How cloud service providers can use data security to win customers
Table of Contents

4 Executive overview

4 Data security is becoming a requirement in the cloud

5 High-value customers view security as a business issue

6 Moving data off-site pushes the security discussion up the chain of command

7 CSPs that meet cloud customers’ needs will transition security concerns to new business

9 Capabilities that meet both customer and CSP needs
   – Capabilities important to cloud customers
   – Capabilities important to CSPs

12 Conclusion

12 About the author
How cloud service providers can use data security to win customers

Executive overview
Typically, the terms "security" and "ROI" do not appear in the same sentence. Increasingly, however, they are becoming imperatives in the business plans of Cloud Service Providers (CSPs) as data security has become a significant way that CSPs can win new customers. CSPs who take security and standards seriously by employing broad-based data security technologies win the customers who are currently reluctant to move to the cloud because of their security concerns. This paper is written for the benefit of CSPs and describes how data security can be an inherent part of their operations and can help them expand their customer base.

Data security is becoming a requirement in the cloud
Security products have never been a discretionary purchase. There must be a compelling reason to buy, install, and manage them or they will not be adopted. That is still true today; however, the number of scenarios where data security controls are essential has grown significantly as virtualization and cloud infrastructure have taken hold. Surveys repeatedly show that security-unsavvy CIOs and IT professionals cite data security as a primary inhibitor to cloud adoption.1

Security software and appliances have traditionally been viewed as overhead—something added reluctantly to the data center. Even when security mechanisms result in little or no performance overhead, they are typically considered an added IT management burden. Even so, security is becoming a hard requirement before customers will transition to the public cloud.

What might have been acceptable security in a customer’s private data center in the past is changing. The increasing frequency of data breaches reported in the press has caught the attention of the corporate CISOs and others, and the bar has been raised. Customers are beginning to require security assurances before they will award cloud services contracts.2 In time, security will move from being a deterrent to cloud adoption to a primary reason customers move to the cloud. Nowhere is this more important than in large customers adopting hybrid cloud deployments. The CSPs network is like an extension of their corporate network and strong security and shared responsibility are fundamentals that enterprise customers expect. Those forward-looking CSPs that embrace data security as a competitive differentiator will be the ones that land these coveted enterprise-scale customers.

1 Wisegate IT, A CIO’s Cloud Decision, http://www.wisegateit.com, 2012, pg. 4., 73% of IT managers cite security as their number one concern around moving to cloud-based services.

The data security solution discussed in this paper protects data in the cloud by automatically encrypting the data and the Virtual Machine (VM) elements that handle that data. This solution applies to the case when customers are running their own VMs in an IaaS public cloud as well as when a SaaS provider runs independent VMs (or creates independent virtual disks) for each customer using their service. In both cases, CSPs are scaling their infrastructure by creating multiple instances of VMs, one or more VMs per customer. These use cases require the CSP to implement a secure multi-tenant environment and be able to assure customers that their data is encrypted separately as it is stored, run, and backed up in the cloud.

This solution uses an administrative model that allows customers and CSPs to make simple policy choices about VM security and then go about their normal tasks. Encryption, key management, audit records, and other elements of the solution function transparently and do not require either the customer, or the CSP, to change their applications or alter the way they use or manage their operations.

Customers naturally become security-sensitive when their high-value data leaves their private data center—they want to ensure that they maintain control of their data and that it remains private. CSPs now know that data privacy is the number one concern for customers that wish to move mission-critical and tier-one workloads to the cloud.3

High-value customers view security as a business issue
Enterprise customers, especially those with a Chief Security Officer or VP/security-level personnel, view IT security in terms of risk versus benefit. These customers recognize the business benefits of cloud services, but they also weigh security risks against those benefits. The following are some technical security issues that translate to business risk:

- **Physical and virtual servers have important differences regarding data security**
  Traditional bricks-and-mortar data centers are built around physical servers, and their approach to security is still dominated by a perimeter-defense strategy. Physical machines are largely fixed, sit in a locked room, and are typically only accessible by a limited number of administrators. Server virtualization, even in the private data center, changes the security landscape significantly. The mobile nature and distributed mechanisms of virtualization introduce new variables, management processes, and security concerns that were much more limited in the traditional and more static data center. Moving those VMs to a managed host or public cloud service can create security problems that undermine every advantage the cloud brings. We’ll discuss those problems below.

