What you need to know about infrastructure as a service (IaaS) encryption
Table of Contents

4 Executive summary
4 Virtualized environments need different security
4 Data out of your control
4 Encryption that travels with the mobile VM
5 Data sovereignty
5 Snapshot and suspend files
5 Administrator access
6 Decommissioning
6 Misconfiguration
6 Multi-tenancy
6 Loss of visibility
6 How does HyTrust DataControl™ help mitigate IaaS data privacy concerns?
7 The benefits of HyTrust DataControl
8 Summary
8 IaaS encryption checklist
9 Appendix A
What you need to know about infrastructure as a service (IaaS) encryption

Executive summary
In this paper, we’ll look at the unique data privacy challenges for virtualized environments, especially public cloud Infrastructure as a Service (IaaS) and review how the HyTrust® DataControl™ solution can help your organization address these concerns.

Virtualized environments need different security
The best practices for securing physical servers are fairly well understood. Firewalls, intrusion detection, anti-virus, encryption, access controls, monitoring and auditing, along with physical security like locked cabinets and data centers, go a long way toward defending your sensitive data.

However, when you consider using IaaS from a cloud service provider (CSP), traditional security measures, such as full drive encryption, don’t always translate. Virtualization is the foundation of most IaaS. It is what allows for the flexibility and fast scale-up that makes the cloud attractive. However, virtualization, without proper controls, introduces new security challenges.

If you are concerned about data privacy and the security of your virtual machines running in the public cloud, here are some basics you need to know.

Data out of your control
This is perhaps the most obvious concern that CSOs voice when considering a move to IaaS. It’s a visceral reaction: Data that leaves your premises simply “feels” less secure. It may be visceral, but this concern is well founded.

Even the most reputable CSP that employs the same security practices you may follow in your own data center is still subject to human error or insider threats. It is no mistake that the contract you sign with your CSP specifically states that your data is your responsibility. This has significant implications for your organization’s reputation as well as its legal and fiduciary responsibilities. Given all of this, it is essential that you understand and control the risks associated with virtualized infrastructure.

Encryption that travels with the mobile VM
By design, virtual machines (VMs) and the virtual disks containing their data, are mobile. In the past, you may have encrypted security-sensitive data via standard disk encryption in order to comply with data protection regulations (like PCI-DSS).
However many of the security solutions that worked with static physical systems are not well suited to the dynamics of the virtualized data center. One of the fundamental strengths of virtualization is that it accommodates the movement of VMs and data to other devices (or to public or private clouds) to take best advantage of compute resources. That movement (in a VMware environment for instance) could be accomplished simply by running the command to perform a Storage vMotion. In such a case, the encryption protections will not travel with the VM. You need to consider more dynamic encryption methods that are built for the cloud and can ensure your VMs remain secure wherever they reside.

**Data sovereignty**

Depending on what country (or other legal jurisdiction) you work in, you may be legally obligated to make sure data is not accessible outside of that jurisdiction. Data privacy laws are now myriad and changing. This is particularly true if your company operates within European Union countries where data privacy laws are strong. It is the legal responsibility of your company, not the service provider, to ensure that data is not accessible outside these jurisdictions. Also consider that in the U.S., a CSP can be compelled legally to turn over private data to authorities without informing the user. In both of these cases, it is valuable to have an encrypting solution that allows you to have control of your encryption keys rather than giving key control to the CSP.

**Snapshot and suspend files**

People are generally familiar with the concept of virtual disks (often called VMDKs in VMware terminology) where each virtual disk acts like a disk in the physical world. There are a number of additional files that collectively make up a VM image: Snapshot files, suspend files, paging files, and other files that the hypervisor uses to run the VM. These files also contain sensitive data like usernames, passwords, credit card data, and literally anything that could reside in a system’s memory. This makes VM images another place where the security of a VM is different from that of its physical host predecessor.

Regulators have now begun to recognize these vulnerabilities. In June 2011, the Payment Card Industry (PCI) Standards Council released “PCI DSS Virtualization Guidelines,” an information supplement to the latest Data Security Standard (DSS). The document highlights vulnerabilities that virtualization introduces, including the exposure of credit card and other sensitive information in snapshot files, as well as dormant VMs.

The backup of a VM image in general has security implications. Consider how they would differ from the traditional backups of older systems in that restoring from a old backup tape would require locating legacy hardware, installing the right (and possibly outdated) operating system and version, prior releases of applications, and so on in order to re-create that system—an arduous task! Compare this to a VM that can lie in backups for years but then be easily spun up since the operating system, applications, and application data are all held together. It not only provides the data but all of the software and conditions that allow the applications to be run again.

