WHITE PAPER

DELL EMC XTREMIO X2 DATA AT REST ENCRYPTION

Abstract

Data at Rest Encryption is a mandatory requirement in various industries that host private or sensitive data. This white paper introduces XtremIO Data at Rest Encryption and explains how it handles the challenges of protecting data, without impacting performance or other services that are provided by the XtremIO All-Flash Array.

August, 2017

Contents

Executive Summary

Information security is a key area of focus for many IT managers. Knowing that data centers are secure against unauthorized access is of critical importance. Yet, how is it possible to secure information on the SSDs in an array when they are easily removable from the system (by design for serviceability)?

Data at Rest Encryption (DARE) provides a solution to securing critical data, even when the media is removed from the array. XtremIO arrays utilize a high performance inline encryption technique to ensure that all data stored on the array is unusable if the SSD media is removed. This prevents unauthorized access in the event of theft or loss during transport, and makes it possible to return/replace failed components containing sensitive data.

DARE is a mandatory requirement that has been established in several industries, such as health care (where patient records must be kept closely-guarded), banking (where financial data safety is extremely important), and in many government institutions.

This white paper focuses on DARE and the way it is implemented in the XtremIO All-Flash Array. It describes the technology behind the XtremIO encryption solution and how the architecture combines encryption with XtremIO's unique data protection and Inline Data Reduction technologies without undergoing any performance penalty. It also discusses key management and key rollover functions that enhance the data at rest protection.

Architecture

At the heart of XtremIO's DARE solution lays the use of Self-Encrypting Drive (SED) technology. An SED has dedicated hardware which is used to encrypt and decrypt data as it is written to or read from SSDs. Offloading the encryption task to the SSDs enables XtremIO to maintain the same software architecture whenever encryption is enabled or disabled on the array. All of XtremIO's features and services, including Inline Data Reduction, XtremIO Data Protection (XDP), thin provisioning and XtremIO Virtual Copies are available on an encrypted cluster (as well as on non-encrypted clusters).

A unique Data Encryption Key (DEK) is created during the drive manufacturing process. The key does not leave the drive at any time. It is possible to erase the DEK or change it, but this causes the data on the drive to become unreadable and no option is provided to retrieve the DEK. To ensure that only authorized hosts can access the data on the SED, the DEK is protected by an Authentication Key (AK). Without this key, the DEK is encrypted and cannot be used to encrypt or decrypt data.

SEDs are shipped out of the factory in an unlocked state, meaning that any host can access the drive data. In unlocked drives, the data is always encrypted, but the DEK is always decrypted and no authentication is required.

