Data Security for an "All Flash" Storage World

Ashvin Kamaraju

Global Vice President,Engineering,
Thales e-Security

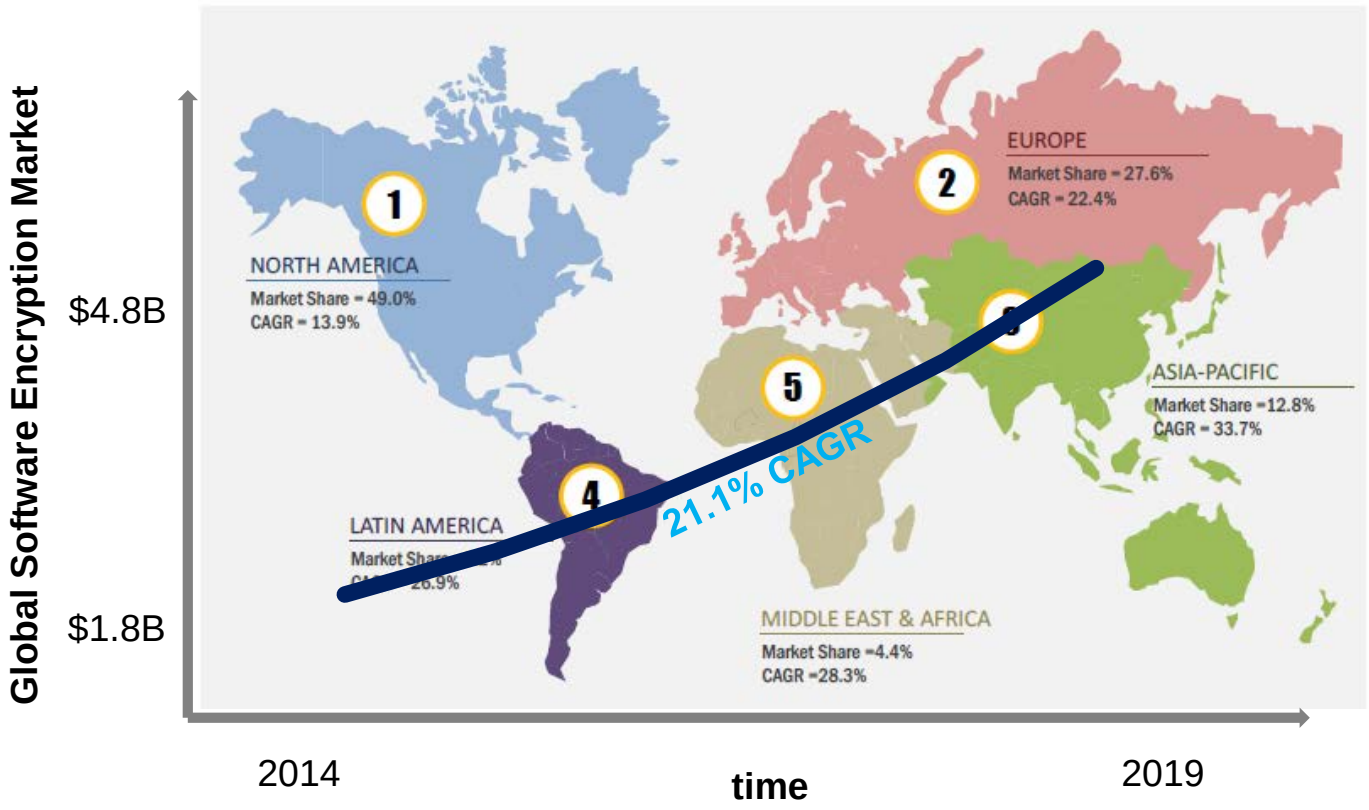
Abstract

Cyber attacks continue to grow more sophisticated and persistent. To combat threats and keep data safe IT teams have to employ robust encryption, key management and access controls. This is especially true for information held in storage environments, which can contain an organization's most vital assets.

To secure storage, many organizations have been leveraging native encryption offerings from their storage vendors. The growing trend with "all flash" storage array deployments in enterprises pose particular challenges when encrypted data from host servers have to be stored in these arrays. Flash storage arrays offer high performance and capabilities like compression and de-duplication for storage efficiency. However, flash storage arrays (similar to most storage systems) only provide checkbox encryption that fails to deliver the requisite levels of security.

