Staying Secure in the Cloud Is a Shared Responsibility

Published: 7 April 2016

Analyst(s): Steve Riley

While public cloud providers typically have strong control attestations, numerous compliance certifications and their own security features, CSPs cannot offer complete security. CISOs and security leaders must understand the scope of their responsibilities for security in the cloud.

Key Challenges

- Provider-supplied security differs between IaaS, PaaS and SaaS. Regardless of the model, identity and access management (IAM) and data security are always customer responsibilities.
- The cloud reduces the scope of required traditional security work, but doesn’t eliminate it. Moving workloads to the cloud doesn’t automatically make them "more secure."
- Cloud service provider (CSP) isolation keeps tenants separated, but customers are responsible for any additional required logical network or storage separation within their deployments.
- Workloads that require compliance must still go through audits and certification at the application level.

Recommendations

- Incorporate appropriate IAM from the outset, ideally based on roles, especially for administration duties. Customers, not the CSP, are responsible for defining who can do what within their subscriptions.
- Isolate data at rest with application-level encryption.
- Use TLS or VPN protected access. For IaaS, segment and contain network traffic using the CSP’s virtual network and filtering controls as a minimum.
- Establish a security control plane using third-party tools to achieve better visibility, data security, threat protection and compliance, as well as to automate security configurations.
- Take full responsibility for instance, application and data security.
- Back up all data in a fault domain distinct from where it resides in production.
 Lemage the benefit of being "compliant by inclusion" by incorporating the CSP’s published attestations into your own.

Table of Contents

Strategic Planning Assumption ................................................................. 2
Introduction .............................................................................................. 2
Analysis ...................................................................................................... 4
   Incorporate Appropriate Identity and Access Management ........... 4
   Isolate Data at Rest With Encryption ............................................. 4
   Segment and Contain Traffic With Virtual Network and Filtering Controls .......................................... 6
   Establish a Security Control Plane for Better Visibility and Automation ................................................. 7
   Take Full Responsibility for Application and Instance Security ............................................................... 8
   Back Up All Data in a Distinct Fault Domain ................................... 9
   Investigate the Potential of Being "Compliant by Inclusion" ........... 9
Gartner Recommended Reading ................................................................. 10

List of Figures

Figure 1. Security Handoff Points for IaaS, PaaS and SaaS ..................... 3

Strategic Planning Assumption

By 2018, the 60% of enterprises that implement appropriate cloud visibility and control tools will experience one-third fewer security failures.

Introduction

This document was revised on 21 April 2016. The document you are viewing is the corrected version. For more information, see the Corrections page on gartner.com.

The increasing popularity of public clouds requires CISOs to develop effective security strategies and tactics to ensure appropriate levels of security for enterprise operations within the public cloud. The popular brand-name public clouds have demonstrated success at keeping their services resilient and available, showing no signs of buckling under attack. Indeed, the question of whether clouds are secure has an answer: yes (see “Clouds Are Secure: Are You Using Them Securely?”).

The popularity and demonstrated security competence of CSPs do not absolve CISOs of their responsibility to actively manage cloud security. Security in the cloud is a shared responsibility.
Where is the balance point between the CSP and the CISO regarding security management? This research provides clear guidelines for defining and allocating responsibility for security planning and operations in IaaS, PaaS and SaaS environments. CISOs should use this research to develop effective security strategies for existing and planned utilization of public clouds.

Figure 1 illustrates the security handoff points for infrastructure as a service (IaaS), platform as a service (PaaS) and software as a service (SaaS) cloud models. The handoff point moves up the stack across the models. IaaS offers the most control, with the commensurate security responsibility left to customers. SaaS offers the least control, with the CSP taking on most of the security responsibility. "People" in the diagram refers to customer-authorized users of applications and data, not to cloud provider employees.

