

# Will the PoPI Act and GDPR see your storage costs triple?

 By [Hayden Sadler](#)

20 Nov 2018

Data privacy and security is a major focus for businesses, particularly with the imminent rollout of the Protection of Personal Information (PoPI) Act in South Africa and the recent implementation of General Data Protection Regulation (GDPR) in the European Union.

This came to the fore recently when a local company – a firm that offers financial services across Africa - experienced a data breach. They were the first company in South Africa to publicly admit the infringement on GDPR, a regulation that the PoPI Act was based on.

The breach resulted in a wake-up call for South African organisations to protect and secure their company and clients' data. However, based on regulations, a key component to solving this problem lies in the effective encryption of data.



Hayden Sadler is country manager for Infinidat in South Africa

Unfortunately, many businesses have invested in technologies that may result in their storage costs increasing at least threefold when attempting to encrypt data at an application level. This is due to the fact that current storage-based data

compression and deduplication technologies cannot perform data reduction when data has been encrypted at the application level.

## How does encryption fit into protecting your data?

Encryption ensures that data is secure. It may sound simple yet data must be encrypted at the application level, when at rest (when the data is digitally stored for example on a disk and inactive) and in flight (when data is transferred to another storage medium such as the cloud), in order to secure the data from an end-to-end perspective and not just at the 'source.' Although many companies may find this a tedious exercise, as each regulation is implemented and data breaches increase, encryption is increasingly important and necessary.



### Don't make your data compliance pop - make it POPIA

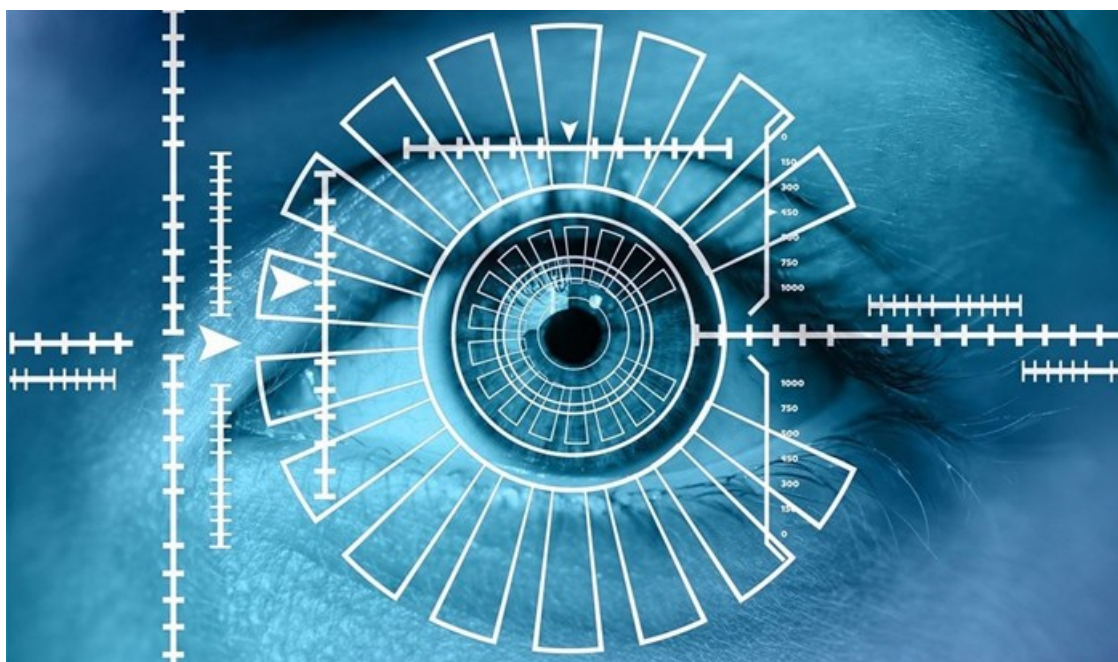
Daniel Lotter 17 Oct 2018



Companies that have invested in All-Flash Array (AFA) storage, may find themselves paying more than they had bargained for. To explain, AFA, is an already costly storage system that comprises only flash media rather than traditional disk drives, providing high performance, but relying heavily on data reduction to be cost-effective. However, AFA is incapable of cost-effectively encrypting data. This is due to the need for more flash capacity when data is encrypted, resulting in an increase in the cost per gigabyte of data stored.

## As data breaches increase so does the need for a 'new' strategy

As data breaches continually increase, companies need to realise that they are happening at all levels of the IT stack. These breaches are occurring from user level compromises via email attacks, to data corruption and theft on the storage array where data lives, to theft of data that is transported across unencrypted networks.



Source: [pixabay.com](https://pixabay.com)

Encrypting data at the storage layer (at rest) has always been the strategy, as storage arrays can encrypt the data instantly without any performance penalty. Yet this does not protect data in flight. If data is encrypted anywhere else, the AFA's can't perform data reduction and the entire economics of AFA's collapses. This will result in enterprises - especially those that have invested in AFA - having to completely rethink their storage strategies.

## Is there another option other than AFA?

The answer may lie in a return to intelligent software-defined storage. There are platforms that are faster than all-flash, deliver reliability, scale to multiple petabytes and feature a low Total Cost of Ownership (TCO). With storage like this, it means that AFA no longer has to be considered above all other storage options for the organisation.



### British Airways highlights need for GDPR compliance

Gary Allemann 7 Nov 2018



However, other than having the correct offering, vendors and resellers need to realign with the realities of digital threats today. The requirements of regulations such as PoPI and GDPR will disrupt this market segment significantly. For enterprises that deal with massive amounts of data - and this is not a small challenge – it's imperative to resolve storage and encryption challenges to avoid putting customers' data at risk and potentially tripling the cost of their storage.

Solutions need to be built on sound principles, as we know that constant innovation in a rapidly evolving security threat landscape is critical. Our goal should be to solve the conflicting requirements of bigger, faster, and less expensive storage.

## ABOUT HAYDEN SADLER

Country Manager - South Africa at Infinidat

- A new tiered approach is needed to secure data collected from IoT devices - 13 May 2021
- Paying less and paying later for data storage is key for businesses - 15 Apr 2021
- Data storage partnerships are crucial going forward - 25 Jun 2020
- Your data storage could be costing you customers - 27 Jun 2019
- Less green through more data protection? - 11 Apr 2019

[View my profile and articles...](#)

For more, visit: <https://www.bizcommunity.com>