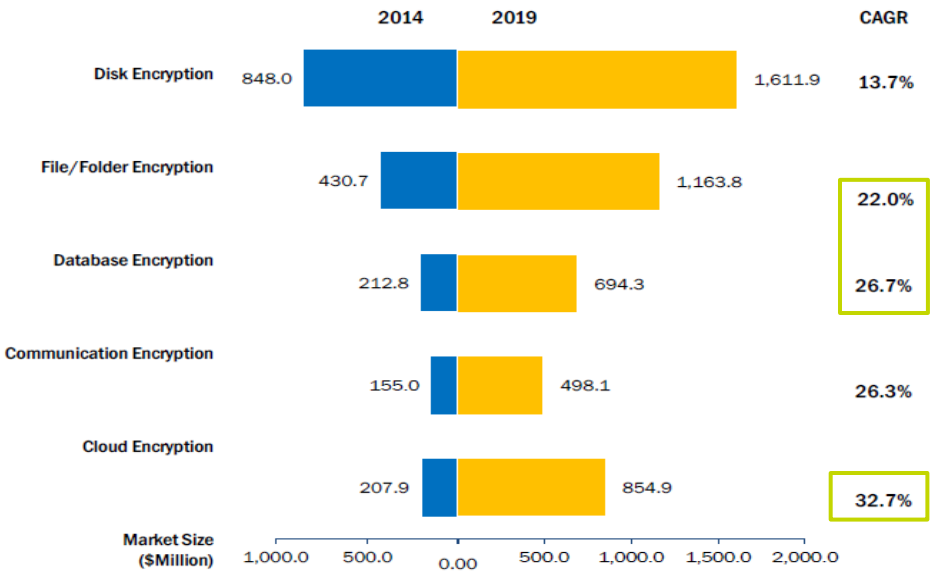
This presentation will offer a look at how storage security demands are evolving and the different approaches that organizations can take to establish strong safeguards, both today and for the long term.

Software Encryption – A Growing Trend



Software Encryption Technologies

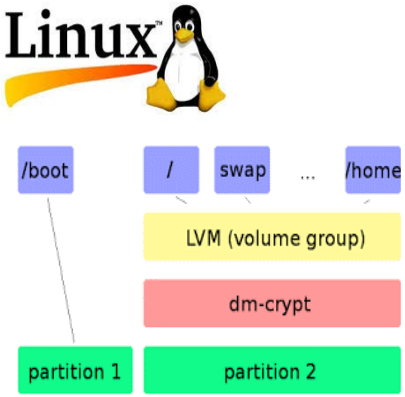
FIGURE 7 GLOBAL ENCRYPTION SOFTWARE MARKET, APPLICATION SNAPSHOT (2014 VS. 2019): MARKET FOR DISK AND FILE/FOLDER ENCRYPTION TO GROW TWO FOLD DURING THE FORECAST PERIOD

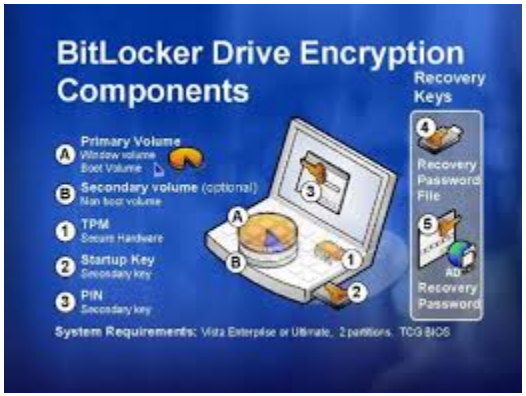


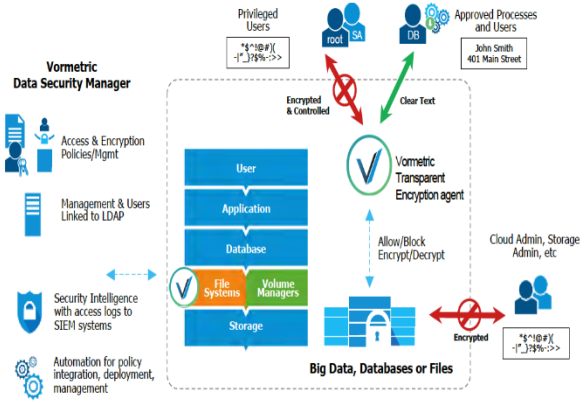
MARKETSANDMARKETS

- Networked disk storage market (NAS Combined with non-mainframe SAN) $20+ billion in 2014 (IDC)
- Disk Encryption includes end-point