Figure 1. Security Handoff Points for IaaS, PaaS and SaaS
Analysis

Incorporate Appropriate Identity and Access Management

**Applies to:** IaaS, PaaS, SaaS

A sound IAM strategy is fundamental for any cloud deployment. Customers, not the CSP itself, are responsible for defining who can do what within their cloud subscriptions. All cloud subscriptions have the equivalent of a customer-level "root" or "administrator" account that requires rigorous management. Sharing this credential among all cloud administrators and developers is an invitation for disaster. Sharing violates compliance schemes, makes true auditing impossible, and creates a very attractive and powerful target for an attacker.

Use the CSP’s IAM capabilities to create individual credentials for each user in your account or subscription. Create roles for specific functions and assign them to users, groups and applications. Where appropriate, add extra conditions that further restrict access. Here are some example roles:

- **Manage-security-groups**: Allowed to create/modify/delete security groups and rules; assigned to security administrator user IDs
- **Manage-dev-instances**: Allowed to start/stop/terminate instances in development; assigned to all developer user IDs
- **Manage-prod-instances**: Allowed to start/stop/terminate instances in production; assigned to cloud resource operator IDs (useful for organizations that maintain separate developer and operations staff)
- **Manage-users**: Allowed to add/remove users; assigned to account administrator IDs; requires logging in with multifactor authentication (MFA)

Privileged user accounts deserve special attention. At a minimum, require multifactor authentication. But because multiple factors don’t necessarily translate into guaranteed higher trust, investigate third-party privileged access management tools for better protection of these accounts.

Isolate Data at Rest With Encryption

**Applies to:** IaaS, PaaS, SaaS

No evidence suggests that CSP employees wantonly access customer data or that disk drives escape from data centers. The brand-name CSPs claim to take many steps to prevent these issues, both technical and procedural. Indeed, CSPs have a vested interest in maintaining strong isolation between routine maintenance procedures and customer data and between the customers themselves. Nevertheless, encryption is a useful tool for creating logical isolation from other tenants, for enforcing classification policies, and for ensuring digital shredding at end of life.

The most important aspect of encryption is good key management, including customer control of the keys. Attributes of a good key management system include:
Access control and auditing — for humans and services, with assurances that keys are not generally available to the CSP

Scale — over time, thousands of keys may be used

Availability — the system must always generate and release keys as necessary

Redundancy — the system must not be a single point of failure

Rotation — periodically changing keys reduces risk of compromise; automating this reduces management overhead

A common approach is to deploy a traditional key management system on-premises or on a network share in the cloud. Applications running in a cloud would make calls into the system to retrieve keys over a secure channel such as TLS or IPsec. However, on-premises key management systems might not operate at cloud scale or satisfy cloud-capable rotation requirements.

Brand-name clouds at IaaS, PaaS and SaaS levels now offer native encryption capabilities. These are designed to have zero or near-zero knowledge by the CSP of customer-controlled encryption keys. Native encryption automates key management tasks: it scales along with workloads, it rotates keys at periodic intervals, and it provides for key backup. Because keys aren’t stored in memory or disk but regenerated as necessary, no single points of failure exist. Higher-level services such as databases and message queues are integrated with native encryption. Hardware storage modules (HSMs) are an option for even stronger key protection. The CSP’s IAM capabilities control access to keys and all key usage can be logged.

Gartner has no reason to doubt the claims stated by the CSPs regarding the security of their native encryption capabilities. While a good encryption design doesn’t permit routine CSP access to the keys, they do persist in RAM; it’s impossible to completely shield the keys from the CSP. Applications must have programmatic access to keys so that the applications can process data in clear text. Some use cases involving sensitive or regulated data might thus become noncompliant or out of scope.

Given the above, we recognize that some clients view this as an unacceptable risk and prefer to maintain complete separation between keys and CSPs. We encourage such clients — who we expect to be in the minority — to use a third-party encryption gateway or cloud access security broker (CASB) to encrypt or tokenize data before sending it to the CSP.

