White Paper

# Top 10 Reasons You Need Encryption

ENTRUST

SECURING A WORLD IN MOTION

# Table of contents

# Introduction

When you talk about encryption – especially to someone who isn't a security specialist – you can get a variety of interpretations. To many, encryption is some kind of high-tech secret science used only by government agencies and spies.

But in reality, encryption is everywhere. Businesses and organizations all over the world use it every day to help them achieve the flexibility, compliance, and data privacy required in today's virtualized and cloud-centric business environments.

In this paper, we explore 10 common benefits of encryption and show how Entrust DataControl™ uniquely removes the barriers to adopting an encryption solution. Entrust DataControl is part of a product suite that delivers solutions for data encryption and multi-cloud key management as well as virtual machine and containerized workload security policy compliance. See table on page 14 for details.

# 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. Entrust DataControl ensures data is encrypted in transit 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 virtual machines (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 (CSP) own the keys?

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 SLAs? The answer is likely "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 CSP to another. If you have encrypted your VMs with Entrust DataControl, then it's straightforward: You shut down your VM and move it to the new provider, then instruct the system to rekey with a new key. You can then 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 be 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. Entrust 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

If the service provider has both your encrypted data and your encryption keys, in theory, they could have access to your data. The rule of thumb that you should never store your keys alongside 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.

Some organizations, however, 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 disaster recovery. 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?

Having a third party host 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 Entrust DataControl it's a win-win situation. You use Entrust DataControl with one service provider, who then holds your data, but doesn't hold your keys. And you install an Entrust Key Management Server (delivered with DataControl) 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-premises computers of your own.

# 5. Encryption helps you meet regulations

For years, the Payment Card Industry (PCI) has had strict guidelines to ensure protection of cardholder data. We all use credit cards and understandably want assurance that our information is safe. Naturally, encryption has become a major piece of the PCI Data Security Standard (PCI DSS). But over the last few years, an evolving understanding of protected consumer data has necessitated broader use of encryption.

Driven by the global adoption of consumer privacy acts such as the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA), the need for many businesses to protect their customer information has grown exponentially. According to a 2021 Global Encryption Trends Study by the Ponemon Institute, 42% of organizations now consider customer data encryption one of their top business priorities.

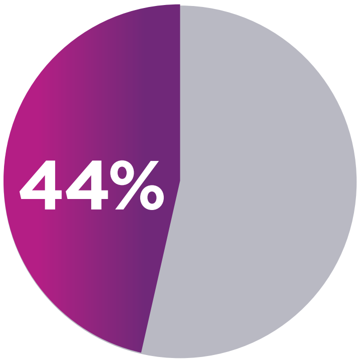
Although not all standards mandate encryption, it's highly recommended. Given the high cost of breach notification and the fact that data loss prevention (DLP) technology is always revealing sensitive data in places you wouldn't have thought, doesn't encryption just make sense? After all, we wouldn't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

## CUSTOMER PRIVACY REGULATIONS

- General Data Protection Regulation (GDPR)
- California Consumer Privacy Act (CCPA)
- HIPAA/HITECH
- Gramm-Leach-Bliley Act (GLBA)
- Sarbanes-Oxley Act (SOX)
- Basel II Accord
- Euro SOX
- 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)
- JAct on the Protection of Personal Information (APPI) of 2003
- Many more

# 6. Encryption gives you a safe harbor from breach notification

In the U.S. there are data breach notification laws in all 50 states and most U.S. territories.[1] According to the IBM Security Cost of a Data Breach Report in 2021, the average cost to an organization for a data breach now stands at $4.24 million globally. The U.S. had the most costly data breaches at $9.05 million per incident, followed by Middle East ($6.93M) and Canada ($5.4M).[2] These costs come from detection and escalation efforts, lost business, notification costs, and post-response activities.



