White Paper

Top 10 Encryption Myths

Remove barriers to adopting an encryption solution

ENTRUST

SECURING A WORLD IN MOTION

Table of contents

INTRODUCTION

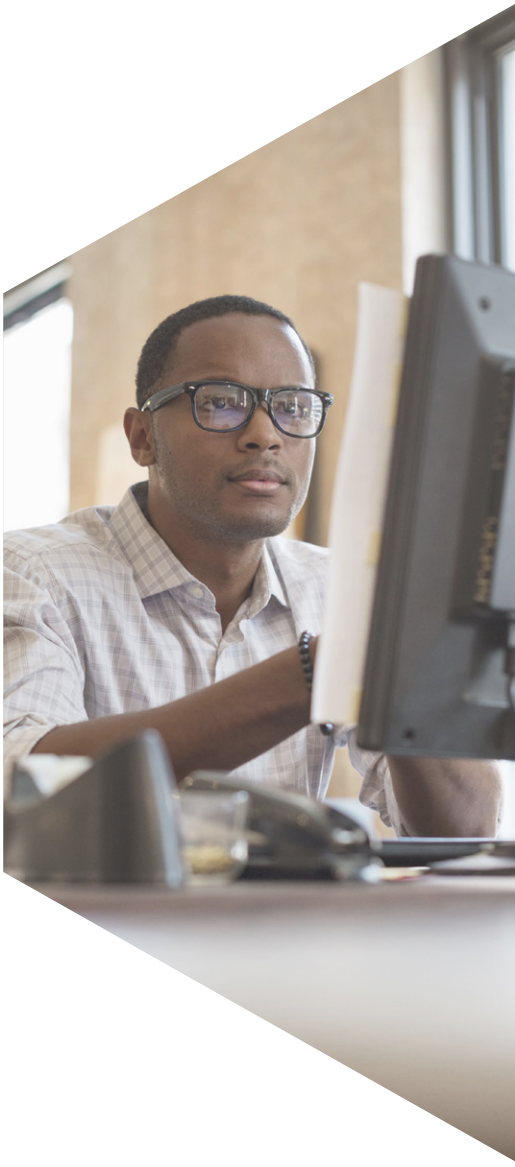
Erasing poor perceptions

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 used only by government agencies with three-letter acronyms – a complex, scary beast that can be tamed only 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 in achieving the flexibility, compliance, and data privacy that is required in today's business environments. In a world that's increasingly built around virtualization and the 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 ten common myths regarding encryption and show you how Entrust DataControl uniquely removes the barriers to adopting an encryption solution.

Myth #1 – Encryption will degrade my system performance



It is true that encryption has a cost, but there are many factors that affect total system performance. This is why most servers are not run at capacity – to ensure that spikes in activity don't cripple the applications that run on them. In fact, applications such as databases and all the major operating systems have been tuned for decades to provide optimal performance by minimizing the amount of time spent going to disk. As long as encryption is implemented correctly, the overhead can be minimal.

Most hardware is now built to help specifically with encryption processing. Most mid- and high-end Intel and AMD processors on the market today support AES-XTS, running AES encryption in hardware to improve performance 8-10 times over encryption done in software. Fortunately, the presence of AES-NI has now become the norm in x86-style processors. This also has the added benefit of offloading encryption from the general CPU processing, freeing up even more CPU capability for applications. Even if AES-NI is not present, as we continue to deploy virtualization on systems with ever-faster commodity processors, the cost of extra CPU, especially in the cloud, is minor and can easily and cost-effectively improve encryption performance.

At Entrust, not only do we automatically detect and use AES-NI for encryption at hardware speeds, we also optimize encryption by performing that processing at precisely the place where the system's normal I/O and memory operations are already happening. In our experience, encryption overhead is minimal and often undetectable because of these benefits. Other throughput constraints in the network or non-optimal storage system configuration are most often the cause of any delays. These are where external bottlenecks typically appear and are not as a result of encryption overhead. This is especially true in virtualized environments.

Myth #2 – Encryption terminology is too hard to understand

AES, Blowfish, Symmetric key, 3DES, NIST key states, KMIP ... there are a lot of buzzwords around encryption and key management. The mathematics of encryption algorithms are difficult to understand, not to mention learning attack vectors like “man in the middle”, spoofing, and many others.

Poor encryption solutions can leave you exposed if they require your staff to understand too many mechanics. You should be able to make simple choices such as:

- I want these new VMs encrypted, and at the end of the year, I don’t want them to run anymore.
- I want to encrypt my data in Amazon, Savvis, and Rackspace. I want to be able to decommission them securely when I choose.

With Entrust, you can make these choices. We’ve engineered Entrust DataControl to defend against the various types of attacks, so you can be confident your data is safe. And there’s no need to be a key management guru. You never see any encryption keys, and the only choices you need to make are simple policy decisions on what you want encrypted and when you want the keys to expire. We support only AES, the strong encryption algorithm recommended by NIST.

Myth #3 – Managing all those encryption keys is a nightmare

There are many encryption solutions in use today, and many of them simply do not address key management effectively. Using password protection for a key that encrypts data on a mobile device, notebook, or desktop is fine; however, this does not scale well when dealing with tens, hundreds, or thousands of encrypted devices. It is also not a good solution when one or two administrators are the only people who have access to the passwords or the keys. What happens if they leave the company? Do you know where all your keys are? Can you get them back?