For SaaS, some providers encrypt data at rest using features available in the underlying operating systems. While this protects against the very unlikely scenario of physical theft, keep in mind that at the application level, data is processed and delivered in clear text. Some regulatory requirements or the data sovereignty laws of some jurisdictions might not allow this. To encrypt data at the application level, use the provider’s native encryption service (if available) or a third-party encryption tool designed to support SaaS applications. (Depending on the number of SaaS applications in use, multiple encryption tools might be necessary.)

Encryption can also help with compliance efforts. For example, consider a health records application. HIPAA provides guidelines for the appropriate use of encryption for data at rest. A
CSP’s native encryption services could isolate protected health information (PHI) from other data being processed by the application. To pass an audit, logging features must be enabled to track whenever encryption keys are generated, used and destroyed, including any access by the CSP.

Segment and Contain Traffic With Virtual Network and Filtering Controls

 Applies to: IaaS

Nomenclature: This section uses Amazon Web Services and Microsoft Azure as models. Where features or capabilities have different names, the following format is used: { AWS name | Azure name }.

In the early days of IaaS clouds, network-level controls didn’t exist. An instance-level logical construct known as a security group acts as a basic stateful firewall. It defines permitted inbound and outbound traffic for instances. Any traffic that fails to match a rule in the group is blocked. Security groups may contain other security groups, which enables a rudimentary form of segregation. For example, instances in the Web tier permit inbound traffic from the Internet, while instances in the database tier permit inbound traffic only from instances in the Web tier.

Over time, IaaS CSPs have added network-level controls. { Virtual private clouds | virtual networks } act as separate networks logically isolated from the rest of the CSP’s infrastructure. Subnets within a VPC further constrain instances by declaring whether the instances have Internet access, VPN access or no external access at all. Finally, { network ACLs | network security groups } define permitted and blocked inbound and outbound traffic for all instances contained within a subnet.

These controls make it possible to implement a well-defined multi-tiered architecture with appropriate network segmentation and without the use of additional virtual firewall instances, especially for east-west segmentation or internally facing instances or lower-trust applications. However, these controls lack other capabilities normally included in traditional firewalls — most notably logging and IDS/IPS, advanced reporting, integration with existing firewall management consoles, and third-party evaluation. If this presents a problem, some options to address this include:

- Host-based firewalls that log to a separate log receiver instance (ideally isolated in a separate subnet)
- Instances running firewall software, with routing configured correctly to pass all traffic through them; this can become challenging to manage at scale
- A packet-logging facility at the virtual network level (not all CSPs offer this capability) configured to dump logs into an SIEM
- Cloud-native network security controls for IDS/IPS, sandboxing, and other payload inspection
- Cloud-native visibility and control tools described in the next section

Segmentation can also help with compliance efforts (see the Compliant by Inclusion section below). For example, consider an e-commerce application. PCI DSS requirements dictate specific security controls for handling credit card information. The cardholder portions of the application could be
placed into a separate virtual network with stricter controls. To pass an audit, this virtual network could contain additional technologies and be governed by specific procedures applicable to PCI DSS.

Establish a Security Control Plane for Better Visibility and Automation

**Applies to:** IaaS, PaaS, SaaS

"When I move to the cloud, I lose visibility and control" — so goes the conventional wisdom, at least. The reality is better. Every resource provisioning event in IaaS or PaaS is performed via a console or an API call. The console and API calls can obtain an inventory of all provisioned resources at any time. Provisioning activity can be logged. Cloud visibility is different from on-premises visibility, and likely requires different tools. However, it’s a mistake to assume that moving to the cloud decreases visibility.

Similarly, moving to the cloud doesn’t eliminate all control. It’s true that CSPs control the physical infrastructure — servers, storage and networking. Customers still retain control of the more important parts of the IT stack: connectivity, segmentation, applications, data and users. What can be daunting at times is the skills shift required. Built-in security controls offered by CSPs are oriented toward developers — the same individuals who write code now need to understand how to manage compute instances, storage volumes and network segmentation. Most organizations don’t want to operate in this fashion.