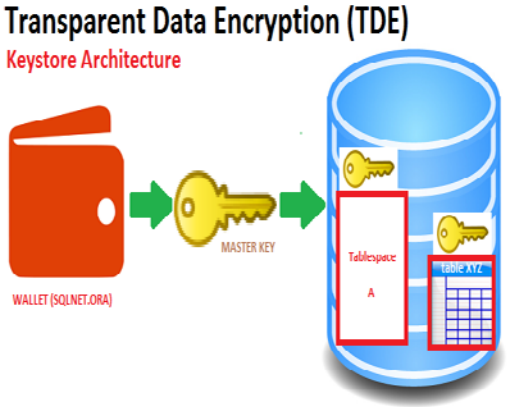
Many Enterprise Applications Offer Encryption

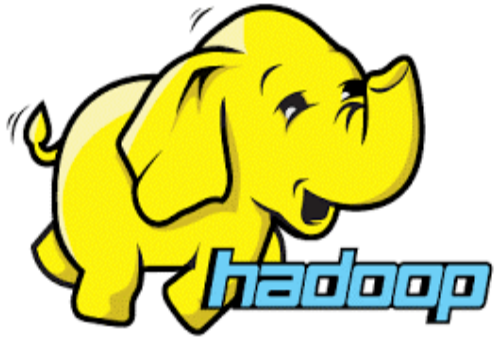




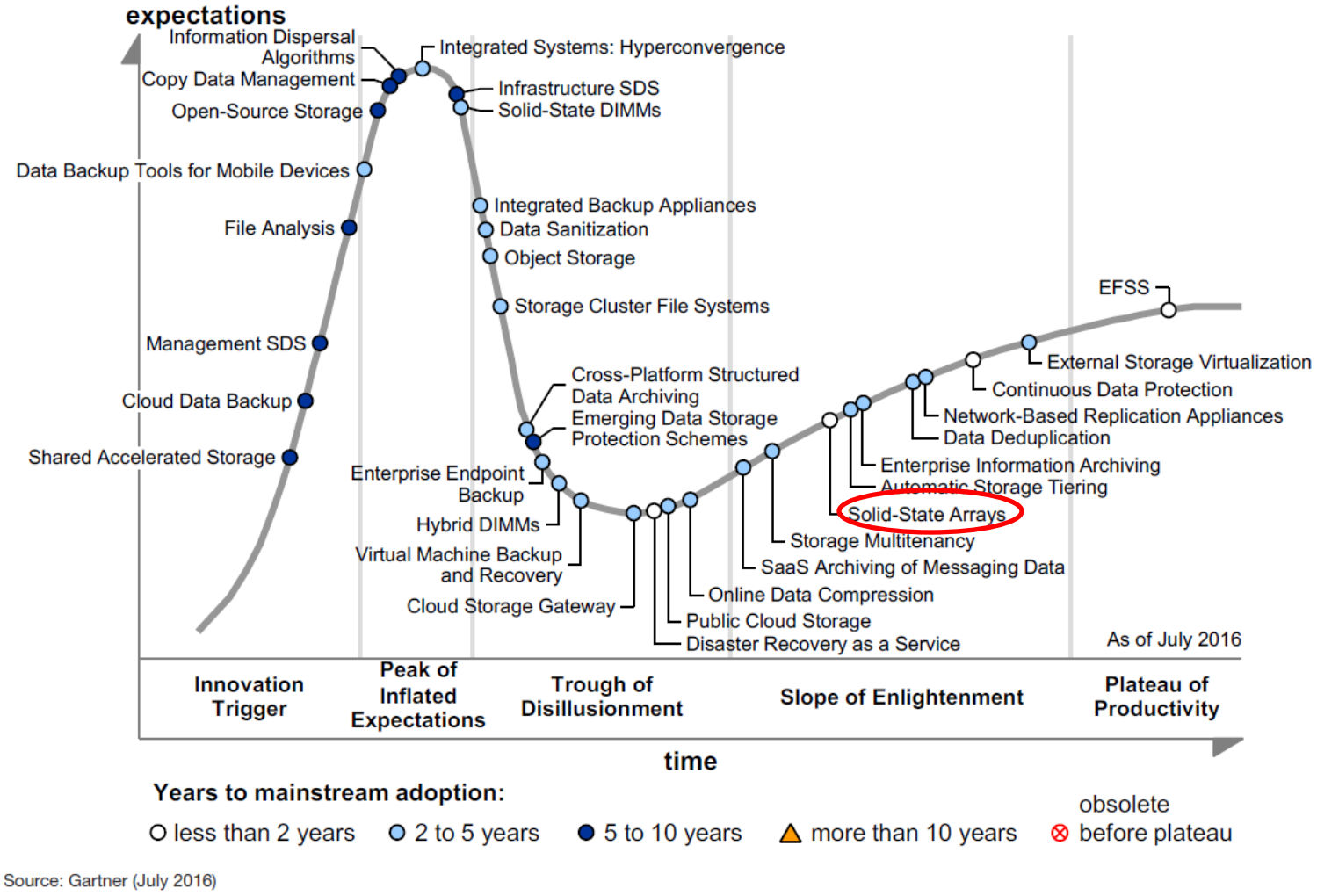


Sample Vormetric Transparent Encryption deployment architecture.





Storage Trends - 2016