- **The cost benefits of commingled infrastructure can bring a loss of data separation and data privacy**
  One of virtualization’s most valuable assets is the possibility of the elastic use of computing and storage resources. A VM can be moved dynamically from one piece of hardware to another as capacity and performance needs arise. This also means that a VM frequently runs alongside other VMs on the same host and typically within commingled storage. The use of VMs in the public cloud almost always involves commingled infrastructure, but maintaining secure separation of data in a commingled environment is important and not trivial. Most providers recognize that, at a minimum, they need to provide multi-tenant separation of data. They can do this by offering separate physical devices; however, this raises the cost and defeats much of the efficiencies and cost benefits for both the customer and the provider. A data-privacy solution that provides cryptographic separation of commingled VMs and data is the ideal answer as long as it operates automatically, with high-performance, and where the associated encryption and security are handled transparently.

---
3 Ibid., pg. 5. 53% of IT managers said they are not ready to move protected-class data to the public cloud because of security concerns.
key management functions work in concert with VM movement and over the entire life of the VM.

- **VMs are exposed to more systems, administrators, hosts, and storage locations than physical servers**

  The number of hosts and persons that a VM is exposed to tends to increase. Unlike their physical server forebears, virtual servers and their virtual disks are highly mobile and are easily duplicated, cloned, replicated in storage, copied to disaster recovery archives, and moved between data centers. For example, a simple Storage VMotion command moves a VMware virtual disk from one device to another location while the VM continues to run. How does the security of the new storage location differ from the previous one? Who has access to it? Who can affect its management or backups? The flexibility and simplicity of these activities belie their potential security risks.

  A knowledgeable IT manager knows that security risks come from more than the actions of an outside hacker. One study of data breaches characterized 52 percent of security incidents arose from insider actions that were predominantly accidental. A CSP's data center is subject to insider threat (whether intentional or accidental) as much as any other IT operation. If customers are going to entrust their important data assets to the care of the CSP, then data privacy must be paramount in the delivery of those services. A solution that not only encrypts customer data but ensures that the provider cannot gain access to that data or the associated encryption keys is becoming a hallmark of security best practices in the cloud.

- **The files that make up a VM image are security sensitive and need protection**

  It is important to protect both the data and the VM images. Here's an example of one of the essential differences between a physical and virtual server:

  A database application is running on a physical server that is required to comply with payment card (PCIDSS) regulations. Common practice has been to use columnNlevel or tableNspace encryption to protect the credit card numbers in that database. Doing this on a physical host satisfies PCIDSS regulations. Now consider if that server is virtualized. If that host becomes too busy, the hypervisor pages virtual memory, or if the VM is suspended, the memory image containing the encryption keys is written to disk and so exposed in storage. To locate and expose those keys is suddenly trivial if the VM image files are not protected.

  The storage where VM images reside must be protected. In fact the recent update to the PCIDSS guidelines published in 2011 now acknowledge the need to protect these memory images.

- **Moving data off-site pushes the security discussion up the chain of command**

  Decisions concerning data security practices have traditionally fallen to the CIO, CSO, or other securityNknowledgeable person. In a purely private data center, most security decisions are about choosing the degree of security best practices to adopt while not disrupting business operations or overburdening budgets. In the public cloud however, the security discussion is increasingly not only one of technical practice, but about contract SLAs, legal, and fiduciary responsibilities. Thus, moving servers to the public cloud raises the visibility of security decisions beyond the IT team alone.

- **Business leaders see the cloud as an essential mechanism for companies to compete and survive**

  Businesses that deliver products, solutions, or services and intend to scale must figure out how to leverage the Cloud to deliver that value to their customers.
Companies that do this will replace those that do not. CEOs, CFOs, and their corporate boards are beginning to recognize that the use of the cloud is not just about IT costs but about achieving the flexibility to rapidly bring up the services and systems needed to be competitive and achieve strategic objectives. To realize these benefits, cloud use cannot be relegated only to ancillary IT functions. Cloud flexibility must be extended to the important applications that are central to the core value proposition of the company.