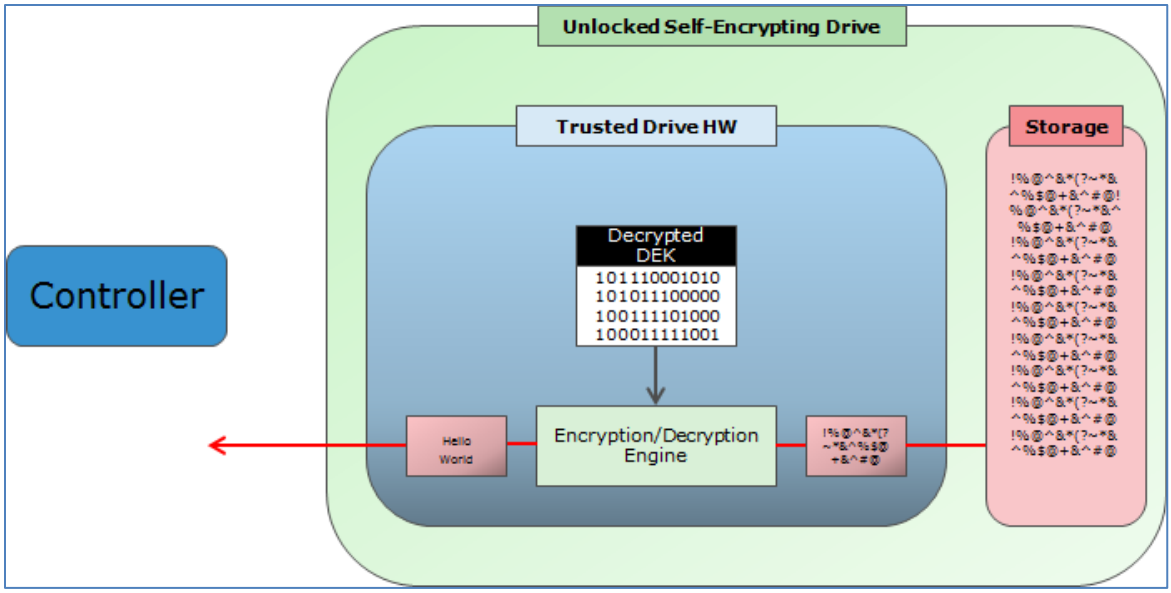

Figure 1. Unlocked SED

Locking the drive is made possible by changing the default drive's AK to a new, private AK and changing the SED settings so that it remains locked after a boot or power fail (such as when an SSD is taken out of the array). When an SSD is taken out of the array, it is turned off and will require the AK upon booting up. Without the correct AK, the data on the SSD is unreadable.

To access the data, the Storage Controllers must provide the correct AK, a term that is sometimes referred to as "acquiring" or "taking ownership" of the drive, which unlocks the DEK and enables data access.

Drive acquisition is achieved only upon boot, and the SED remains unlocked for as long as the array is up. Since data passes through the encryption or decryption hardware in all cases, there is no performance impact when locking an SED.

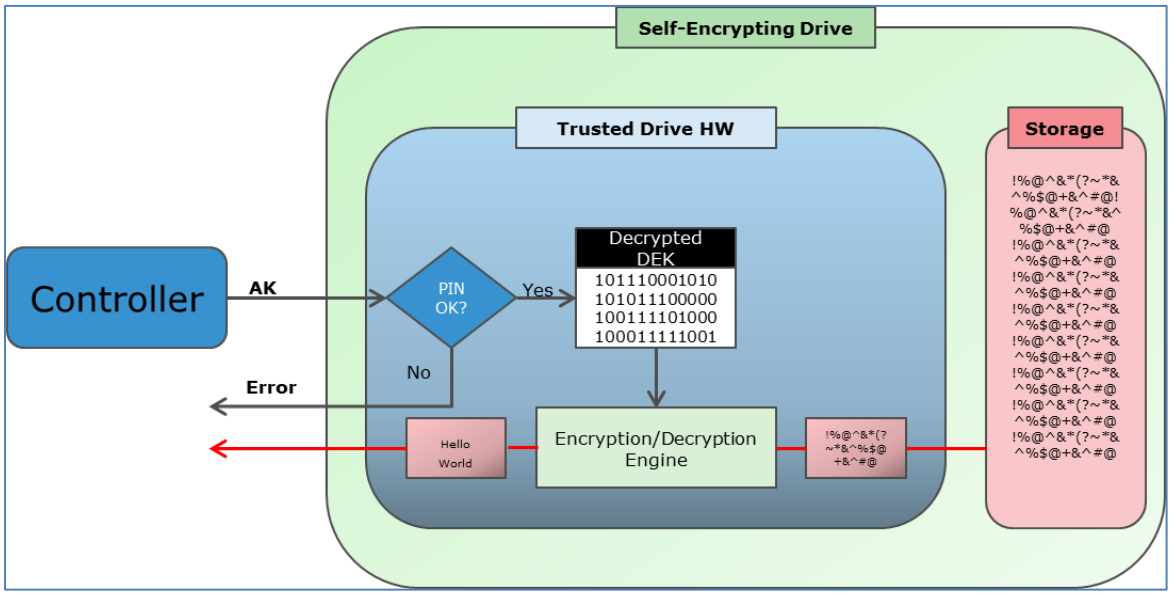

Figure 2. SED Operation Mode

The XtremIO All-Flash Array encrypts data on the Data SSDs, where all user data is stored.

