challenges.

In a public cloud computing world, IT's job shifts from trying to implement adequate controls over your technology to assuring that the CSP (cloud service provider) is implementing adequate controls over its technology. If your CSP cannot assure you sufficient controls are being applied, it's your job to recommend to senior management that the organization take its business elsewhere. Senior management may not always be aware of the differences between traditional IT and the public cloud, so you'll need to be ready to make a strong case as to why or why not a particular CSP should be used.

Cloud security defense assumptions and best practices

Cloud security is an evolving field. To begin with, cloud solutions are subject to all the conventional attacks a traditional IT network must face: buffer overflows, password attacks, physical attacks, exploitation of application vulnerabilities, session contamination, network attacks, man-in-the-middle attacks, social engineering, and so on. But they also present new challenges and assumptions.

As a public cloud customer you may lack basic transparency into the security controls protecting a particular cloud service. That's why the best time to find out what security controls your CSP has in place – as well as the visibility and auditing rights you have into those controls – is before you commit.

Defending your data and applications in the cloud will also be a little different than you're used to. You'll need to start with the following assumptions.

- **Attackers are authenticated users.** Unlike on internal networks, attackers in the public cloud are likely to be logged-in, authenticated users – and, given the cloud's global reach, there may be many more of them. This means that many conventional defenses (separated security zones, firewalls, and so on) may have little effect. You'll need to rethink your strategy accordingly.

- **Say goodbye to the DMZ.** In the public cloud, there is no DMZ that separates your corporate network from the Internet. If the DMZ was porous (at best) in the past, it has now completely evaporated. You'll need to forget about establishing a "safe zone" and think about isolating your domains.

- **Say hello to a world of providers.** Although a particular cloud service is often completely created and provided by a single vendor, as cloud services mature they are likely to be represented by four main, possibly separate, symbiotic parties: consumers, network providers, identity/authentication providers, and cloud service providers.

In the past, each cloud provider had its own identity and authentication mechanism. This is quickly changing, with many cloud services relying on identity and authentication services provided by other vendors. For example, many cloud services allow you to log on with a Facebook identity (which relies on the OAuth authentication protocol standard).

More and more organizations are allowing users to access applications and data using cloud identities such as Gmail, iCloud, and Microsoft accounts. That mean if a zero-day vulnerability is discovered at one authentication provider, many different cloud service customers could instantly be put at risk.

Cloud security best practices

The traditional computer security models spread defenses over confidentiality, integrity, and availability. The Cloud Security Alliance spreads them over governance, risk management, and compliance. Both approaches are valid and

Deep Dive

should be used, but here we'll concentrate on practical and applied best practices.

Identity and authentication providers

If you thought identity management and authentication were confusing before, the cloud brings a new level of sophistication that makes the old models look easy.

You'll have a rash of things to consider, ranging from what types of identities (log-on names, biometric tokens, smartcards, etc.) are allowable, to what authentication mechanisms are required to access a cloud service. You'll need to know what processes the CSP uses for provisioning and deprovisioning users, and what level of assurance the CSP's authentication providers offer. The size of passwords or PINs, the frequency with which they're updated, how log-on credentials are stored and protected are all vital parts of the puzzle.

What processes are in place when an identity is compromised? If the authentication database is breached, will your CSP tell you? How long will it take them? These answers need to be obtained not only for you but also for your engineering, operations, security, and auditing teams.

Best practices demand that authentication requirements are documented and followed to the letter. Elevated system access should always require two-factor or better authentication. Identity and authentication providers should provide transparency on guaranteed security assurances and the security practices they follow. Passwords should be a minimum of 12 characters and be changed at least once a quarter. PINs should be at least five characters and only be used as part of two-factor authentication or with strict lock-out mechanisms. When the authentication system has been compromised, you should be notified within a reasonable amount of time.

The answers to all of these questions are among the most important any CSP can provide.

Best practices demand that authentication requirements are documented and followed to the letter.

Covering your assets

You can't manage what you don't know you have. In a traditional IT world, asset management is fairly straightforward. You track the hardware and software your organization maintains, as well as the details of different service offerings. Every item used to provide a particular service (infrastructure services, DNS, namespace, databases, routing, etc.) is part of that inventory. A comprehensive list of assets not only includes the servers and infrastructure involved, but also every client workstation that can or will connect to those servers and infrastructure devices.

Enterprises are often compromised because a single workstation has been compromised. So good asset management is essential to good security. With best practices, each inventoried asset item would be well managed through the various phases of its lifecycle: starting with procurement and following through ownership, configuration, deployment, operations, change management, deprovisioning, and finally replacement. If you don't have these items documented on each asset you manage, you aren't really managing them.

With the public cloud, asset management becomes much more problematic. It is now up to your CSP to handle all of that, and it is up to you to find out what assets have been deployed on your behalf and all the interconnections between them. Because your CSP may be unwilling or unable to share this information with you, you need to do your best to determine if the service provider has a serious asset management plan that is governed across the entire product lifecycle.

Let's get physical

Computer security is also physical security. Just as you wouldn't let some stranger wander into your corporate data center, you need to ensure your CSP has adequate physical security protecting its data centers, as well as sufficient power, redundancy, and environmental controls.

No one should be able to assess any critical assets at your CSP without multiple levels of authentication and authorization. Elevated access, remote or on-site, should require two-factor authentication. Remote access should be limited and possible through a minimum of connection points and programs.

The CSP should also document the physical requirements of each asset, with power and environmental controls that exceed the specs. The best organizations provide fault tolerance with separate power and environmental facilities, dual pathways, and SLAs with related providers.

Deep Dive

Availability

With a public cloud service, availability is everything. An outage at a critical moment could cost a large organization millions of dollars in lost transactions and damage its reputation. But availability also entails adequate resource planning, fault tolerance, hardware and software redundancy, disaster recovery plans, and business continuity procedures.

Your CSP should provide anti-DoS protections, which can include both asset hardening, fail-over resources, and external service protections. You'll want a SLA on all critical services, including guarantees on the time needed to do complete (or at least acceptable) service-level restoration.

What are the minimum downtimes during service updates? How long does it take to recover from a service update failure? What procedures are executed to ensure quality testing before an upgrade? The answers to these questions should be part of your documented business requirements and included in the SLA.

You should ask to see security audit reports that detail the efforts your CSP takes to avoid vulnerabilities.

Backup and restoration

Though technically part of a comprehensive availability plan, backup and restoration deserve special consideration. There are many stories of data forever lost because the cloud provider failed to perform adequate backups or restore data to a customer's satisfaction.

What data does your CSP back up and how frequently? How do you request a backup? Are the backup sets encrypted? How long are they kept and where are they stored? What techniques does the CSP use to restore data? How often does it test restorations, and how thoroughly does it test data integrity?

You'll want to spell all of that out in your business requirements and make them part of your SLA. In general, your CSP should test its restores at least once a year, if not more often, and document the results. When testing, it should examine each restoration for completeness and integrity. All backups should be encrypted (using industry-accepted crypto and key sizes) during the backup process, with the encryption key known by only the individuals needed. You'll want to ensure your backup sets are well managed and kept in a secure location.

Application security and vulnerability testing

Most websites are not compromised because of operating system or Web server software vulnerabilities. Security holes within applications easily account for the biggest percentage of successful exploits. Although all enterprises need to follow best practices in terms of vulnerability testing, you also need to make sure your CSP isn't exposed in a way that could compromise your data.

The Open Web Application Security Project (OWASP) Top Ten list is considered by many to be the most concise list of the top causes of website hacking. All cloud providers should know the list well and create controls to offset the risks.

Try to ensure your CSP designed its websites using security design lifecycle techniques and that the sites undergo internal and external vulnerability and penetration testing at least once a year. Ideally, your CSP's developers will have used strong and secure programming languages, checked for known weaknesses, and used vulnerability testing tools during all phases of any project. Even though you will likely have little control over this, you should ask to see security audit reports that detail the efforts your CSP takes to avoid vulnerabilities.

Patch management

After application vulnerabilities, the second biggest source of security breaches is unpatched software. You want to be sure your CSP regression tests critical security patches and applies them as quickly as possible – ideally within a week of the patch's availability, and even faster during an aggressive "in-the-wild" malware campaign.

Find out how your CSP performs patch management and verifies patch status. Ideally mission-critical servers will have patches applied first, followed by less-critical assets. Regression testing must be done aggressively to assure the least amount of downtime, and your CSP should scan all systems on a daily or weekly basis to check patch status. You also want to make sure that all involved assets identified by the asset management program are regularly patched – not just operating systems.

Data handling

Everything we do in computer security is really to protect the data, so it's no surprise that this area is

Deep Dive

particularly important when it comes to choosing the right CSP. Public cloud providers should have particularly strong requirements due to multitenancy.

You want to know how your service provider will protect your data. Is your data separated into different classes, and if so, is the security different for each? Does your CSP encrypt the data? How does it ensure data integrity and privacy?

You'll also need to know how data is separated and protected between the CSP's different tenants, how it prevents unauthorized leaks, and how long it takes the CSP to notify you if your data has been compromised.

Best practices dictate all data be classified, usually with three to four levels of sensitivity (high business impact, medium business impact, low business impact). Data classification should be a documented business requirement and the data marked, either electronically and/or physically, so all stakeholders are aware of how the data should be treated.