When IT was entirely on-premises, organizations operated with clear delineations between network operations, software development and information security. People developed skills related to their roles and knew when to enlist the aid of others. In cloud deployments, particularly IaaS, the distinctions are blurred. Who becomes responsible for security decisions, such as configuring security groups, managing encryption keys, or keeping compute instances patched? When the answer is unclear, IT security teams may feel less influential.

For IaaS and PaaS, third-party tools can relieve developers of these additional burdens and restore a sense of purpose to IT security teams. For SaaS, a third-party CASB functions in much the same way. These purpose-built tools, designed specifically to augment CSP-provided visibility and control capabilities, create a security control plane that consolidates numerous tasks into a single panel and provide dashboards that show overall security posture. Using policies, security administrators can:

- Automate security settings so that security controls scale as virtual compute and network capacity expands or shrinks
- Define permitted and blocked traffic flows and track communications patterns
- Create application allow lists that place limits on the software that instances can run
- Compartmentalize workloads based on roles, geographic locations, business criticality, regulatory requirements and other factors
- Generate, store, release, rotate and destroy encryption keys as required by applications; log the use of keys
- Provision additional third-party security products (usually on separate instances), and automatically configure traffic routing through them.
- Ensure instance template images remain up to date with patches and application-appropriate hardening.
- Scan current instance configuration and patch state then compare to desired baselines and automatically remediate if necessary.
- Verify compliance and report deviations as they occur, including a list of actions required to develop a remediation plan.
- Monitor the integrity of files and instances; raise alerts during suspicious activity.
- Visualize overall behavior of cloud deployments, and investigate specific workloads or users in greater detail.
- Integrate, via APIs, with security incident and event management (SIEM) tools.

**Example vendors and products:**

- **SaaS:** Bitglass, CloudLock, CipherCloud, Elastica, Microsoft Cloud App Security, Netskope, Skyhigh Networks, Vaultive.

**Take Full Responsibility for Application and Instance Security**

**Applies to:** IaaS, PaaS

IaaS and PaaS CSPs take no responsibility for the security of application code that customers develop and run in clouds. A Web application with a SQL injection vulnerability is as much at risk running in a CSP as it is in a traditional data center. Use static and dynamic testing tools to identify and remove application vulnerabilities. For cloud-based workloads, consider using cloud-based testing tools.

IaaS CSPs also take no responsibility for the security of guest operating systems. Unpatched vulnerabilities in guest operating systems will be discovered and exploited. As explained in the previous section, third-party tools can help with scanning instances for vulnerabilities. Use tools that integrate with CSP APIs to automate scanning and remediation procedures. Increasingly, CSPs are adding built-in capabilities to help customers detect and fix security issues without the requirement of using third-party tools.

Additionally, develop the habit of creating hardened instance image templates and storing them in a library. System hardening is a very effective process that can significantly reduce overall attack surface whenever instances are started. Apply patches to the templates to ensure that new...
instances are always as up-to-date as possible and start replacement instances from the updated templates.

Back Up All Data in a Distinct Fault Domain

**Applies to:** IaaS, PaaS, SaaS

To increase storage durability, many CSPs create multiple copies of data objects and periodically validate their checksums. This helps maintain the integrity of objects and negates worries about bit rot or other corruption. However, it isn’t a substitute for proper backups.

While it’s true that brand-name CSPs rarely experience widespread security problems, localized outages involving data loss do happen. For IaaS and PaaS workloads, designing redundancy into your architecture can mitigate data loss problems to a certain degree. A typical CSP data loss incident occurs within a single geographic region. Replicating data in separate geographic regions will protect against such loss. Customers, not CSPs, are responsible for determining appropriate replication strategies. In general, for IaaS and PaaS, maintaining backups is a customer responsibility. IaaS and PaaS CSPs generally don’t provide backup features as built-in capabilities. Some might offer backup as an extra cost option, but configuration is entirely a customer responsibility.

SaaS providers vary in their support for geographic dispersion and duplication of data. Some offer backup capabilities, but more for business continuity or accidental deletion than for long-term retention. As with IaaS and PaaS, data backup for SaaS is a customer responsibility, but the procedures can be more complicated. To spread risk most effectively, back up data in SaaS applications to a separate CSP, such as the general object storage capability of an IaaS CSP.