Source: Gartner (July 2016)

Storage Vendor Encryption is Inadequate for Data Centers

DATA STORAGE SECURITY SUMMIT

Technologies

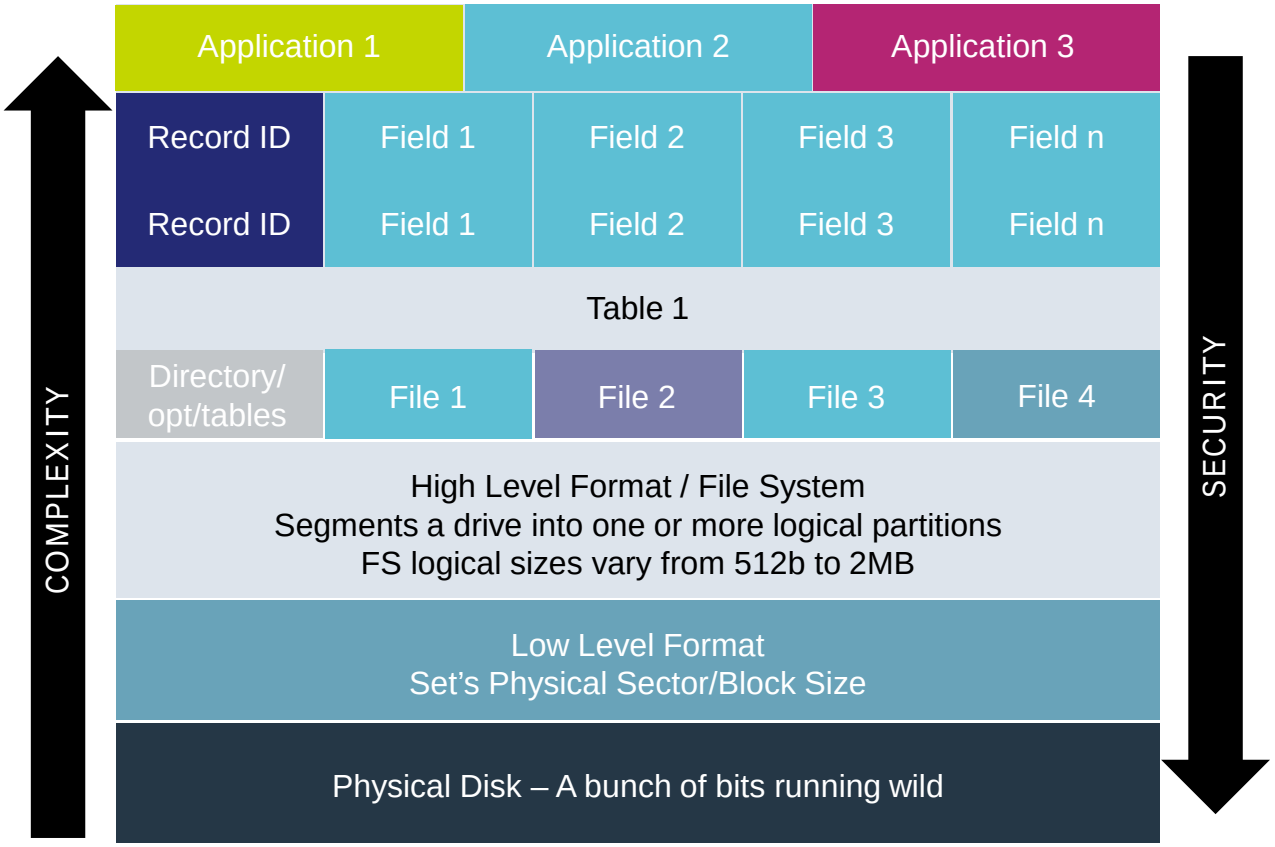
- Software Solutions
- Appliances
- Tape Drives
- Self-Encrypting Drives
- Native Encryption