Likewise, your CSP should encrypt critical data using industry-accepted algorithms and key sizes. Data with a medium business impact should be encrypted when stored. Data with a high business impact should be encrypted when stored and transmitted. All data must be properly disposed of when it becomes inactive or your CSP is no longer authorized to have it.

Another fundamental question: Who owns the data? There have been several instances of public CSPs closing and the customer's data becoming inaccessible or – worse – sold to whoever acquires the service provider's assets. Make sure your SLA spells out that you own the data and that only you have the right to access it.

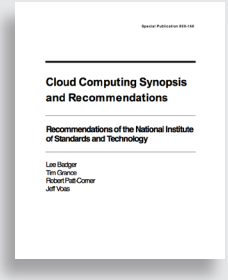
Encryption

You know you need to encrypt your data in the cloud. The question becomes what kind of encryption algorithms does your CSP use, and how are they applied? Is data encrypted at rest and in transit? Are all Web connections protected? What key sizes are used? How often are keys renewed and replaced? Who has access to what keys? Are keys shared between different tenants' data? These are all questions you need to settle before you hand your data to any CSP.

Best practices dictate service providers use industry-accepted algorithms and key sizes,

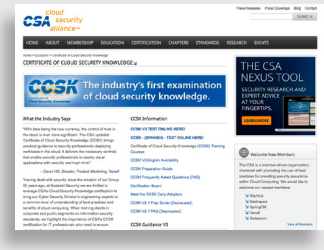
Additional resources: Secure Cloud Computing

Cloud computing is a new paradigm that requires new security defenses. The material included here covers only a small portion of the considerations you need to weigh when preparing a holistic cloud defense. The following Web assets are excellent sources of additional information:

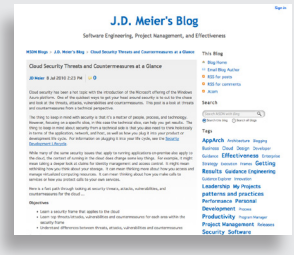


NIST's cloud section. A great PDF to quickly get up to speed on cloud terminology without reading a book.

Cloud Security Alliance. Site represents a good collection point for enterprise-level cloud-related security. Look under the New Research section.



Cloud Security Alliance IT Certification



Cloud Threats and Security Measures. MSDN, J. Meier

Deep Dive

though the latter may vary depending on the value of the data being protected, strength of the cipher, and the security of the key management system. In general, RSA-style asymmetric key sizes are generally believed to be strong if they are 2.048 bits long. Symmetric keys are considered strong if they are at least 256 bits long.

Industry-accepted algorithms can be found in several locations, including the National Institute of Standards and Technology. Readers unfamiliar with recommended key sizes should read the Wikipedia explanation. You can calculate industry-accepted key sizes here.

Networks need to meet or exceed documented SLAs, including performance, availability, and security. These requirements are the same whether considering public or private cloud projects.

Network security

How does your CSP secure its own network? What wireless security does it use and how are unmanaged computers detected, prevented, or used?

You'll want to know what devices and software are used and how often they are patched. In general, network devices should receive critical security patches within one week. Computers that don't meet the required security configurations should be prevented from connecting using network access controls.

Networks need to meet or exceed documented SLAs, including performance, availability, and security. These requirements are the same whether considering public or private cloud projects.

Domain isolation

Traditionally, most computing environments were split between internal, external, and DMZ. Unfortunately, cloud computing really doesn't fit into those convenient categories. The best you can do is make sure your CSP employs security domain isolation to ensure that only devices and users that need to connect to each other can do so.

Domain isolation can be enforced using any available method, including physical separation, router, firewall, proxies, switches, IPSec, application-level firewalls, etc.

All computer systems should be prevented from making successful connections (the lower in the network OSI model the better) to computers they do not have a business requirement to connect to. Obviously this is easier to implement when you control the computers, so with a public cloud provider you'll need to ask how domain isolation is done.

Anti-malware

Of course your CSP scans its systems for malware. But what software does it use? How often are scans performed and anti-malware definitions updated? Are the scans performed on demand or on a fixed schedule? How much do scans delay service transactions? In general, your CSP needs to scan every server and workstation, with new data inputs scanned in real time and full disk and memory scans performed at least once a week. They should use anti-malware software with a proven track record for accuracy and update their definitions at least daily, if not continuously. The scans should never affect performance enough to impact SLAs.

Event management and intrusion detection

You want to get an understanding of how mature your CSP's event log management and intrusion detection systems are. What systems does the cloud provider use to detect, record, and alert on security events? How many of the involved systems are covered? What events create alerts?

All systems involved in critical service deliveries should have event log management enable and configured to provide relevant security events. Security event messages should be collected, evaluated, and generate timely incidence responses when appropriate.

