WHITE PAPER

HYTRUST
Cloud Under Control

# Top 10 Reasons You Need Encryption

## Executive Summary

When you talk about encryption — especially to someone who isn't a security specialist — you often get a variety of interpretations. In general, encryption is most often perceived as some dark alchemy only used by government agencies with three-letter acronyms — a complex, scary beast that can only be tamed by brilliant mathematicians. More commercial applications like SSL have come a long way in helping to 'modernize' this perception, but we still have a way to go. As with any technology, poor implementation can result in poor perception, and encryption has definitely suffered from this in the past.

In reality, if deployed correctly, encryption does not need to be a headache. Instead, encryption can be an enabler to achieve the flexibility, compliance and data privacy that is required in today's business environments. In a world that's increasingly built around virtualization and cloud, the need for encryption is even more important, and the need for organizations to retain control over data, particularly in cloud environments, is paramount.

In this paper, we explore 10 of the common benefits of encryption and show you how HyTrust DataControl™ uniquely removes the barriers to adopting an encryption solution.

## Benefits

### 1. Encryption Helps you Move to the Cloud

Everyone is concerned about moving sensitive data to the cloud, and many organizations perceive that the cloud is not as safe as their own data center. If your data is in the cloud, it's not only possible that strangers might see it, but your data could be sitting on the same storage as your competitors. Imagine how much that treasure chest could be worth?

Encryption can make it possible to leverage the benefits of Infrastructure as a Service, while still ensuring the privacy of your data. HyTrust DataControl ensures data is encrypted in flight, and at rest in storage. Because you retain control of your encryption keys, you're still in control, even when data has left your building. If the service provider makes copies of your VMs, only encrypted data is copied. And at all times, you determine when to deliver — or revoke — the keys.

### 2. When You Own the Keys, You Can Easily Decommission/Deprovision

Would you put your most treasured valuables in a safe and give a stranger the key? Would you have your data encrypted in the cloud and have the cloud service provider own the keys? Probably not the most secure option?

Organizations want to take advantage of the cloud for its cost and flexibility. Part of this value is the ability to spin up or decommission servers as business needs change. But what happens if you want to leave your service provider? How do you avoid "vendor lock-in" when dealing with a provider? You want to be sure you can get your data back, but you also want to make sure you're not leaving sensitive data behind. How many copies or backups of your VMs has your service provider created so that they can achieve their operational uptime SLA's? The answer is "Many". It's simply impractical for a CSP to retrieve and delete every copy.

Let's suppose you wanted to transition your operations from one cloud provider to another. If you have encrypted your VMs with HyTrust DataControl then it is straightforward. You shut down your VM and move it to the new provider, then instruct the system to rekey with a new key. Then you can withdraw from the old cloud provider by simply instructing the system to shred the old key. All your data held by the old provider — including copies and backups — is as good as gone! Without encryption your data could remain in storage or backups and potentially exposed into the indefinite future. Think of encryption as a form of insurance against a future data breach.

### 3. Encryption Helps you Achieve Secure Multi-Tenancy in the Cloud

In virtualized cloud environments, multi-tenancy is what drives costs down and increases flexibility. Why dedicate one enterprise-level server to one workload when it can serve many? While virtualization is not new and organizations have taken advantage of its virtues for years, having your VMs and applications running on the same physical servers as other departments or organizations raises some security concerns. Not only do virtualized servers become richer targets, but if those machines are running in a public cloud infrastructure, you have limited control over who 'shares' your hardware. And while strides have been made solving many of the network segmentation issues, another major security challenge still exists: what happens to your data within the storage fabric?

If you encrypt data before it enters the cloud, and retain control of the encryption keys, you can ensure your data is safe, regardless of its neighbors. HyTrust DataControl provides the ability to encrypt the data in VMs before moving them to the cloud while you retain control of the encryption keys in your data center.