To summarize the problem as seen by many, cryptography expert Bruce Schneier wrote in the preface to his book "Practical Cryptography":

> "Key management is the hardest part of cryptography and often the Achilles' heel of an otherwise secure system."

At Entrust, we layered the system so that you never have to deal with encryption keys, yet we ensure they are kept safe and secure. All you need to do is make sure your KeyControl server is occasionally backed up, just like you would any other data. And Entrust KeyControl functions as a virtual appliance deployable as a highly available, active-active cluster, the gold standard of high-availability. Failure of any physical host or key server will not result in loss of access to keys.

"KEY MANAGEMENT IS THE HARDEST PART OF CRYPTOGRAPHY AND OFTEN THE ACHILLES' HEEL OF AN OTHERWISE SECURE SYSTEM."

Bruce Schneier, "Practical Cryptography"

Myth #4 – It's easy to lose my encryption keys

With encryption, if you lose your encryption keys, you lose access to your data. It is very important that no single person has control of the keys, both for security reasons and because simple human error can result in a very painful situation.

This is why a layered, highly available key management system is so critical. Entrust KeyControl was built by the same team that brought you the VERITAS file system and volume manager and have been building encryption and key management solutions for many years. High availability and zero downtime is in our genes. With our key management cluster, you can have any number of key servers in any physical location.

Our key server backup images are encrypted, and we even provide you with a simple policy option should you want to ensure no single administrator can restore from backup. Further, if you have encrypted VMs in Azure, Google Cloud, or another public/private cloud provider and your keys are stored in your data center, there is no way that the provider can gain access to the keys.

Myth #5 – Encryption is hard to deploy

One of the most successful and widely used deployments of encryption is SSL. We all use SSL on a daily basis as we shop on the web or access online banking and other sites where sensitive data resides. We don't typically hear complaints about the complexity of web access or poor performance. We need our credit card data protected, and the networks have been built to accommodate this.

At Entrust, we strive to make the deployment of encryption as simple as possible. Do you have some VMs you want to encrypt?

- **First,** install Entrust KeyControl. Point your browser there, and use the default policy or customize with your own policy choices.
- **Next,** install the Entrust DataControl module on any VM you wish to protect.

You can now run that VM in any private data center or public cloud – your data automatically becomes encrypted.

Myth #6 – Encryption secures only the application

We often hear concerns about securing the snapshot and suspending files that are supported by virtualization platforms, because any data that is in the VM's memory is available to VM administrators in clear-text by simply snapshotting the VM.

With Entrust, you can selectively encrypt all or part of the VM, without making any changes to the VM or applications. And we work with all the major hypervisor vendors. Imagine a situation where a PCI auditor requires encryption of the snapshot and suspend files. For this we have Entrust DataControl – Virtual Storage Edition. It acts like a proxy between your storage and the hypervisor. It will encrypt snapshots as well as suspend files and other VM image files on the fly – all under the same Entrust KeyControl policy.

Myth #7 – Rotating encryption keys means application downtime

Key rotation is one of the biggest problems with traditional encryption systems today. Many regulations require periodic key rotation or that you rotate keys if administrators leave the organization. Security best practices also often mandate key rotation. To rotate keys, you need to decrypt the data with key A and then re-encrypt the data with key B. Key A will then no longer be used. Vendors who do support key rotation require that you take your applications offline to rekey. With databases reaching the hundreds of gigabytes or even terabytes, this process can take many hours, if not days.

Entrust DataControl is the only encryption solution that performs key rotation while your applications are still running. When you set your policy, you simply state how frequently you want key rotation to take place. Key rotation starts automatically and when it finishes, a completion message is generated. It is hands-free and done with no application downtime. It's that simple.

Myth #8 – Enterprise-grade encryption is expensive

Basic open-source encryption software like TrueCrypt have downloads in the tens of millions, which certainly speaks to the need for encryption solutions. Enterprise-grade solutions traditionally require hardware-based key management systems, which can cost you tens of thousands of dollars before you secure your first server. As you add servers, costs can skyrocket. As organizations move to virtualization and the cloud to get better scalability and cost savings, they don't want to break the bank just to ensure their data is secure.

Entrust changes this model. We let you implement enterprise-grade security with ease, and we let you get started for free.

Myth #9 – Encryption in the cloud isn't secure

Cloud service providers encrypt their customers' data in the cloud using keys that they keep protected. But this gives you little control. When you hold the keys that protect your data, you are in control.

Entrust DataControl has a range of options, depending on your security requirements. You encrypt your data in the private, hybrid, or public cloud and maintain your own key server. And at all times, you stay in control. Decommissioning from the cloud or switching providers is simple: Click a button and you can ensure that any data left behind is fully encrypted and will never be accessible.

Myth #10 – Encryption solutions don't work across all platforms

Most organizations use hardware and operating systems from multiple vendors. Encryption vendors have typically faced challenges supporting this myriad of platforms. This is even more true for virtualized environments, especially if your organization leverages public cloud, where you have limited control over infrastructure.

Because of its architecture, Entrust DataControl supports the dominant virtualization platforms. We support all hypervisor platforms (VMware, Xen, KVM, Hyper-V) and support encryption within the guest operating system (Windows and Linux) or at the storage layer, offering consistent security and key management as you make the move from private to hybrid to public cloud.

CONCLUSION

Summary

Practicing good security 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 and move to the public cloud. To learn more about cloud security, encryption, and key management, visit https://www.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 and the Hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer.
© 2021 Entrust Corporation. All rights reserved. HS22Q1-dps-top-10-encryption-myths-wp

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