Investigate the Potential of Being "Compliant by Inclusion"

**Applies to:** IaaS, PaaS

Many of the larger brand-name clouds routinely undergo various compliance audits including SOC 1/2/3, ISO 27001, PCI, FedRAMP and NIST 800. These serve as signals to customers, indicating the seriousness with which CSPs regard security. They are time-consuming and expensive to achieve; the majority of smaller SaaS providers likely won’t have an appetite or budget for continuous third-party auditing.

A provider’s compliance doesn’t automatically extend to applications running on that provider’s infrastructure. A SaaS application built on an IaaS cloud can’t rightfully claim to simply inherit that CSP’s set of compliance certifications. The vendor of the SaaS application must undergo an audit and receive its own certification. The scope of work for certification covers only the portions of the workload above the CSP’s handoff point.

Similarly, any CSP customer wishing to certify applications running in a cloud would need to focus audit efforts on the portions within the customer’s responsibility. The findings of that audit could be combined with the published findings of the CSP’s audit to demonstrate full compliance of the entire application stack.
**PCI DSS:** PCI compliance and PCI certification are distinct states. An independent qualified security assessor (QSA) validates a CSP’s services as PCI DSS compliant. Enterprises can then use the services to develop and deploy workloads that process credit card transactions; these workloads can achieve PCI certification from a separate QSA who evaluates both the CSP’s attestation and the customer’s custom software and workload configurations. The certification process will focus on the requirements for which customers are responsible, such as encrypting data at rest.

**HIPAA:** No program exists to issue HIPAA certifications for CSPs. HIPAA certification applies to the applications, data, and security and privacy policies created by CSP customers. However, under HIPAA regulations, CSPs are classified as business associates. To achieve HIPAA certification, customers will need to execute business associate agreements. Some CSPs require signing a separate business associate agreement (BAA); others incorporate BAA terms into their general terms of service. Most CSPs won’t sign BAAs.

**CJIS:** Unlike other compliance frameworks, CJIS has no accredited assessors and no standardized assessment procedure. Thus, uniform "CJIS compliance" isn’t possible. Instead, each law enforcement agency must enter into its own authorization agreement with a CSP. Some states have entered into statewide agreements with certain CSPs that would cover agency use of clouds. CJIS agreements typically rely on some other compliance audit, like FedRAMP or ISO 27001, to demonstrate CSP compliance with applicable CJIS requirements.

**ITAR:** No formal ITAR certification exists. Maintaining ITAR compliance is a customer responsibility. To ensure that compliance is possible, customers must verify that the CSP can provide services that meet ITAR requirements for handling information covered by the United States Munitions List. CSPs can engage independent QSAs to evaluate security controls under another framework, usually FedRAMP, and determine whether the CSP can properly support workloads that must be ITAR compliant.

---

**Gartner Recommended Reading**

Some documents may not be available as part of your current Gartner subscription.

"Best Practices for Securing Workloads in Amazon Web Services"

"Simplify Operations and Compliance in the Cloud by Protecting Sensitive Data"

"Develop an Encryption Key Management Strategy or Lose the Data"

"Develop Encryption Strategies for the Server, Data Center and Cloud"

"Simplify Operations and Compliance in the Cloud by Protecting Sensitive Data"

"Market Guide for Cloud Workload Protection Platforms"


"Market Guide for Privileged Access Management"
"Magic Quadrant for Application Security Testing"

"Data Backup/Recovery Factors to Consider When Adopting SaaS"

"You May Need Additional Backup to Prevent Data Loss From Your SaaS Solutions"

"Regulatory Compliance Alone Cannot Mitigate Cloud Vendor Risks"

Evidence

1 For example, the Customer Lockbox feature of Office 365 requires not only multiple levels of approval for Microsoft engineers to access customer data but also adds a customer approval step to the request.

2 See Download CIS Benchmarks Free of Charge for some excellent examples.
GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp