

Pervasive Guidance

for 2020 Pervasive Encryption Adopters



Bryan Childs
Solution Offering Manager
z/OS Security
bchilds@us.ibm.com

\$3.9M

Average cost of data breach in 2019

&

\$150

cost per record

See the report:

<http://www.ibm.com/security/data-breach>



European Union General Data Protection Regulation (GDPR)



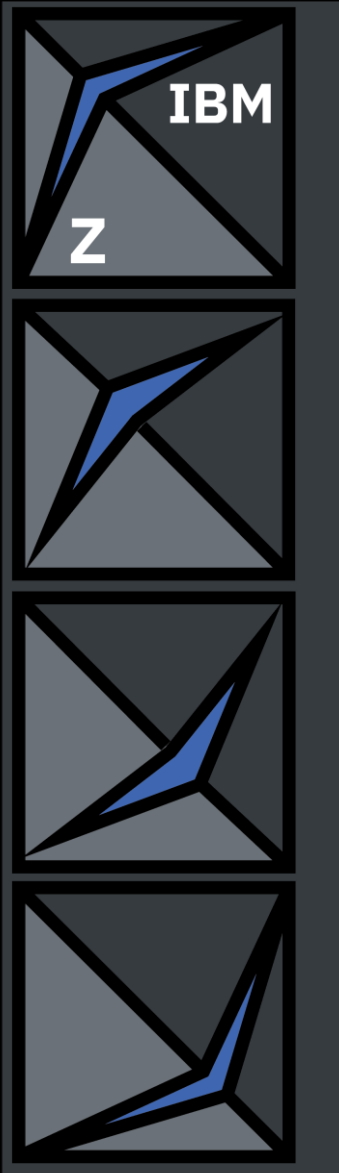
Payment Card Industry Data Security Standard (PCI-DSS)



Health Insurance Portability and Accountability Act (HIPAA)



Use Cases for Cyber Resiliency are called Risks.



ENCRYPT

EVERYTHING

An umbrella of encryption differentiation

- z/OS Data Set Encryption (DSE)
- z/OS Coupling Facility Encryption
- z/OS Network Encryption Analysis
- z/VM File & Network Encryption
- IBM Cloud Hyper Protect Services
- Fibre Channel Endpoint Security*
- and more

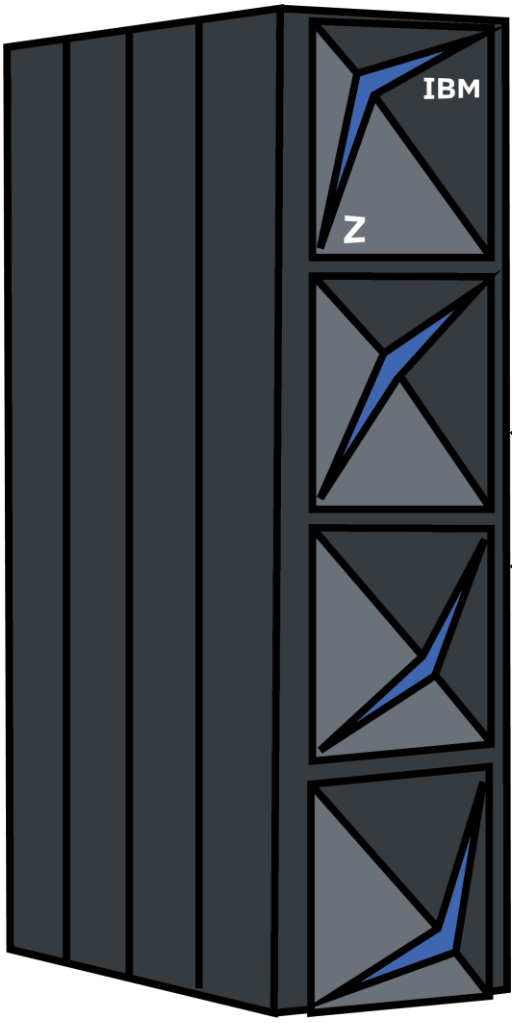
Addressing a critical need in mitigating data breach risk and simplifying audit compliance

*New for the z15 T01 as of 1Q2020

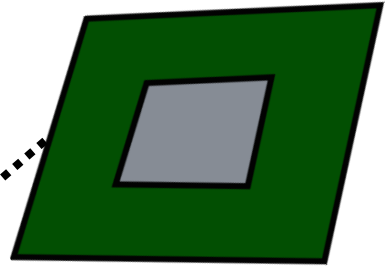


Hardware Designed for Encryption

#trustIBMZ

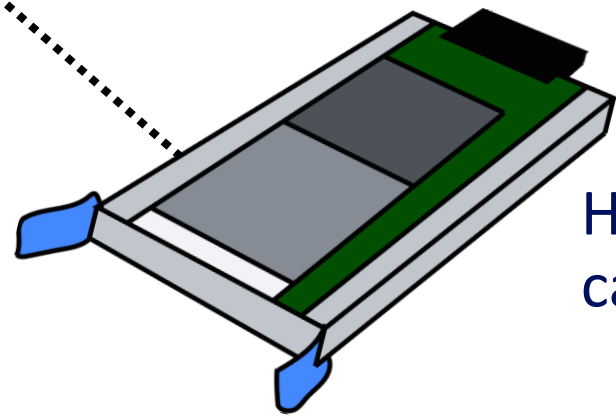


CPACF



High performance symmetric key calculations

Crypto Express 7S



High security key calculations

Simplified & secure Master Key management

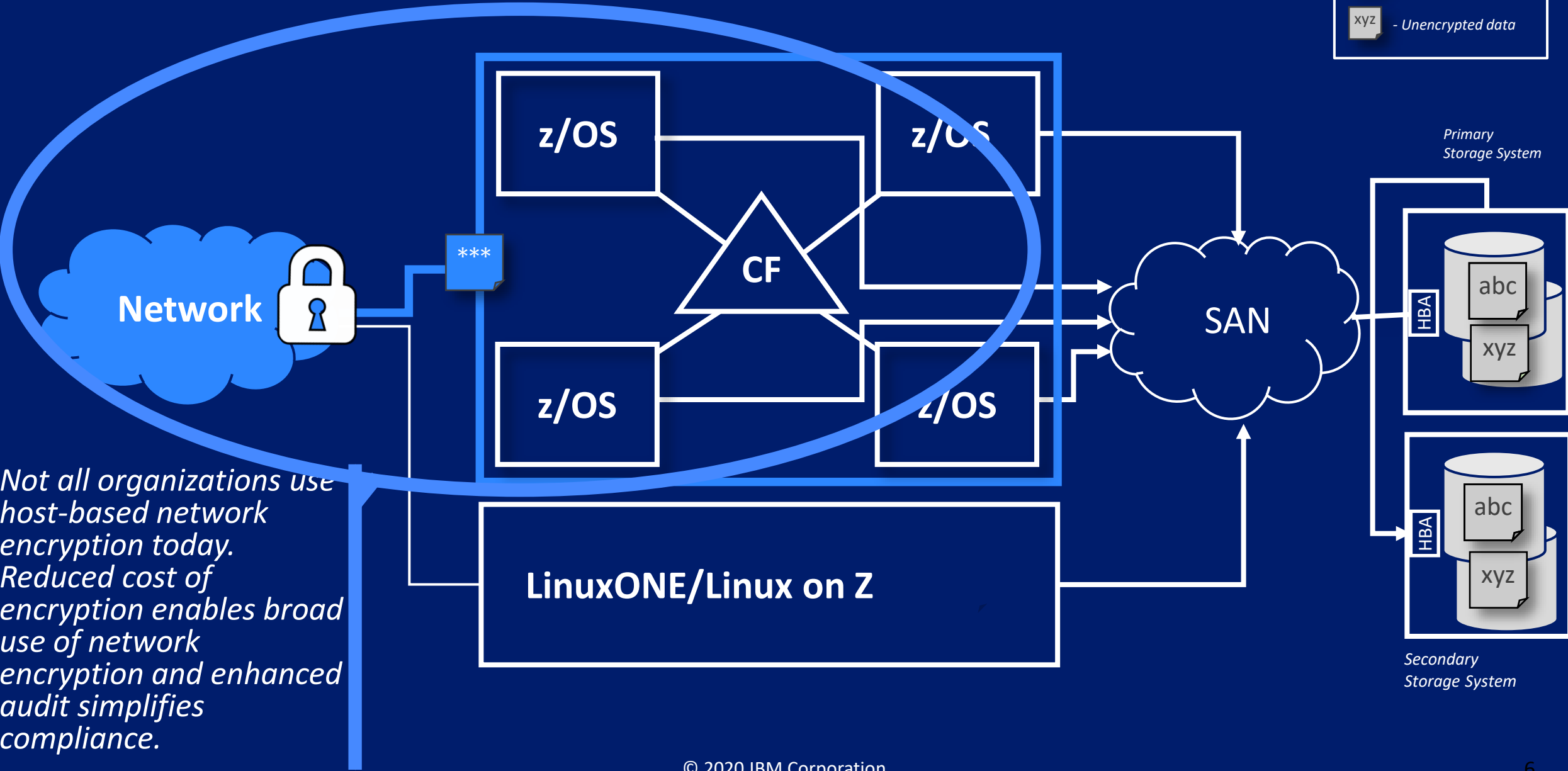
TKE Workstation



Blueprint #1: z/OS Network Encryption

Legend

- *** - Encrypted data
- xyz - Unencrypted data

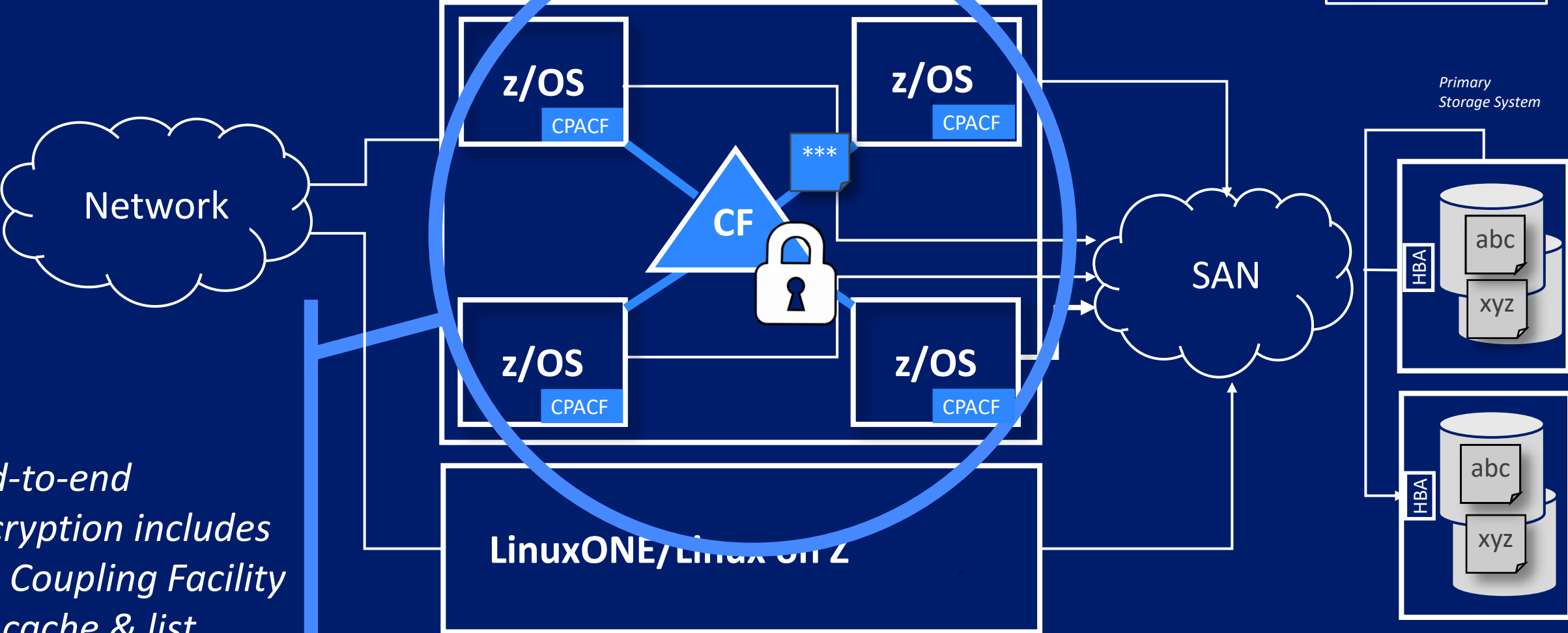


Not all organizations use host-based network encryption today. Reduced cost of encryption enables broad use of network encryption and enhanced audit simplifies compliance.

Blueprint #2: z/OS Coupling Facility Encryption

Legend



- ***** - Encrypted data
- xyz** - Unencrypted data

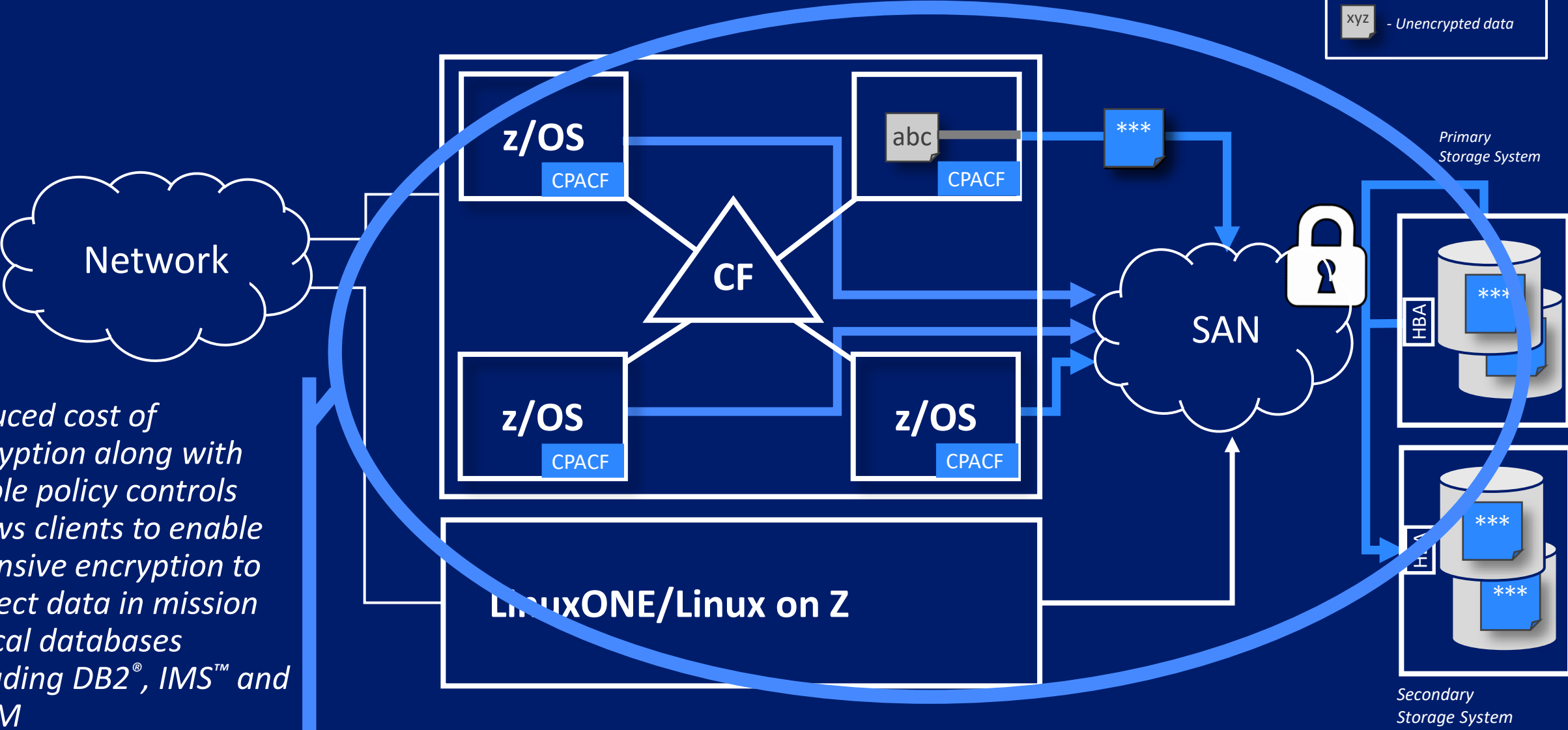


End-to-end encryption includes the Coupling Facility for cache & list structures.

Blueprint #3: Data Set Encryption

Legend

-  - Encrypted data
-  - Unencrypted data

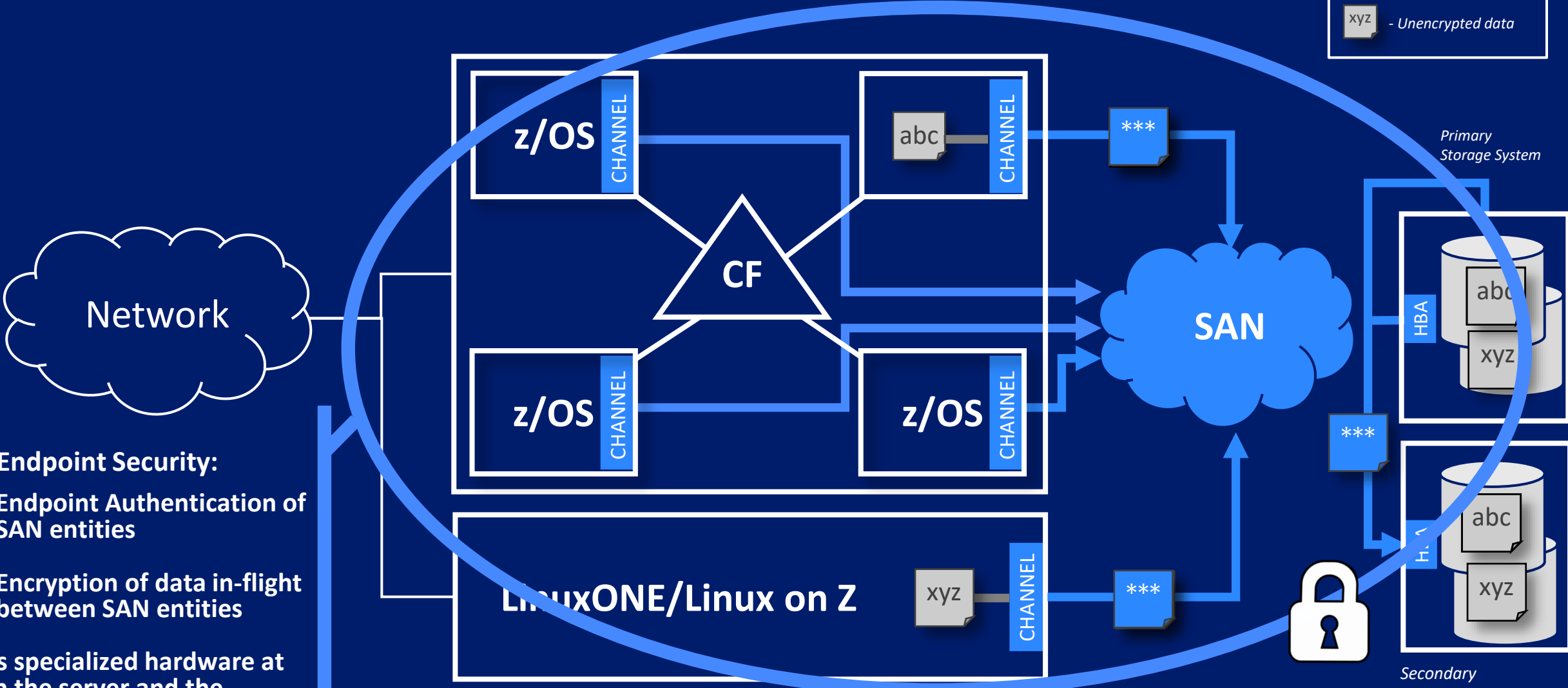


Reduced cost of encryption along with simple policy controls allows clients to enable extensive encryption to protect data in mission critical databases including DB2[®], IMS[™] and VSAM

Blueprint #4: Fibre Channel Endpoint Security

Legend

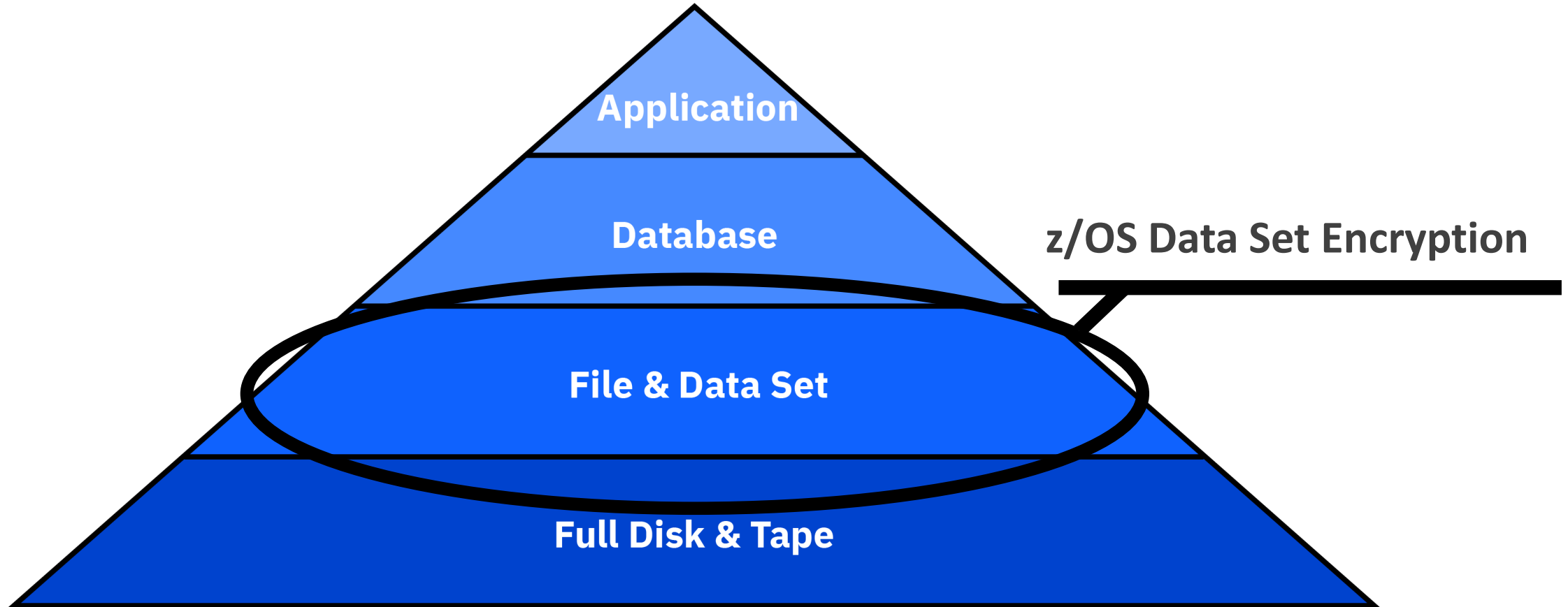
- Encrypted data
- Unencrypted data



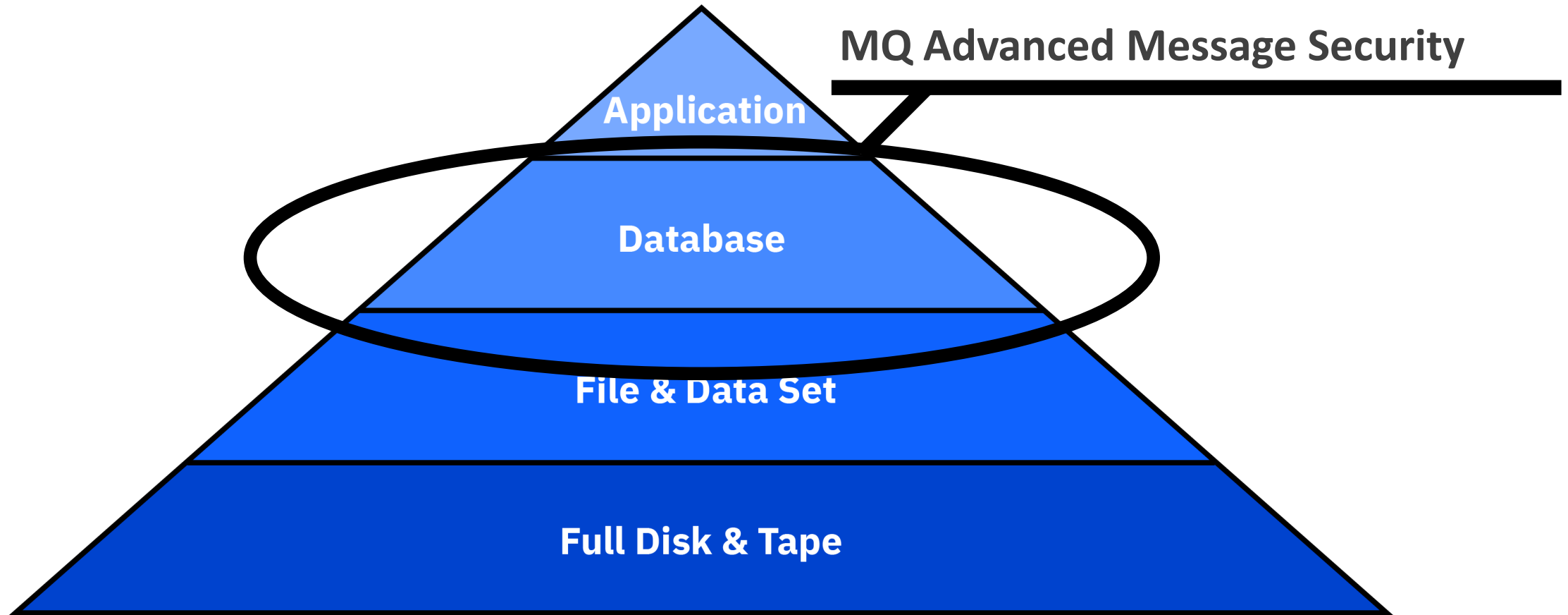
- FC Endpoint Security:**
1. Endpoint Authentication of SAN entities
 2. Encryption of data in-flight between SAN entities