Weak Protection

- Only media theft protection
- Checkbox for compliance requirements
- Poor Encryption Key Management

Types of Encryption

Risk Mitigation vs Deployment Complexity



- Application
  - Data specific (PII data)
- Database
  - Column, Record & Field Encryption
- File Encryption
  - Directory or File Groups
- Operating System
  - File System Encryption (FDE)
- Physical Disk
  - Self Encrypting Drive
- Unformatted
  - No cryptography

What is Being Protected?

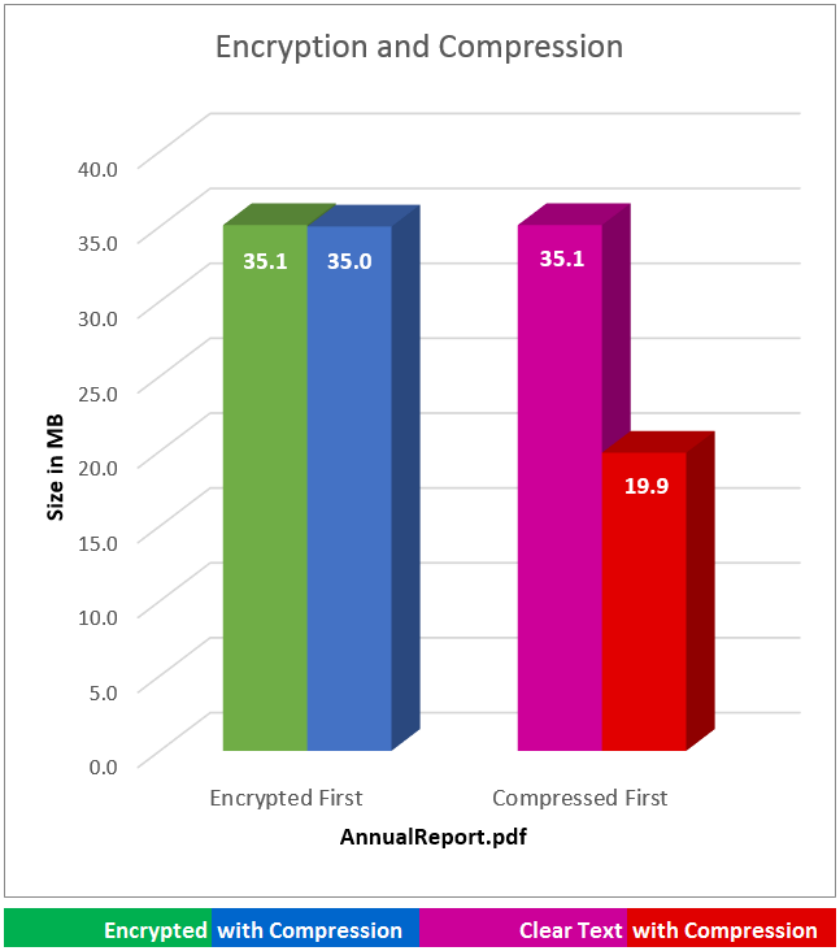
- Data at Rest
  - Encrypting stored data no matter where it sits - disk, tape, static RAM, USB storage, SEDs, etc.
- Data in Motion
  - Encrypting data traversing from point A to point B - Link Encryption
  - Provides protection for data in areas outside your control
  - Data should NEVER leave a controlled environment in the clear
- Data in Use
  - Protects data right up until it is as close to the user as possible - Software versus hardware cryptography
  - Protects data end to end by only exposing components that need exposed - Hardware Security Modules
- How does the encryption system get the Key?
  - Enterprise Key Manager

Encryption with Access Control for Threat Mitigation

- Encryption with access control policies is inherently more secure
- Offers separation of duties – only data user has access to clear data
- Deny access to privileged users (e.g. root user, DBA, system admin)
- Only allow authorized binaries to execute
- Host servers are the only entities that have the context to enforce access controls with encryption