Some IT managers have pushed back, saying that the cloud can’t handle mission-critical and security-sensitive data. However, the increasing adoption of cloud services demonstrates that these excuses have lost their potency. Organizations know that in time they will move much of their operations to the cloud. The critical question that remains is which CSPs will they trust to house their most important application workloads.

- **Data privacy legal issues now have the attention of customers’ top-level legal counsel**

   Approximately 51 laws about data breach exist in the United States alone. If certain private data is exposed, or is suspected of having been exposed, these laws and their legal consequences are triggered. It does not matter whether the data breach occurred within a private data center or at a CSP’s site. It does not matter if the breach was due to the activities of an outside hacker, the deliberate actions of a rogue insider, or an error made by a trustworthy employee. A data breach and its legal consequences remain the responsibility of the company that owns the data, which makes the legal risks substantial enough that these issues now have the attention of the customers’ legal counsel.

   Similarly, issues of data sovereignty have legal significance when companies move their data to the cloud. In some European Union countries, it is a violation of law for certain private information to cross national borders. In the U.S., a CSP can be compelled legally to turn over an individual’s private data without informing the individual. For example, BAE, the large UK defense contractor, withdrew from its planned adoption of Office 365, Microsoft’s cloud collaboration software, at the behest of its legal advisors because Microsoft was unable to guarantee BAE’s data sovereignty.

- **CEOs increasingly recognize that accountability for data security risks is part of their fiduciary responsibility**

   The cloud will become the dominant model for corporate IT, so it follows that data security in the cloud is being discussed in the corner office. Today’s CEOs have read the horror stories of public data breaches that have resulted in millions of dollars in damages to a company’s finances and reputation, and they recognize that the resulting cost to a company’s reputation can go far beyond the cost of a lawsuit. The loss of faith by customers following a data breach can be devastating. Until recently, a CEO’s plan for responding to those threats would have been to bang the table a bit harder when meeting with IT management and discussing the importance of data security. But now the CEO expects the IT managers to provide a cloud adoption plan and one that includes assurances about data security. CEOs know that these issues can be significant enough to affect their own tenure and the future of their company.

- **CSPs that meet cloud customers’ needs will transition security concerns to new business**

   It is important to understand the questions that cloud customers have about data security and how to provide them with answers they need to hear. Data security does not have to be burdensome. A suitably designed data security solution can
operate simply, automatically, and without disrupting the functioning of customer applications. The solution can be easy to manage, not cause applications to run slowly, and need not be a continual problem for customers and customer support personnel. Customer questions about any security solution (in particular, an encryption-based security solution) usually revolve around overhead and risk: How much management complexity and time will it impose? How much performance overhead will we experience? Will it slow down our applications? What are the risks of not being able to retrieve our data in an unencrypted form? Is there a risk that we could lose our crypto keys? The goal of a well-designed solution is to address these concerns while satisfying the most important needs for data security in the cloud.

**Cloud customer needs satisfied by an encryption-based security solution:**
- Data remains private in the comingled environment of the cloud
- Access to customer data as it is stored, moved, and replicated in the cloud
- Ability to retrieve or withdraw customer data from the cloud without leaving unprotected data behind
- Compliance with data regulatory requirements like PCINDSS, HIPAA, etc. when needed
- Access to audit records that demonstrate that they have taken proper care in securing their data
- Meet safe harbor requirements from breach notification laws in the event files were exposed in the cloud
- Minimal management complexity, overhead, and risk

The CSP that makes these benefits available to its customers is creating an environment where customers can be confident about deploying mission-critical and security-sensitive virtual workloads in the cloud. While we know that providing these services can attract new cloud customers, how can these services be offered in a way that satisfies the business, economic, and legal needs of the CSP?

**CSP needs satisfied by providing an encryption-based security solution:**
- Wins new business by providing sufficient answers to the data security questions of prospective cloud customers
- Allows the CSP to (optionally) up-sell secured infrastructure services at a premium price
- Offers support for cloud customers requiring regulatory compliance (PCINDSS, HIPAA, etc.)
- Offers improved service level agreements as part of cloud customer contracts when demanded
- Provides the means to securely migrate VMs and data from a customer’s private environment to the CSP’s cloud
- Maintains separation from the customer’s actual encryption keys to avoid exposure to the customer’s data, legal issues, and disclosure demands from authorities
- Provides encryption of VM images for backup and disaster recovery
- Affords safe harbor from public notification in the event that customers’ stored data was accidentally exposed or is suspected to have been exposed. This applies where data breach laws provide safe harbor from notification for data that was encrypted.