### 4. Separating Data from Key Services can Prevent Service Providers from Accessing or Accidentally Exposing your Data

Earlier we talked about putting the family treasures in a safe and giving the key to a stranger. If the service provider has both your encrypted data and your encryption keys, in concept, they could have access to your data. The rule-of-thumb that you should never store your keys along side your data is a good one. While you may be working with great service providers, as has been seen in the news, problems and security breaches happen to them as well. So to avoid this problem, the practice of encrypting your data in the cloud and holding your own keys in your private data center just makes sense.

However, some organizations simply don't want to host key management on their own computers. They want to put it all in the cloud given all the benefits of elasticity, backup, availability and DR. This is where a third party comes into play. Why not have your encrypted data and virtual machines with one service provider and have your key management hosted with another service provider?

A third party hosting your key management solves many of these challenges by making sure that key servers are always accessible — always backed up, replicated and not prone to disaster.

With HyTrust DataControl it's a win-win situation. You use HyTrust DataControl with one service provider, who then holds your data, but doesn't hold your keys. You install HyTrust KeyControl™ with another service provider and they then hold your keys but have no access to your data. With the simplicity of self-service elastic hosting today, this can be accomplished in a matter of minutes. Encryption now becomes a simple option even if you don't have any on-premise computers of your own.

### 5. Encryption Helps You Meet Regulations

The Payment Card Industry (PCI) has strict guidelines to ensure protection of cardholder data. We all use credit cards and understandably want assurance that our information is safe. Naturally, encryption is a major piece of the PCI Data Security Standard (PCI DSS). But there's also HIPAA/HITECH, regulations that mandate protection of health care information. Once again, encryption is a critical part of the standard.

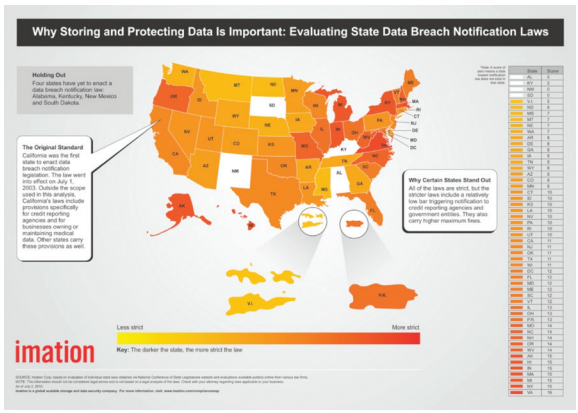
Add to the mix the Gramm-Leach-Bliley Act (GLBA), the Sarbanes-Oxley Act (SOX), the Basel II Accord, Euro SOX, the Financial Instruments and Exchange Law of 2006, FDA Title 21 CFR Part 11 (1997), 95/46/EC European Union (EU) Directive, Germany's Bundes-Datenschutz-Gesetz (BDSG), California Senate Bill 1386 (SB 1386), Canada's Personal Information Protection & Electronic Documents Act (PIPEDA), Britain's

Data Protection Act (DPA) of 1984 (Amended 1998), Japan's Personal Information Protection Law (PIPL) OF 2003 and many, many others.

Although not all standards mandate encryption, it's highly recommended. Given the high cost of breach notification and the fact that DLP technology is always revealing sensitive data in places you wouldn't have thought, doesn't encryption just make sense? After all, we wouldn't shop online without it.

### 6. Encryption Gives you Safe Harbor from Breach Notification

Did you know that there are data breach notification laws in 46 of the 50 states. The Imation graphic on the right shows the variations of the laws by state. In fact the average cost to an organization for a data breach was $5.5 million in 2012!




If a data breach occurs and personally identifiable information is lost, the breached party must notify all individuals who are impacted. Just recently, Global Payments indicated in their quarterly SEC filing that the company expects to pay $94M to address its 2012 security breach of 1.5 million credit and debit card numbers.

The vast majority of these laws have a safe harbor clause from public notification if the stolen data is encrypted and if the encryption keys are not compromised. Therefore, deploying encryption and robust key management could save you millions of dollars in the event of a breach.

With HyTrust DataControl, no-one can get access to your encryption keys!