The Big Problem
Storage Efficiency Vs. Data Encryption

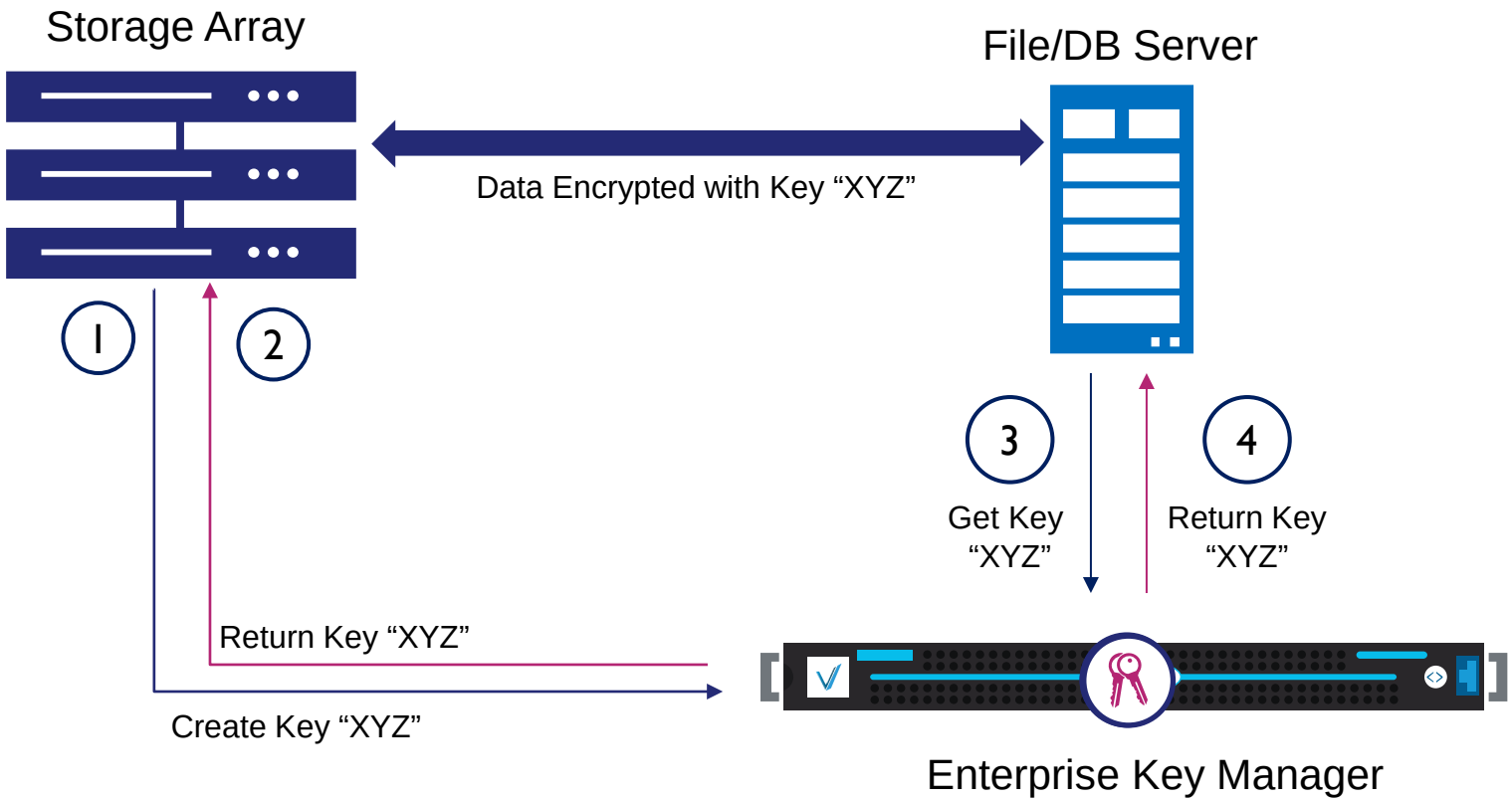
- Storage Arrays use data De-Duplication and Compression technologies to reduce the cost of storage
- Flash Storage Arrays in particular rely on compression to compete on price-performance with traditional disk Storage Arrays
- Encrypted data destroys the compression efficiency



