White Paper

Data Encryption and Rekeying Made Easy

Top tips when to performing critical data security functions

ENTRUST

SECURING A WORLD IN MOTION

Table of contents

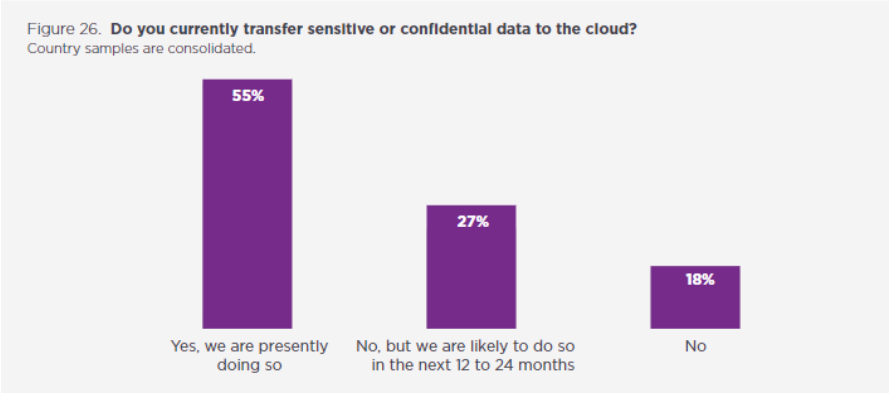
Avoiding encryption and rekeying because they are difficult and time-consuming to execute?

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?

System performance and latency are the most important features of an encryption solution with key management coming 3rd. (Top 5 most important feature of encryption solutions Ponemon Institute 2022 Global Encryption Trends Study)



Data volume size

The main barrier to implementing encryption is the time it takes to encrypt data due to the volume. In fact, many databases are hundreds 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 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 modern day processors use of AES-NI (hardware acceleration of AES encryption), the time it takes to encrypt can be operationally burdensome.

The need for speed

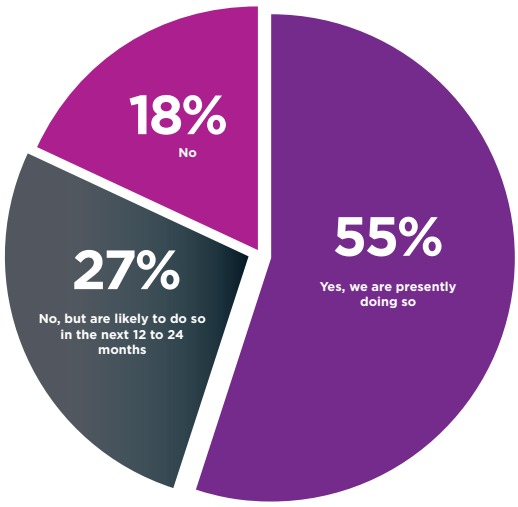
With Entrust's advanced data encryption and key management technology, DataControl, the initial encryption can be accomplished without taking the applications offline. Our expertise in this space has been developed through thousands of hours of R&D and countless production deployments. Further, Entrust 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?

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.

Do you currently transfer sensitive or confidential data to the cloud?



Source: Ponemon Institute 2022 Global Encryption Trends Study

There are many performance aspects to take into consideration as well 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 Entrust 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.

Entrust DataControl encryption and rekeying solution

Entrust 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." Entrust 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?** Entrust 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 ENTRUST 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

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

Summary

With Entrust 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 – meeting organizational, compliance, and cloud demands with ease.

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**