Self-Encrypting Drives (SEDs)

XtremIO encryption capable All-Flash Arrays have always used SEDs. Enabling encryption simply means that the SSDs are now locked with an auto-generated Personal Identification Number (PIN). This is the main reason why there is no performance overhead for encrypting data on XtremIO.

SED solutions, based on Trusted Computing Group (TCG) specifications, enable integrated encryption and access control within the drive's protected hardware. The TCG is an international industry standards group that develops specifications amongst its members. Upon completion, the TCG publishes the specifications for use and implementation by the industry. TCG's open standards provide multi-vendor interoperability, allowing application vendors to provide management for multiple SED providers.

Using an SED which is based on TCG specifications ensures that the drive encryption is based on proven standards for data confidentiality, that the drive utilizes optimized hardware components within its electronics, and that it does not rely on XtremIO's Storage Controller processing power. A TCG-certified SED provides better security because encryption is always enabled and transparent to the user, keys for encryption are generated in the drive and never leave the drive, and user-authentication is performed by the drive before it unlocks, independent of the operating system.

Encryption Algorithm

XtremIO SEDs use the Advanced Encryption Standard (AES-XTS) 256 encryption algorithm as per the recommendation of TCG specification. AES-XTS is a widely-used block encryption standard, and is acceptable by the most rigorous regulations and federal governments' standards.

PCI-DSS and Key Management Requirements

The Payment Card Industry (PCI) Data Security Standard (DSS) was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. All companies that transmit, process, or store cardholder data, including Primary Account Numbers (PAN), must comply with the twelve requirements of PCI-DSS. The PCI-DSS Requirement 3 details the card data protection methods, such as encryption, that are critical components of cardholder data protection.

Compliance with the key management controls outlined in Requirement 3 of the PCI-DSS can be time-consuming and expensive. Retailers, payment card transaction processors, hospitality, transportation, government agencies, and other industries that need to protect cardholder data may find substantial benefit from products that are purpose-built to implement the security controls of PCI in a cost-effective manner, without disruption to existing infrastructure or business processes. As such, Dell EMC has taken significant measures to ensure that XtremIO All-Flash Array complies with the applicable guidelines of PCI-DSS outlined in Table 1.

Table 1. PCI-DSS Requirements

Requirement Number	Requirement Details	XtremIO Implementation
3.6.1	Generation of strong cryptographic keys (ensuring that all keys generated to encrypt data meet industry standards of key length, generally a minimum of 128 bits).	Hardware-Based AES 256 encryption algorithm.
3.6.2	Secure cryptographic key distribution (once the keys are generated, they must be securely distributed to the locations required for use and storage).	Data Encryption Key (DEK) never leaves the SSD encryption Hardware. Authentication Keys (AK) are generated on the array and are not distributed externally.
3.6.3	Secure cryptographic key storage (keys must be stored in a secure manner that prevents [and can show evidence of] unauthorized access or change).	DEKs are stored on SSD's hardware. AKs are not stored in plain text and are calculated upon array startup.
3.6.4	Cryptographic key changes for keys that have reached the end of their cryptoperiod.	It is possible to regenerate new AKs for all SSDs to minimize the risk of someone obtaining the encryption keys and using them to decrypt the Data Encryption Key and the data.
3.6.5	Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened, or keys are suspected of being compromised.	Using SED makes the retirement or replacement of old keys transparent to the user. DEK and AK are unique per SSD and are not used when an SSD is pulled out of the array. When a new SSD is inserted into the Array as a replacement, it will have its own DEK and the cluster will generate a new AK for it.
3.6.6	If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key).	No clear-text key is transmitted within the cluster.
3.6.7	Prevention of unauthorized substitution of cryptographic keys (key management processes must be developed and implemented in such a manner as to control and ensure that illegitimate keys are not substituted into the process).	TCG-certified SEDs guaranty that it will not be possible to inject or substitute the Data Encryption Keys. Keys are generated on the SEDs' dedicated hardware and do not leave the SEDs.
3.6.8	Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	Both types of keys used in XtremIO DARE implementation are internal to the array and do not require custodians.