Uses specialized hardware at both the server and the storage device

Cost-Effective Encryption of Data at Rest to satisfy compliance requirements

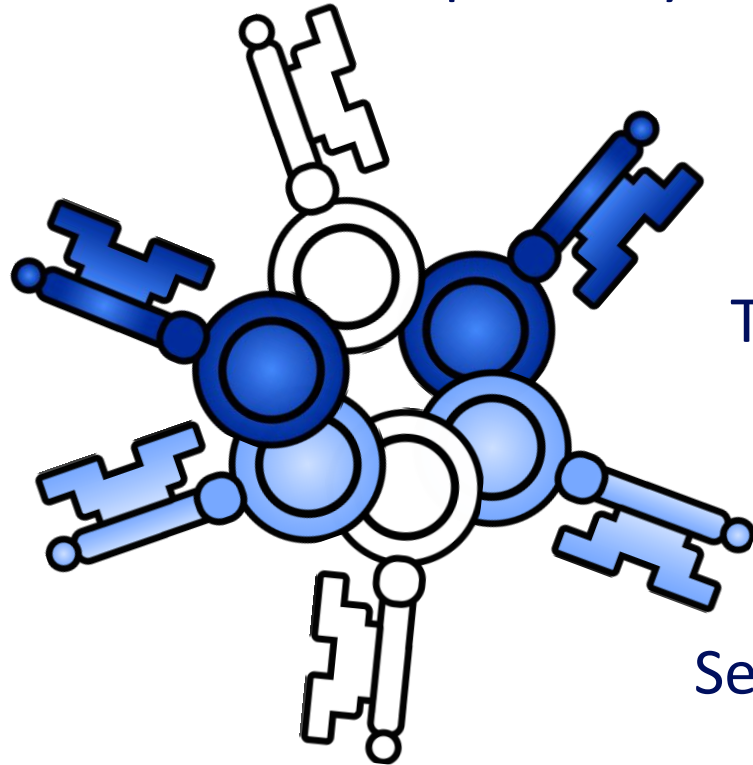


Complementary to Pervasive Encryption



Enterprise Key Management Foundation – Web Edition (EKMF Web)

Operational Keys



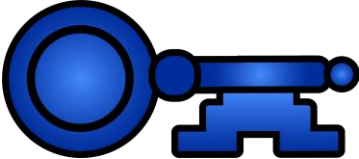
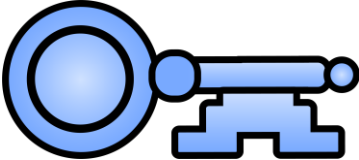
Trusted Key Entry (TKE) Workstation

Master Keys

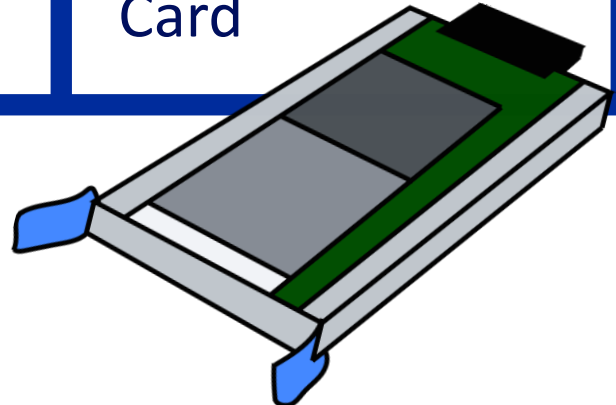
Security Key Lifecycle Manager (SKLM)

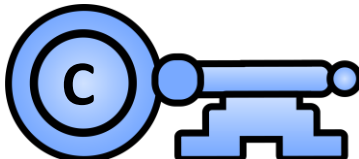
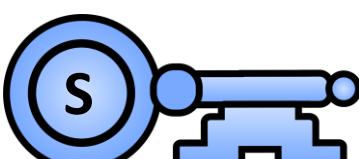
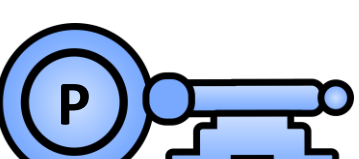
Self-encrypting Device Keys

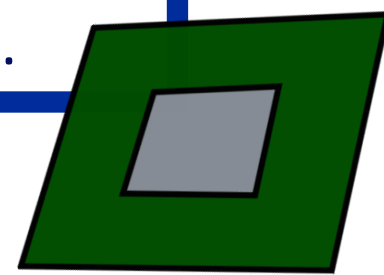




Key Type	Storage Location	Purpose
Operational Key	Key Store	Used to encrypt & decrypt z/OS data sets.
Master Key	Crypto Express Card	Used to encrypt / “wrap” an Operational Key to securely store it.