- Differentiates the CSP’s service offering from lesser providers based on promoting their data security best practices.

Capabilities that meet both customer and CSP needs

Given the needs described in the previous section, the following are the specific capabilities and features of a suitable encryption-based solution.

Capabilities important to cloud customers:

- **Data4security controls are provided automatically, transparently, and easily, without customers having to change their operations.** The best way to mitigate customer concerns is to make the solution (almost) entirely transparent. Customers should be able to go through the same process of signing up with the CSP as they always have. In the simplest case, customers need not do anything other than check the box that indicates they want their data encrypted. For more sophisticated use cases, customers should be able to make a few policy choices and stipulate who is granted administrative privileges for controlling policy on a given set of VMs. Once that is done, the customer can simply proceed with their normal use and management of those VMs.

- **Encryption should be non-disruptive to the customer’s applications and business practices.** Traditional encryption solutions have too often been complex and disruptive. For instance, a customer deploying encryption has had to take their important applications offline for extended periods in order to initially encrypt large data stores. Further, the added CPU burden of encryption has slowed their important applications and compromised efficiency and the quality of the user’s experience. Still more disruptions would occur when encryption software was being upgraded, key management servers went offline, or when data needed to be “re-keyed” because of regulatory requirements or in response to security-sensitive circumstances. A modern and proper encryption solution solves these problems and does so without burdening the user. With these solutions there are now ways to automatically encrypt data on-the-fly as an application runs, and to do this while leveraging on-the-chip crypto acceleration capabilities for high-performance. Lastly, the Key Management system serving these deployments must be highly available and the customer should never experience a situation where keys are not available.

- **Encryption should be comprehensive and applicable to any virtual workload that needs protection.** In the past, encryption was complex enough that only a small number of systems would be encrypted and only when absolutely required. Now, with virtual workloads and data moving between data centers and into the cloud, encryption can and should be applied to any workloads as a fundamental security practice. Virtualization-aware encryption solutions are capable of encrypting any virtualized workload, any data store being used by it, and encrypting the system drive (containing the guest OS) of the VM itself. All of these elements are important for the security of the VM and its data. All should be encrypted, and all encryption should happen automatically.

12 Re-keying: The process of decrypting data previously encrypted with an old key and re-encrypting it again with a new key. Re-keying is most often undertaken because of data security regulatory requirements, or as good data security hygiene when a change is made in the admin personnel of an IT organization.
Key management, and the complexities of handling, escrowing, recovering, and protecting keys, should be done automatically.

Key management is not well understood and is often intimidating to customers and many IT staff. Crypto language is arcane, and the mechanics of secure key storage and distribution are often counterintuitive even to IT professionals. The solution should provide a policy management model that automatically deals with the mechanics of key handling to remove this burden from customers and CSPs.

Customers can retain exclusive control over who can grant access to their encryption keys.

Some security-sensitive customers are concerned about issues of data sovereignty and about the access to encryption keys by accident or misuse of privilege. For those customers, a well-designed system allows them to retain control over who can gain access to keys. This key-handling mechanism should not interfere with normal operations, but should act as assurance to customers that only they can grant access to encryption keys and that CSPs do not have the means to bypass that authority.

Data should be accessible at any time in unencrypted form as long as suitably authenticated access is granted.

Customers need to know that there is always a way that they can gain access to their data. Sufficient access controls need to be part of the system, but customers should not feel like access to their data could be permanently lost if a hardware error or other problems arose.

All administrative and data-access activities should be audited with a history available at any time.

Customers want to know that their protected data is being monitored and that an audit log is being kept that shows their due diligence in data-security practice and to accommodate regulatory compliance requirements.

Capabilities important to CSPs:

Data security controls delivered automatically, transparently, and easily, without CSPs having to change their infrastructure.

CSPs need an encryption system that automatically provides multi-tenant separation of customer data within a CSP’s comingled infrastructure. The encryption solution must automatically protect a customer’s VMs and data and have that protection travel with the VM throughout its life. Protection, and the associated security policy, should inherently move if the VM is moved between virtualization hosts, transferred to other storage locations, copied to backups or disaster recovery systems, etc. The solution should act in a way that does not interfere with a CSP’s existing IT management practices, security tools, and storage and network hardware.

