TECHNICAL BRIEF

Pure EncryptReduce

Get the benefits of full pathway encryption and full data reduction.

One of the best value propositions of Pure Storage® solutions is that we fit a lot of data into small places. To do that we compress, deduplicate, and remove patterns. It can save you a lot of money. But the savings don't stop with fitting data into small places: By reducing the write volume to flash media, we can also extend the life of a flash drive by many times, which means you also gain substantial maintenance savings and reliability.

Why are we repeating the well-known advantages of data reduction? Because you lose the advantages of data reduction when a server writes encrypted data to a Pure Storage FlashArray™.

We have worked around this for some time with our novel approach to data at rest encryption. While all data on the array is encrypted using FIPS 140-2 certified AES256 encryption, you couldn't encrypt the incoming data if you wanted to capitalize on the benefits of data reduction. Until now.

Pure EncryptReduce solves the problem. In partnership with Thales, EncryptReduce enables full inflight encryption from a host over the network to a FlashArray. This provides the following benefits:

- Allows for inflight encryption over the wire
- Allows for the FlashArray to perform its standard data reduction
- Provides physical security through Key Management Interoperability Protocol (KMIP)

The solution requires four components to achieve inflight encryption with data reduction. Thales provides two of the components: the host software Thales Vormetric Transparent Encryption (VTE) and the Thales Data Security Manager (DSM). The other two components are a Pure FlashArray and Purity//FA software (version 5.3 and beyond).

Encrypt inflight

Encrypt inflight data and still have the ability to compress and deduplicate data.

Physical security

EncryptReduce provides physical security through Key Management Interoperability Protocol (KMIP).

Meet standards

All data on the array is encrypted using FIPS 140-2 certified AES256-encryption

The Key Is to Share Keys

The way EncryptReduce works is conceptually simple, although the underlying technology is complex. The Thales DSM sits between the host and FlashArray and retains the key used by the host and the FlashArray. For the FlashArray, you define the DSM as a KMIP resource, then exchange certificates between the FlashArray and the DSM. This process is defined with a known protocol, KMIP, so nothing unusual is happening under the hood. The host also exchanges a key between itself and the DSM. The host and the FlashArray now share the same key and as the host writes data to the FlashArray, we decrypt it in memory and then employ our standard process of data reduction. Taking this approach allows for minimal modification to the FlashArray I/O path. EncryptReduce still preserves the data-at-rest encryption and writes out the reduced data with the AES256 algorithm.

EncryptReduce in Action

Figure 1 shows some volumes on an EncryptReduce-enabled FlashArray. The non-encrypted volume is the same data from another host. We used the Enron Email Corpus, since it is dependably reducible and publicly available for testing and validation.

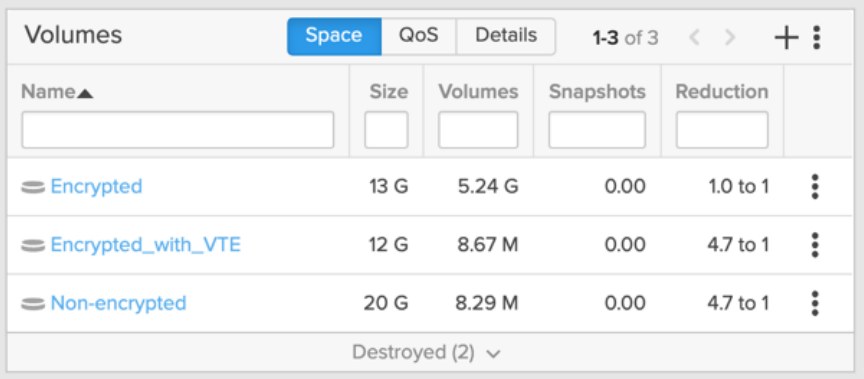

Figure 1. Volumes on an EcryptReduce-enabled FlashArray.

Although the volume names are good enough descriptions, it's important to reiterate that the VTE-encrypted volume benefits from precisely the same data reduction as the non-encrypted volume. There is no difference in how both volumes were reduced.

Pure Storage doesn't believe in the dogma that people must make compromises with useful technology. We don't believe that something on the left needs to be given up in order to gain something on the right. We prove this time and time again with how we operate with the Pure Storage Evergreen™ subscription model, all-inclusive licensing, and non-disruptive hardware and software feature upgrades. We're bringing this approach to the realm of total data center security as well. You can encrypt inflight data and still have the ability to put lots of data into small places. The combination of Purity EncryptReduce and our partner Thales makes it possible.

ps EncryptReduce_technical-brief