### 7. Encryption Gives Services Providers a Competitive Edge

As a cloud service provider (CSP), you are a guardian of your customers' applications and data. Thieves are getting smarter and regulations are getting more stringent. The good news is that security technology is also getting better.

Encryption and key management software, designed specifically for virtualized environments, can help you significantly improve your security posture, attract new customers, and expand your business with existing clients. This allows you to:

- Gain competitive advantage and differentiation
- Expand revenue potential to customers with sensitive or regulated data
- Protect customer data against access by unauthorized users
- Satisfy data residency and privacy requirements

- Reduce hardware costs through cryptographic multi-tenancy
- Assure customers that they can de-provision securely without leaving data behind

Newer encryption technologies like HyTrust DataControl are easy-to-deploy, offering robust APIs that allow for seamless integration into the CSP environment.

### 8. Encryption Gives you Confidence that your Backups are Safe

In October of 2012, TD Bank reported the loss of two backup tapes that may have exposed personally identifiable information about 260,000 of the bank's 8 million U.S. customers.

In March of 2012 the California Department of Child Support Services lost the private data of 800,000 of its clients because of lost data storage devices.

In November of 2011 there was a massive data breach affecting 4.9 million individuals who received services from TRICARE, a provider of health care services to active and retired military personnel. Once again, the data breach occurred as a result of lost backup tapes.

These are not isolated cases. A simple Google search will show many more examples of backup tapes that go missing, disk drives being disposed of without erasure, etc. Now what would happen if the data on these tapes or other backups was encrypted? The answer is quite simple — nothing! Without access to encryption keys, data protected using HyTrust DataControl and its NIST-approved strong-encryption cannot be decrypted. Use encryption to be sure that any device (tapes, backup drives, solid-state drives, backup-images in the cloud, etc.) are safe.

### 9. Encryption Allows you to Secure your Remote Offices

Many organizations have remote offices that, by their very nature, are not as secure as they should be. The opportunity for physical theft of computers and storage is very real. Many of these organizations have sensitive data sitting on these servers unprotected. Just think about it. Financial planners, tax accountants and other service organizations all have important data sitting in their offices. And these are many of the same organizations that are afraid of data leaving the building and going to the cloud.

Well trained IT staff are often scarce at these sites, so remote management from the data center becomes the norm. Encrypting data on these servers helps against theft or accidental loss of data, and today's encryption solutions have even broader capabilities. Imagine only delivering encryption keys to remote data during office hours, ensuring that the data is completely unusable to anyone once the lights go out.

With the centralized key management capabilities of HyTrust DataControl, your IT staff can be confident that remote servers are protected and no-one in the remote offices can control access to encryption keys.

### 10. Secure Outsourcing, Licensing...

The flexibility of virtual machines has opened up a new world to many organizations. Instead of shipping software packages, why not just ship the virtual machine? After all, it's just a set of files and the ease by which it can be spun up reduces the complexity of support different operating system versions and platforms.

Organizations who are outsourcing application development, maintenance, quality assurance testing, etc. often ship virtual machines. Companies with remote offices are now sending complete VMs to their branch offices or to some business partners. These companies may be shipping their applications as physical or virtual appliances. In both cases, data security is of paramount importance. These VMs may have intellectual property such as test data containing customer information, program source code, or proprietary product, market, or competitive plans.

Software development organizations making their products available as VMs creates a licensing challenge.

In both cases, the important data could be encrypted, the application stack can be configured to meet the security needs of the company shipping the V and by holding keys in their data center, they control access to the data. Imagine if you could just clicking one button to revoke keys allowing you to safely terminate an outsourcing contract or remove access to applications if a customer doesn't renew his/her license? Encryption and strong key management helps you meet these challenges.

Once again, HyTrust DataControl allows you to take advantage of the flexibility of virtualization while staying in control of your data.

## Summary

Good security practice shouldn't happen just because someone tells you to. With a 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, we recommend you start by visiting **www.hytrust.com**.

Contact us for further information at **info@hytrust.com.**