The encrypting system does not impose an unreasonable performance burden.

At some level, both IaaS and SaaS providers are in the business of selling compute cycles. A data security system must not consume too many cycles and unduly affect the business economics of a CSP’s infrastructure. Encryption has traditionally been reserved for limited use cases and special data sets, but that old view is giving way to new technology, software techniques, and the need to protect data as it moves between different physical systems.
Crypto technology itself is now faster and more ubiquitous. CPUs are substantially faster and better equipped to service the underlying mathematical operations that crypto requires. Additionally, specialized hardware for crypto is now available or is already present in most servers hosting virtualization. For example, the AESNNI capability is built into standard Intel and AMD x86 chipsets and provides the means to do AES bulk encryption at hardware speeds, up to ten times faster than software-based encryption. It is important that the solution is able to automatically detect and utilize these crypto-hardware accelerators. Further, the software of the solution should be smartly designed, should operate transparently and in conjunction with the underlying mechanics of the virtualization and storage infrastructure, taking advantage of caching and performing only-as-needed encryption at the points that are most optimal.

- **A fully capable management API and CLI alongside an easy-to-use (but optional) GUI is included**

  CSPs must operate their infrastructure in a way that scales; is extensible, highly available, and recoverable; and can be managed entirely using automation. The solution should have an intuitively simple and easy-to-use GUI for customers and CSPs. However, a CSP must be able to call on an API that lets management of the system be scripted and able to run with no (or very little) human attention. These API functions must provide for all administrative functions, from initial provisioning of a customer to the point where the customer’s VMs and data are securely decommissioned.

- **The solution must generate an audit stream suitable for the customer’s regulatory compliance needs and to show evidence of the CSP’s proper due diligence**

  The CSP is the custodian of the customer’s data and must be able to show they provide due care to both the customer and to any authorities or auditors. The encrypting solution should provide an audit stream of who, when, and where all administrative functions were performed. This audit history should be easily viewable by customers and should be easily exported to or imported by standard log management servers.

- **The CSP can host key management while the customer (or third-party service) keeps access to the actual keys**

  In some circumstances CSPs will want to keep access to a customer’s actual data encryption keys at arm’s distance. The system should be able to utilize the needed keys automatically while the actual keys that encrypt the customer’s data are also securely encrypted and safely stored within the key management system. A further step, and one that benefits both the customer and CSP, is to further encrypt keys in a way that only the customer can grant access to their stored data encryption keys. This gives the customer the confidence that only they can expose keys to others and gives the CSP protection from any ability or perception that they could expose the customer’s keys.

  Alternatively, a third-party key management service could be offered out of the cloud. This service can be used by the customer directly or by the CSP. In either case, the result is the same: The CSP will have no ability to directly access the data encryption keys of the customer or offer...
those keys to another agency. This possibility has become a concern for customers sensitive to the legal jurisdiction in which their hosted VMs and data may reside. If the customer is the only one able to grant authority to view data encryption keys, then the CSP does not have the means to expose keys and so cannot be compelled to do so.

Conclusion
Encryption is a powerful tool to ensure that data remains private. Its use has traditionally been reserved for special circumstances and selected hosts. The fact that data processing and storage is now moving to the cloud has changed the demand for data privacy and the need for encryption in substantial ways. Customers are increasingly moving mission-critical applications to the shared IT infrastructure of the cloud. However, they will do this only with CSPs that can fully satisfy their regulatory, legal, and data privacy needs. Fortunately, new and well-designed encryption-based solutions are capable of satisfying both the needs of customers and the business imperatives of the CSP. Those CSPs that adopt these solutions will be the ones that differentiate themselves from their lesser peers and so win the business of new cloud customers.

About the author
Bill Hackenberger is the VP of Data Security at HyTrust, Inc. Bill is a 25+ year veteran of enterprise security and just prior was CEO of HighCloud Security, a software company specifically created to address unique data privacy and encryption needs within private, hybrid and public clouds and serving corporate and government organizations. For more information on HyTrust, visit www.hytrust.com.