	Key Type	Location	Purpose
	Clear Key	Host Memory & Key Store	No encryption to protect the key. This is not recommended.
	Secure Key	Host Memory & Key Store	Encrypted with a Master Key to best protect it in the Key Store.
	Protected Key	Host Memory	Encrypted using CPACF wrapping key for hybrid security & performance.



DATASET profiles are denoted for Data Set Encryption by the presence of a **key label** that corresponds to a profile in the **CSFKEYS** class.

DFSMS will respond to the presence of the **key label**, check the user's access to **CSFKEYS**, and interact with ICSF for the associated protected key.

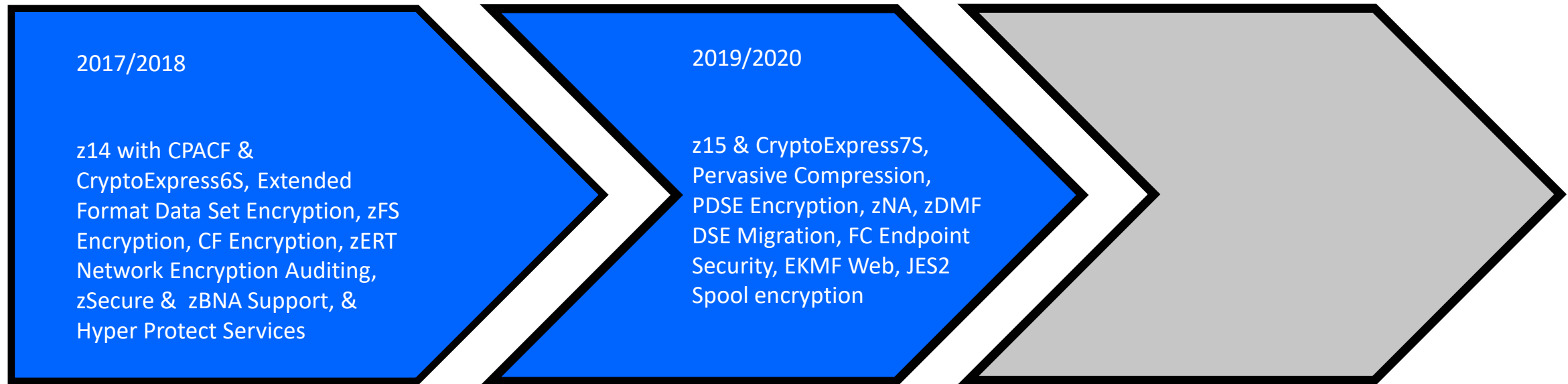


The **CSFKEYS** class controls access to the cryptographic keys in ICSF Key Stores, e.g. the Cryptographic Key Data Set (CKDS).

The **CSFSERV** class controls access to ICSF's cryptographic services & its TSO panel utilities.

The Pervasive Encryption Roadmap

#trustIBMZ



IBM clients leveraging Pervasive Encryption

Financial Services	Credit Card	EU Bank	EU Org
<ul style="list-style-type: none">• Deliver services and solutions to the top mortgage lenders and services in the nation.• Mortgage Servicing Platform on IBM Z automates all areas of loan servicing.• Currently encrypting ~5 million datasets	<ul style="list-style-type: none">• Benchmark for application level encryption solution revealed expected 100% CPU overhead.• Abandoned application encryption and shifted to pervasive encryption to protect all data for critical systems.	<ul style="list-style-type: none">• CIO directive to encrypt all data enterprise-wide in response to GDPR.• Mainframe team deploying IBM Z and Pervasive Encryption to meet CIO directive.• Plan to encrypt all application data (DB2, IMS, CICS/VSAM, batch, etc...)	<ul style="list-style-type: none">• Secure confidential tax data exchanges• Existing solution had the Java application running on x86 & SOR on z/OS.• Moving application server to Linux on Z allowed for end to end security of the entire data processing.

Find more content
on Pervasive Encryption at:

<https://www.ibm.com/support/z-content-solutions/pervasive-encryption/>