Enabling Encryption

As discussed in this document, drives encrypt data constantly, and enabling encryption simply means that the SSD lock mode changes from "Open" to "Lock on boot", and a new PIN is generated. Nevertheless, to minimize the risk of data corruption, the process is performed while the cluster is in a stopped state.

When the `modify-clusters-configuration encryption-command="switch-mode" encryption-mode="self"` command is initiated, the cluster generates a unique AK per SSD. The AK is created from a secret seed and unique identification of the SSD. Using a secret digest function, it is turned into the SSD's AK. Once the software has the AK, it configures each SSD in the DAE in turn, by setting the new AK, setting the mode to "Lock on boot", and acquiring the SSD, thereby unlocking it and verifying that data can be read from it. Upon success, the software moves to the next SSD. When done, the cluster can be started and IOPS can be resumed. This process is carried out in parallel for each
X-Brick and takes the same time for any size XtremIO cluster. Initial encryption of a cluster takes approximately ten minutes.

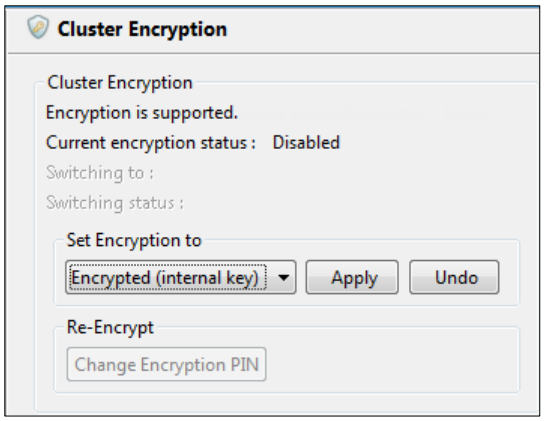

Figure 1. Enabling Encryption

Key Management

As discussed in this document, each SSD has its own AK. The key itself is kept only in memory and is not stored in clear text on SSDs or in logs. The AK seed is stored on the boot SSD's unencrypted partition.

It is possible to change the SSD AK to comply with key rollover requirements. Once the `modify-clusters-configuration encryption-command="re-encrypt" encryption-mode="self"` command is initiated, the software generates new seeds per SSD, and changes the AK on each SSD in turn. Old seeds are kept for as long as the operation continues, ensuring access to SSDs that have not changed yet. When the process is completed, the new AKs are kept in memory and the old AKs' seeds are retired. This process is carried out in parallel for each X-Brick and takes the same time for any size XtremIO cluster. Changing the cluster's AK takes less than a minute.

Disabling Encryption

It is possible to disable the encryption on an encrypted cluster if the customer wishes to do so. Disabling encryption is performed with the cluster in a stopped state. Once the `modify-clusters-configuration encryption-command="re-encrypt" encryption-mode="disabled"` command is initiated, the software changes the configuration of each SSD to "Unlocked" and resets the AK to its original value, as received from the manufacturer. When encryption is disabled, the data on the SED is not protected and can be read by any host.

Conclusion

Data at Rest Encryption is a mandatory requirement in many industries. XtremIO's solution, based on Self-Encrypting Drives (SED), addresses this mandatory requirement without impacting performance or services. Customers can benefit from XtremIO's Inline Data Reduction, high performance, thin provisioning and snapshot capabilities while resting assured that the data on the SSDs is protected from peering eyes.