As the new PCI guidelines indicate, encryption of just the application data is no longer sufficient, especially as we move to a cloud-based world where VMs are increasingly mobile. Each place a VM runs, you have the potential of leaving a trail of sensitive data.

**Administrator access**

The exploitation of insider accounts has been in the news with increasing regularity. The spectacular data breach at the U.S. National Security Agency (by Edward Snowden) or the theft of credit card and identity data of more than 100 million consumers at the large retailer Target are just a few examples. These are examples...
of either the intentional misuse by an insider or an external party that was able to gain the privileges of an unknowing insider. In either case, breaches through the use of an insider are significant, typically take much longer to identify, and cost the company significantly more than a breach from outside. The reality is that no matter how well you hire, there is still a risk of an administrator, either intentionally or by accident, accessing or exposing information that they shouldn’t.

When you outsource to a CSP, you are forced to place your trust in their insiders and IT administrators. If you do not encrypt any data you put in the cloud (and maintain the keys yourself), the administrators who have access to the CSP’s infrastructure (and your stored VMs) can easily access data.

**Decommissioning**
Ask your CSP how many copies of your VMs exist in their cloud. A large CSP we spoke to explained that they immediately replicate VMs at least three times to different locations to ensure availability and disaster recovery. While this is good for service level agreements, it’s concerning from a security perspective. Not only are there more copies of your data floating around, but what happens if you want to leave that CSP? Can they guarantee that your data has been removed from all locations, including backup media? CSPs will not state in writing that all copies of your data can be deleted—it simply isn’t feasible. There are no existing standards to ensure that disks and backup media are properly wiped before disposal or repair. Keeping your data encrypted and retaining the keys in your own data center allows you to safely decommission a VM by no longer communicating the keys for decryption into the CSP’s environment.

**Misconfiguration**
Humans make mistakes. Amazon learned this lesson recently when users who misunderstood or misconfigured privacy settings had inadvertently exposed 126 billion files on its S3 cloud. Simple errors by users or IT staff can accidentally leave data accessible to unauthorized users.

**Multi-tenancy**
Even if you subscribe to a virtual private cloud at your CSP, you will likely be sharing physical servers with other cloud tenants. The co-mingled data on the CSP’s servers can become a very attractive target for an attacker. If the CSP’s storage device incorporates encryption, it is often the case that the same key is used for your data and everyone else’s. This is why a multi-tenant key management system is so important. It keeps your VMs and data cryptographically separated (encrypted with many different and confidential keys) even as your VMs are co-mingled in storage.

It’s also possible that your data could be inadvertently seized should one of your cloud neighbors get into legal trouble. A situation like this happened in Ohio in 2012 when a local broadcaster had his videos taken offline when authorities seized servers from his CSP that contained his data along with the data of another company that was the target of a criminal investigation.

**Loss of visibility**
Because your applications and data no longer reside on your network, you have reduced visibility for monitoring and analysis. While forward-thinking CSPs are finding ways to improve these capabilities, you need to have a certain level of comfort that your data is safe, even if you don’t have the regular reporting feedback to prove it.

**How does HyTrust DataControl™ help mitigate IaaS data privacy concerns?**
HyTrust DataControlTM is software that addresses data privacy concerns for enterprises and for CSPs with flexible, easy to deploy encryption and
HyTrust DataControl is composed of two key components, which work together to achieve your security objectives in both private and public clouds.

HyTrust DataControl incorporates:

- **HyTrust KeyControl™**: HyTrust KeyControl software is a robust, security-hardened key management system that is simple to deploy and easy to use. It is a clustered, highly available solution suitable for any organization from the smallest firm to the largest enterprise. KeyControl administrators don’t need to understand cryptography—administrators simply set the desired key strength and policies for key retention or rotation, and the KeyControl software does all the work. KeyControl is a virtual appliance, deployable as a high-availability, active-active cluster, supports role-based administration and separation of duties, is fully multi-tenant, and automatically generates an audit-history of all administrative functions.

- **HyTrust DataControl Policy Engine**: Organizations that want to encrypt applications and data in any virtualized data center and any private or public cloud can quickly install the Policy Engine module into the guest OS of their VMs, ensuring data is secure regardless of where the VM runs. HyTrust encrypts any virtual disk partition and protects the system/boot drives of the VM. The Policy Engine automatically encrypts and decrypts transparently, as the VM runs. Further, HyTrust can initially encrypt data – or re-key it – without taking applications offline. This unique capability prevents downtime and more easily enables compliance with regulations like PCI.

**The benefits of HyTrust DataControl**

Using HyTrust DataControl software, organizations can address a wide range of data privacy concerns in virtualized environments.