**of breaches include customer PII**

In Europe, where the General Data Protection Regulation (GDPR) is in place, organizations can face severe fines for data breaches. For especially severe violations, the GDPR fine framework can be up to 20 million euros, or up to 4% of the organization's total global revenue.

In most cases, if a data breach occurs and personally identifiable information (PII) is lost, the breached party must notify all individuals who are impacted. However, 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. Similarly, in the EU, organizations can reduce the probability of a data breach – and thus reduce the risk of fines in the future – if they adopt state-of-the-art methods such as encryption as specified in the GDPR regulations. Security officers may reference information security standards like ISO/IEC 27001 or other equivalent national IT-security guidelines to determine qualified methods.

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

[1] https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
[2] https://www.ibm.com/security/data-breach

# 7. Encryption gives service providers a competitive edge

If you are 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:

- Differentiate yourself and gain a competitive advantage
- 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 deprovision securely without leaving data behind

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

# 8. Encryption gives you confidence your data is safe in a multi-cloud world

In February 2021, Kroger Co. reported that a third-party data breach at Accellion, a cloud solutions company, had allowed hackers to access human records data and pharmacy records. The records that were accessed included names, email addresses, phone numbers, Social Security numbers, and even private medical information.

In January 2020, more than 280 million Microsoft customer records were left unprotected and exposed on the web due to misconfigured Azure security rules that Microsoft had deployed a month earlier.

These are not isolated incidents. A simple Google search will reveal many more examples of breaches that exposed PII in public and private clouds. In all these cases, we only hear about them because the data wasn't adequately protected or encrypted.

Now imagine you have data spanning multiple clouds and applications. How can you possibly implement and manage native data protection solutions and encryption keys for each solution independently? Using Entrust DataControl to encrypt data consistently across cloud platforms and Entrust KeyControl, Entrust's Key Management Server product, to manage your enterprise encryption keys, multi-cloud encryption strategies are much easier to execute than you think!

# 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 Entrust 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 and 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 for 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 these scenarios, the important data could be encrypted; the application stack can be configured to meet the security needs of the company shipping the VM; and, by holding keys in their data center, they control access to the data. Imagine if you could just click one button to revoke keys – allowing you to safely terminate an outsourcing contract or remove access to applications if a customer doesn't renew their license? Encryption and strong key management helps you meet these challenges.

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

# Conclusion

Good security practice shouldn't happen just because someone tells you to. With a rock-solid, enterprise-grade encryption and key management system – such as Entrust DataControl – security can become an enabler. You can virtualize your mission-critical applications. You can move to the public cloud.

Entrust DataControl is part of a product suite that delivers solutions for data encryption and multi-cloud key management as well as virtual machine and containerized workload security policy compliance. See chart below for details.

**Entrust Cloud Security, Encryption, and Key Management Products**

| ENTRUST PRODUCT | DESCRIPTION | LICENSING/DEPLOYMENT |
|---|---|---|
| **KeyControl** | Enterprise encryption key management for KMIP-enabled workloads | Licensed standalone or can be deployed with KeyControl BYOK and/or DataControl |
| **KeyControl BYOK** | For generating and bringing your own cryptographic keys to AWS, Microsoft Azure, or Google Cloud platform | Licensed standalone or can be deployed with KeyControl and/or DataControl |
| **DataControl** | For fine-grained, agents-based control and encryption key management of virtual machines in multi-cloud environments | Licensed standalone or can be deployed with KeyControl and/or KeyControl BYOK |
| **CloudControl** | For automated workload security policy enforcement and compliance in virtualized and containerized environments protecting sensitive data against misconfigurations in the cloud | |

Learn more about cloud security, encryption, and key management at: entrust.com/digital-security/cloud-security-encryption-key-management

For more information

**888.690.2424**
**+1 952 933 1223**
**sales@entrust.com**
**entrust.com**

## ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments, and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

**Learn more at**
**entrust.com**

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
**info@entrust.com** entrust.com/contact