

Now get Secure and Efficient Storage with Purity EncryptReduce



Update: Pure Storage® has ended support for EncryptReduce capability

Vormetric Transparent Encryption for Efficient Storage is the first and only solution that keeps enterprise customer data protected without negatively impacting flash storage efficiency.

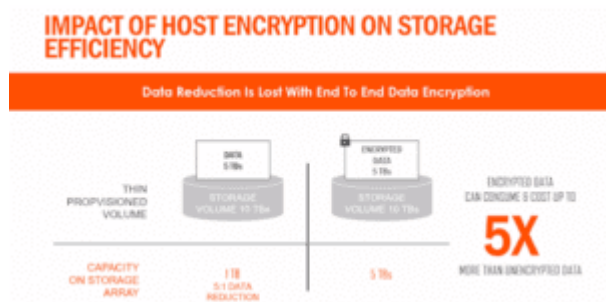
The challenge - in the past, host data encryption has sometimes been a trade-off.

Before I get into the details of our EncryptReduce technology, let's first look at the traditional challenges with respect to storing encrypted data. Well-designed storage solutions typically implement techniques to reduce the amount of data stored on the physical media. This data reduction results in significant cost & maintenance savings for customers in two ways - first, it reduces the total amount of storage capacity required to purchase and second, for flash-based storage solutions, it reduces the number of writes directed to the flash media thereby extending the life of the media.

Pure Storage FlashArray provides always-on deduplication and encryption of data at rest, providing a secure and efficient storage platform trusted by our customers. Some customers have additionally decided to encrypt data at the host level, which has traditionally proved a challenge to storage-level deduplication such as that provided by FlashArray.

Pure Storage FlashArray provides always-on deduplication and encryption of data at rest, providing a

secure and efficient storage platform trusted by our customers. Some customers have additionally decided to encrypt data at the host level, which has traditionally proved a challenge to storage-level deduplication such as that provided by FlashArray. This is because data reduction technologies rely on identifying repeatable patterns in the data and removing them whereas host-level encryption has the effect of randomizing & scrambling the data that does not leave any repeatable patterns in it, thus preventing efficient storage-level deduplication, thus preventing efficient storage-level deduplication. As a result, one has to trade-off host-level encryption against storage deduplication this requiring the purchase of more storage space against storage deduplication this requiring the purchase of more storage space - not an ideal choice!

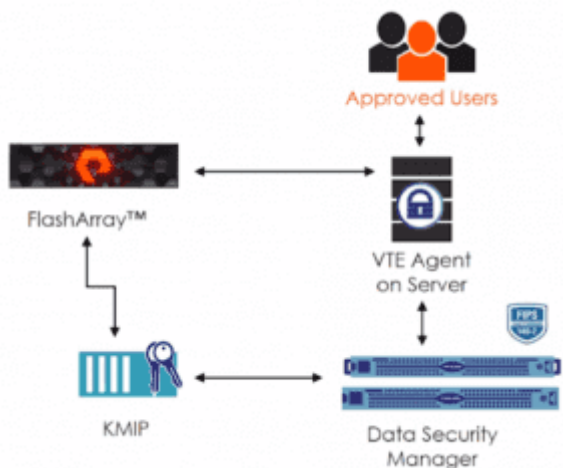


The solution to this problem - Pure Storage EncryptReduce!

In partnership with Thales, Pure Storage has now added EncryptReduce Technology that allows us to maintain storage efficiencies while delivering end-to-end data encryption from the host to our FlashArray.

Let's see how this works.

The solution requires four components to achieve end-to-end data encryption with data reduction.



1. **Pure Storage FlashArray:** With Purity OS and EncryptReduce Technology
2. **Thales Vormetric Transparent Encryption (VTE):** Agent on the host that applies encryption, access control and data audit logging
3. **Thales Data Security Manager (DSM):** Provides information on the keys associated with storage volumes to VTE hosts and storage array systems
4. **KMIP:** Protocol for sharing keys between DSM and Storage Arrays.

Below is an overview of how the four components work together to deliver end-to-end encryption while maintaining storage efficiency.

1. The Vormetric File System agent is installed on the host
2. The host checks out an encryption key from the Vormetric Data Security Manager (DSM)
3. The FlashArray registers as a KMIP client with the DSM and checks out the host encryption key
4. The host writes encrypted data to the FlashArray
5. The FlashArray decrypts the data using the host key, reduces it, and re-encrypts it at the storage level with the FlashArray key before writing it to flash. This step results in achieving the same data reduction & storage efficiency, but with host-level encrypted data which has also been deduped and encrypted at the storage level!
6. When the host reads the data, the FlashArray decrypts the data using the FlashArray key and re-encrypts with the host key prior to sending the data to the host, thus preserving encryption while in transit.

With the above flow, FlashArray with EncryptReduce continues to maintain storage efficiency, preserve data at rest encryption and send back the data to the host in the original secure format.

Here are the results from one of the tests that compare storage efficiency benefits with EncryptReduce Technology

Name	Size	Volumes	Snapshots	Reduction
Encrypted	13 G	5.24 G	0.00	1.0 to 1
Encrypted_with_VTE	13 G	8.29 M	0.00	4.7 to 1
Non-encrypted	13 G	8.29 M	0.00	4.7 to 1

Based on these results, you can see that without host-level encryption our FlashArray achieves 4.7:1 data reduction. If the same data is host-level encrypted and EncryptReduce is disabled, there is zero data reduction but if we enable EncryptReduce for host-level encrypted data the data reduction achieved goes back to 4.7:1 which is identical to the efficiency achieved with host-level unencrypted data. This demonstrates that with Pure Storage EncryptReduce Technology, you do not have to choose between host-level data security and data efficiency anymore. They say you can't have your cake and eat it too. Well, with Pure Storage EncryptReduce, now you can!

Get more technical details on Pure Storage EncryptReduce technology, in this [Technical Brief](#).

Contact your Pure Storage value-added-reseller or account team for additional information.