- **Regulatory compliance**
  Much has been written about privacy laws like HIPAA/HITECH, PCI DSS, and the disclosure laws that exist in almost every state in the U.S. PCI DSS has recently included specific language, drawing attention to the vulnerability of VMs. HyTrust DataControl can help your organization maintain compliance with these regulations, even as your organization moves to private, hybrid, and public clouds. Further, HyTrust’s NIST-approved AES-256 encryption, along with secure key management that can be managed on premise, can reduce the chance you will have to make any costly notifications in the event of a breach.

- **Separation of data from keys**
  HyTrust KeyContol can be run on physical or virtual hardware, on premise, or even at a third-party service provider, separate from the CSP. This ensures only you—and your authorized administrators—have access to keys. KeyControl is policy based, so you don’t have to be a crypto expert to use it.

- **Zero-downtime deployment and re-keying**
  Many regulations, including PCI DSS, have requirements to re-key encrypted data on a periodic basis. Further, organizations also have internal policies that mandate re-keying data if administrators leave the company or when other security-sensitive events happen. If you have a lot of data, re-keying can be a lengthy and time-consuming process that is disruptive to your business operations and requires you to take applications and data offline for extended periods. HyTrust DataControl allows you to initially encrypt and re-key data while your VMs are...
running to minimize any downtown of your applications and your business operations.

- **Cryptographic multi-tenancy**
  You can easily introduce true multi-tenancy to provide separate policy administration and cryptographic separation of data for the departments or customers your virtualized infrastructure is supporting. Enterprises running private clouds can ensure applications and data from different departments or offices are not exposed to anyone who shouldn’t see them.

- **Constrain admin access**
  With Hytrust DataControl in each VM, you can encrypt data from within the VM itself and so it is protected all the way through the hypervisor as it travels to storage. This can prevent an administrator with management access to the virtualization infrastructure from directly accessing your applications and data. Further, the Policy Engine provides for encryption of the VM’s operating system drive and includes a first-time authentication process, which ensures that VMs that have been suspended or copied cannot be spun up into a new instance without proper credentials.

- **Avoid being locked-in to a single IaaS vendor**
  Encryption is one of the best ways to ensure that you don’t leave a data trail as your VMs travel around the cloud. With HyTrust DataControl, you can change service providers or withdraw from the cloud by simply shutting down your VMs and deleting the encryption key, ensuring that any copies of data that still exist in the provider network are permanently inaccessible.

**Summary**
Good security practices shouldn’t happen just because someone tells you to. With HyTrust’s rock solid, enterprise-grade encryption and key management system, security can become an enabler. You can virtualize your mission critical applications. You can move to the public Cloud. If you’d like to learn more about encryption, visit http://www.hytrust.com.

**IaaS encryption checklist**
If you are evaluating encryption for private, hybrid, or public clouds, Appendix A will provide a handy checklist of features you should look for.
## Appendix A: Checklist for evaluating VM encryption systems

<table>
<thead>
<tr>
<th>Capabilities</th>
<th>Key functionality</th>
</tr>
</thead>
</table>
| Supports all IaaS environments    | - Vendor and platform agnostic  
- Works with any IaaS cloud  
- Supports public, hybrid, and private clouds  
- GUI and/or API driven                                                                                                                                  |
| Optimized for virtualized environments | - Scalable to large enterprise and multi-tenant cloud environments  
- Integrates with all DAS, NAS, and SAN storage systems for rapid deployment  
- De-duplication of VMs for space efficiency and reduced storage cost                                                                                  |
| Transparency                      | - Can be deployed into functioning networks  
- Able to re-key data in place, while VMs and applications are running                                                                                   |
| Strong encryption                 | - Uses standards-based, NIST-approved algorithms like AES-256  
- Can support encryption of all VM files, including snapshots, suspend files, and so on, that can contain sensitive data, as recommended by PCI standards                                                                 |
| Policy-based key management       | - Easy to deploy and manage without crypto expertise  
- Can be replicated for redundancy and availability  
- Can run on a physical host or run as a VM  
- Can be deployed on premise or at a service provider  
- Supports true multi-tenancy, role-based administration and separation of duties  
- M of N recovery for master key to protect against insider attacks                                                                                   |
| Performance                       | - Auto-detection and use of in-chip hardware encryption, like Intel's AES-NI, for 3-10X performance increase  
- Encryption happens at hardware speeds; overhead is negligible                                                                                         |
| Integration                       | - Complete APIs to allow custom integration into existing cloud infrastructures and to automate broad deployments                                                                                                 |
| Support backups                   | - Encrypted backup of complete VMs using standard storage backup tools                                                                                                                                              |
| Auditing and reporting            | - Supports auditing and reporting of all administrative and VM runtime activities  
- Capable of meeting legislative and regulatory compliance requirements, PCI-DSS, HIPAA, etc.  
- Support exports to external log systems                                                                                                               |