According to the Verizon Data Breach report, each year most security incidents were recorded in event logs, but did not incur timely incident responses because the affected companies were not doing appropriate management. Make sure your cloud provider is not one of those companies.

Incident response

Each cloud provider should have an appropriately trained incident response team that responds quickly to critical events. If a security event is noted, how long does it take the cloud provider's team to respond? How long does it take the CSP to notify you after a related data compromise is noted? You want to make sure the cloud provider has a dedicated and trained incident response team and that the procedures and guarantees are part of your SLA.

Deep Dive

Transitive trusts

Every external link, piece of infrastructure, or software component used to support a service establishes a "transitive trust" – and thus can become a potential hacking point or service disruption. The problems inherent in this were made clear by a recent Facebook error that disrupted service for thousands of sites simply because they had Facebook links on one of their pages. This is a huge, relatively new field of computer concern, one that clouds surely complicate.

Transitive trusts include not only Web links, but also any dependencies outside the main cloud service, including namespaces, programming languages, identity/authentication providers, third-party vendors, consultants, and other service providers. Hackers are becoming more sophisticated and will use the weakest link in your dependencies to attack you.

All developers (program, site, content, and distributors) should understand the concept of transitive trust. Every external link should be justified, and the transitive trust implications debated. Site developers should build in test and recovery plans for each external link.

Transitive trust issues are harder for public cloud customers to understand. It would be great if all customers communicated their transitive trust concerns to cloud providers and sought reassurances that the vendor is familiar with the issue. The use of a public cloud product is in itself a big transitive trust issue that a CSP's customers must consider.

The time when cloud computer providers were given a pass on security issues is coming to close.

Governance and compliance

Before you sign on the dotted line, you'll want to know what governing and regulatory rules the cloud provider falls under, and whether an independent third party has certified those compliance standards.

Besides the normal regulatory compliance standards, such as HIPAA, SOX, PCI-DSS, etc., there are some developing cloud standards. The most notable and mature standards have been published by the Cloud Security Alliance. Detailed controls and auditing questions can be downloaded here. No single document can be perfectly inclusive, but the security best practices listed are a good start to understanding and improving cloud security.

When dealing with a public cloud service it can be very difficult to get detailed, specific answers. Try your best. If you can't get specific answers, see if your cloud provider offers results or public attestation letters from regulatory or accreditation authorities. If you don't get enough answers, don't go with the service. In a very true sense, the trust you are extending to an external cloud vendor is the biggest transitive trust you have.

The time when cloud computer providers were given a pass on security issues is coming to close. Customers want assurance that basic security controls are in place, and the more a CSP can transparently show that assurance, the more you can trust it with your data. ■

Deep Dive

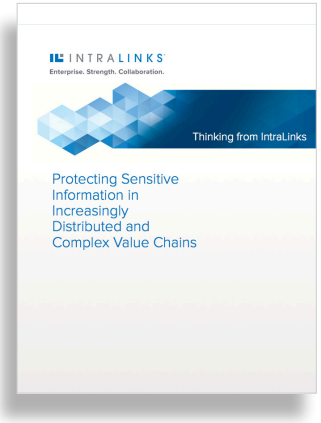
Cloud Security Resources

Report

Market Trends: Collaboration Suites Enhance Team Relationships Through Virtual Interactions

Collaboration software helps improve the connectedness of workers to capture and diffuse formal and informal knowledge. View this Gartner report on the disruptive forces and growth opportunities impacting the secure collaboration and file sharing market.

Read

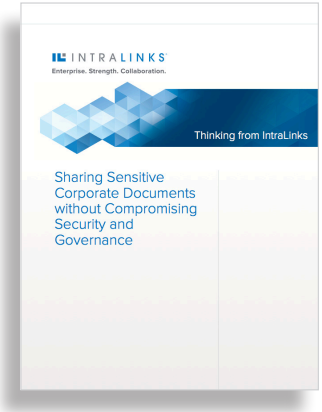


White Paper

Protecting Sensitive Information in Increasingly Distributed and Complex Value Chains

Businesses need to collaborate more closely with third parties with more agility than ever before. Yet, in the rush to collaboration, the secure sharing of information can be neglected. This white paper explores strategies and tactics – ranging from culture-based methods to new and emerging technologies – to securely enable the information sharing that leads to collaborative success among value chain members.

Download



White Paper

Sharing Sensitive Corporate Documents Without Compromising Security and Governance

SaaS-based (Software as a Service) collaboration and information sharing repositories are paramount for secure file/document sharing, yet, not all GCs are truly aware of the benefits they can bring to an organization. In this white paper, discover the value these solutions create in terms of security and compliance with a focus on how they dramatically enhance the legal department's oversight, while simplifying e-discovery and making the e-discovery process more efficient than in other models.

Download