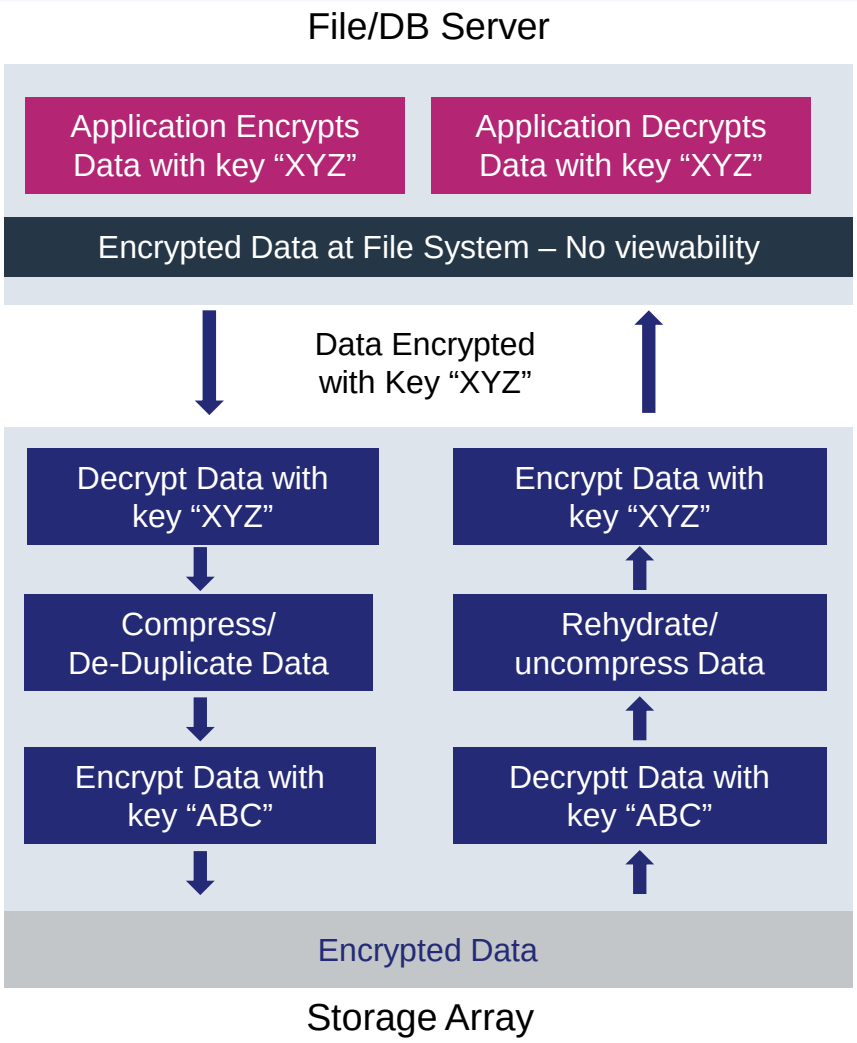
Processing Encrypted Data Streams without Loosing Storage Efficiency

A New Approach

Key Sharing Between a Storage Array and a Host Server



Maintaining Storage Efficiency with Encrypted Data Streams



- Encryption key is shared by the host server and the storage array
- Ensures highest level of data security
- Possible performance penalty in the array can be overcome by leveraging HW crypto acceleration, more processor cores

In Closing….

