HYTRUST

Data Encryption and Rekeying Made Easy

Sweat-free secrets to performing critical data security functions

White Paper

Table of Contents

HYTRUST

White Paper

Data Encryption and Rekeying Made Easy

Sweat-free secrets to performing critical data security functions

Companies cite budget, performance concerns, and lack of deployment knowledge as the top three barriers to implementing an encryption solution. (Sophos Survey 2016)

Avoiding Encryption and Rekeying Because They are Difficult and Time-consuming to Execute?

Data encryption is fundamental to successful cybersecurity in modern enterprises. And a critical best practice of encryption, as well as a common regulatory compliance requirement, is the rotation of encryption keys on a periodic basis (aka, rekeying). Why? Because it's like changing locks on an apartment between tenants. Rekeying reduces the risk of someone using an old key to break in.

Since rekeying is so important, it raises some critical questions for organizations that want to address cybersecurity threats:

- What are rekeying best practices?
- Why aren't organizations rekeying consistently?
- Why is the process so difficult?

Data Volume Size

The main barrier to implementing encryption is the time it takes to encrypt data due to the volume of data to encrypt. In fact, many databases, for example, are 100s of GBs or TBs in size. As a result, the downtime required for encrypting a running workload can be significant—potentially even taking days! When performing a rekeying operation, the downtime required can be the same as the initial encryption.

For example, the typical steps for both the initial encryption are:

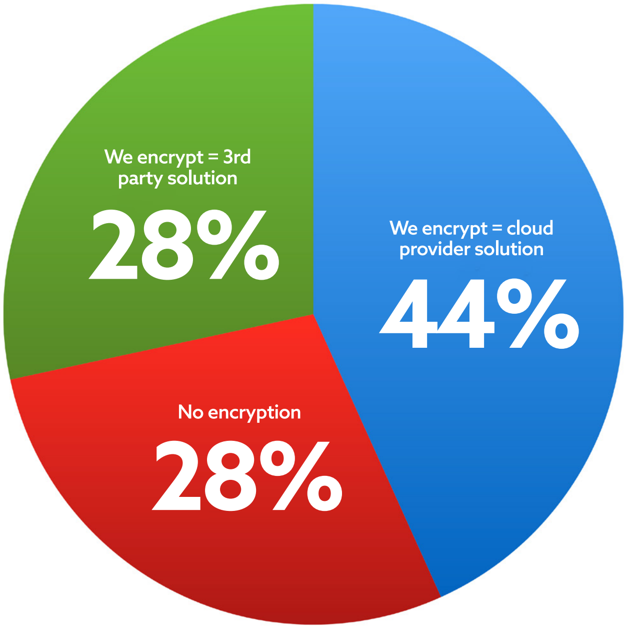
1. Create a symmetric key
2. Start at block zero and repeat for every block in the partition:
    a. Read the block
    b. Encrypt the block with the symmetric key
    c. Write the block back to the partition

Although straightforward, the time-consuming process is one of administrators' most disliked and frustrating aspects of encryption. Even with the performance gains delivered by Intel's AES-NI (hardware acceleration of AES encryption), the time it takes to encrypt can be operationally burdensome.

The Need for Speed

Initial Data Encryption. With HyTrust's advanced data encryption and key management technology—DataControl—the initial encryption can be accomplished without taking the applications offline. Our expertise in this space has been developed through thousands of hours of R&D and hundreds of production deployments since 2011. Further, HyTrust engineers have ensured that encryption can handle a wide range of deployment scenarios to overcome the challenges of multiple cloud deployments.

How are You Handling Encryption in the Public Cloud?



Source: HyTrust 2016 Cloud Adoption Survey

Based on our experience, here are some issues we've observed that must be addressed when performing an initial encryption:

1. **The application continues to use the partition.** I/O performed by the encryption driver must at times be throttled to ensure that it does not impede the application causing the timeouts.
2. **The driver must maintain a window as it moves throughout the partition.** Let's assume that we're halfway through encrypting the partition:
   a. Any I/O the driver sees from the beginning of the partition to the window must be encrypted.

b. Any I/O the driver sees from the window to the end of the partition must not be encrypted, since it will be encrypted later as the window moves through the partition.

c. Any attempt to write into the window must be blocked until the initial encryption process completes and moves the window forward.

d. If the system crashes or reboots in the middle of the initial encryption, the process should be automatically started on reboot so that the applications see no outages.

There are many performance aspects as well to take into consideration when performing an initial encryption. For example, throttling I/O too much could result in making little progress through the partition, thereby, making what could be a long time with offline encryption take many times longer.

Rekeying Process. The rekeying process takes place at a later date to protect against possible exposure of the initial encryption key. In fact, rekeying operations should be performed periodically. To rekey, the HyTrust DataControl solution includes these steps:

- Create a new key, at which time two keys are in play simultaneously.
- As the window moves through the device, the I/O driver is reading or decrypting with the old key and encrypting or writing with the new key.
- This doesn't change the process or alter the overall time considerably, but it's critical to carefully manage both keys so that the process is prepared to handle a system crash or reboot.

There is an additional complication in the rekeying process when a VM is restored from a backup, because the encryption solution needs to know which keys were used for the data when the backup occurred. For example, if encrypted data is rekeyed every six months and then eventually restored from a two-year-old backup, several rekeys have taken place since the original backup. Thus, the encryption driver, in conjunction with the enterprise key management solution, must be able to determine which are the correct keys and execute appropriately.

HyTrust Encryption and Rekeying Solution

HyTrust DataControl abstracts the complexity of encryption and rekeying away from organizations with simple policy and GUI-based actions. In other words, you don't need to be involved in the process.

- Want to encrypt a disk partition? Simply right-click and select "Add and Encrypt." HyTrust DataControl will create the key and encrypt the partition without any downtime or application interruption.
- Want to rekey? Simply set the date or time interval (e.g., six months, one year) and DataControl will perform the rekey without any downtime or application interruption.
- Need an audit trail? HyTrust DataControl provides audit records to show start and completion times for your records—and you don't need to be involved in the process.

> “Role based key management (in the HyTrust DataControl product) actually allows us to place encryption control into our clients’ hands, simplifying our contract and their audits.” [1]
>
> Eric Novikoff, Chief Security Officer, Enki

With HyTrust supporting your encryption operation, you can execute the time-consuming data encryption and rekeying processes automatically and effortlessly. As a result, you’ll elevate your cybersecurity program to new levels of data protection—that meet organizational, compliance, and cloud demands—without breaking a sweat.

[1] - TechValidate TVID: 5F8-42F-649

HyTrust
1975 W. El Camino Real, Suite 203
Mountain View, CA 94040, USA
Phone: 1-844-681-8100
International: 1-650-681-8100