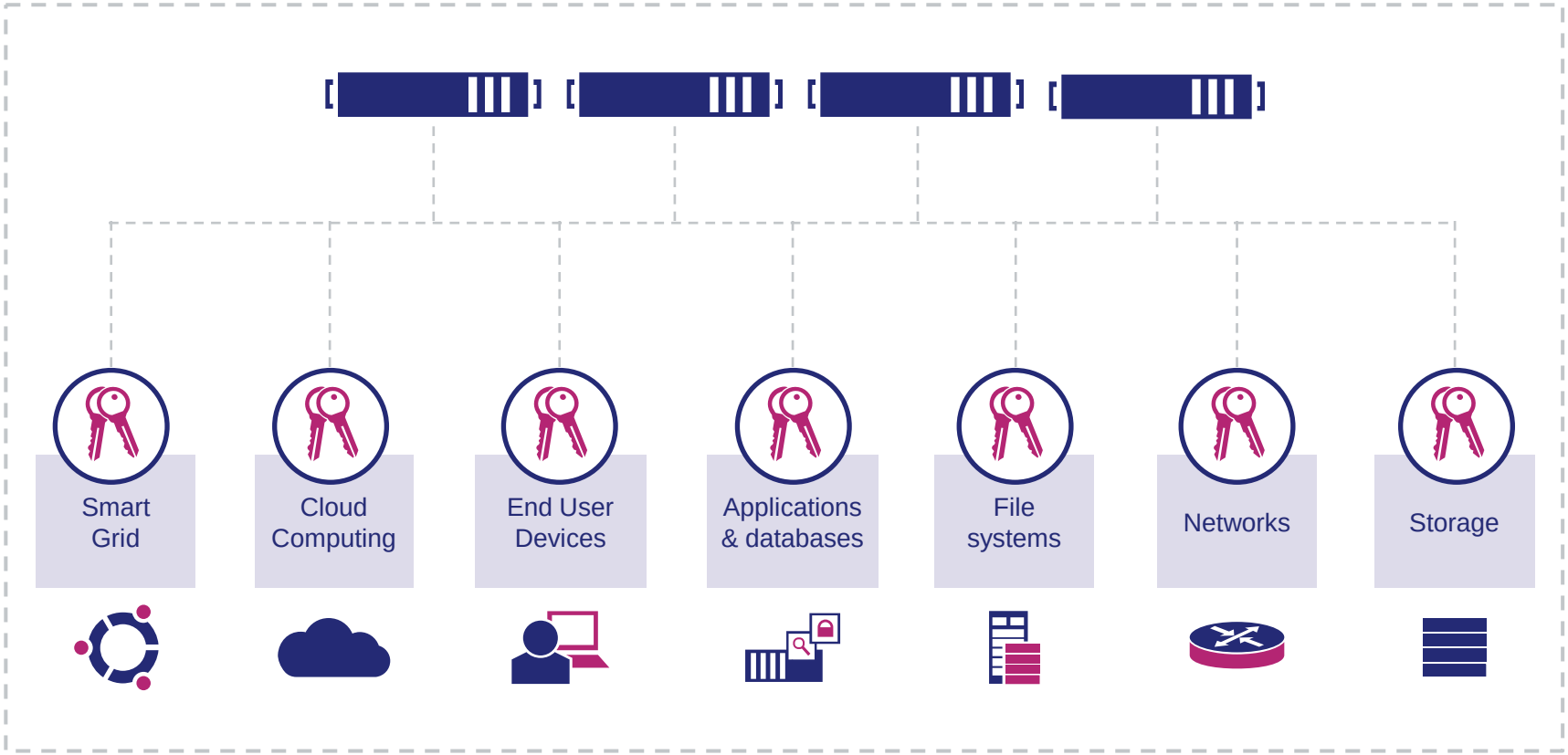
Storage Vendors Must Take Note of Growing Trends in Encryption

- Data at Rest Encryption in an array offers minimal to no data protection
- Data from host servers/applications will be encrypted i.e. storage arrays will receive encrypted data streams
- Most storage arrays do not have robust encryption key management that meets enterprise standards
- Encryption destroys storage efficiency in arrays especially when using compression – a problem that is particularly acute with “all flash” storage arrays

What Storage Vendors Should Do

- Encryption - Use an external key manager and a standards based key management protocol (e.g. KMIP)
- Storage Efficiency – Decrypt the encrypted data streams from the host first and then compress/de-duplicate. Re-encrypt data being read by the host
- Key Sharing – The storage array and host/application share the same encryption key provisioned by an external key manager
- Standards – Influence standards bodies to provide a method/protocol for hosts and arrays to share/associate keys with blocks of data

Enterprise Key Management - The Big Picture



Consolidated Key Management Reduces Costs Through Centralized Operations

Thank you!

Download this presentation and others from SNIA's Data Storage Security Summit at:
http://www.snia.org/dss-summit

Role Based Controls with Enterprise Key Management

Function	Admins	Security Office	Recovery	Application Managers	Auditor
System Configuration	☑				
Add users	☑				
Assign Administrator Role	☑				
Assign Security Related Roles		☑			
Define & Assign Key Groups		☑			
Create & Manage Policies				☑	
Manage Keys		☑ Master Keys		☑ Data Keys	
View Logs (Event, Audit or Group)	☑ Event Logs	☑ System Audit		☑ Application Audit	☑ All Logs
Export Logs					☑
Recover System Key - M of N		☑ Commit Recovery	☑ Recover Shares		
System Backup to NFS server		☑			
System Restore from NFS server	☑	☑			