IBM z14 Pervasive Encryption
An Overview

Dejan Mihajlovic
SW Architect – IBM Austria
dejan_mihajlovic@at.ibm.com

IBM z14

Location: IBM Vienna

Date: 05. Oct. 2017

Data protection and compliance are business imperatives

"It's no longer a matter of if, but when …"

26%

Likelihood of an organization having a data breach in the next 24 months [1]

European Union General Data Protection Regulation (GDPR)

Payment Card Industry Data Security Standard (PCI-DSS)

$4M

Average cost of a data breach in 2016 [2]

Of the **7 Billion** records breached since 2013 only **4%** were encrypted [3]

Health Insurance Portability and Accountability Act (HIPAA)

1, 2 Source: 2016 Ponemon Cost of Data Breach Study: Global Analysis -- http://www.ibm.com/security/data-breach/
3 Source: Breach Level Index -- http://breachlevelindex.com/

Extensive use of encryption is one of the most impactful ways to help reduce the risks and financial losses of a data breach and help meet complex compliance mandates.

However, implementing encryption can be a complex process …

Organizations struggle with questions such as:

1. What data should be encrypted?
2. Where should encryption occur?
3. Who is responsible for encryption?

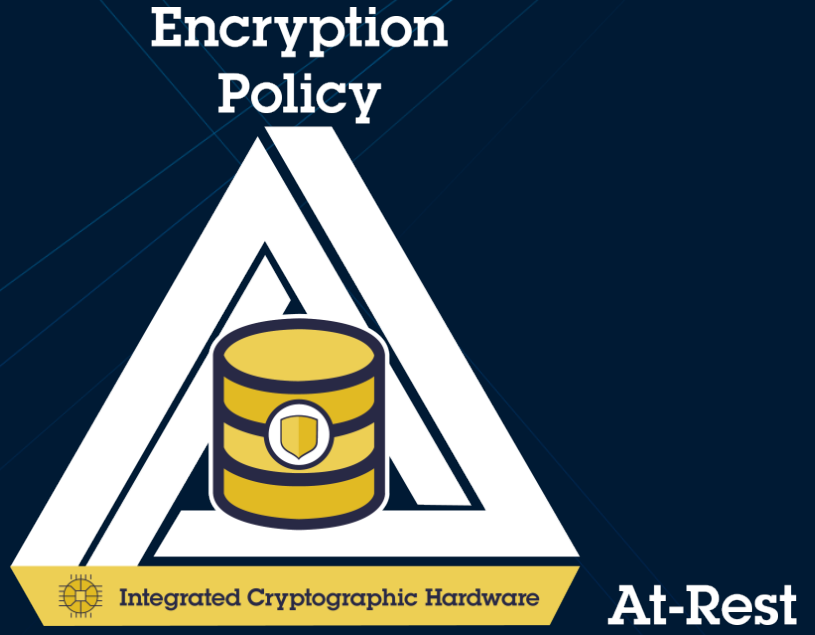
Comprehensive data protection requires a huge investment to deploy point solutions and/or enable encryption directly in the applications.

IBM z Systems Pervasive Encryption

A Data Centric Approach to Information Security

Data is the new perimeter

A transparent and consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify & reduce the costs associated with protecting data & achieving compliance mandates.



zNext

The world's premier system for enabling data as the new perimeter across the value chain.

Pervasive Encryption of sensitive z Systems data with no impact to service level agreements and no application changes.

Real-time audit verification that z Systems data and infrastructure is protected and encrypted through IBM Security solutions.

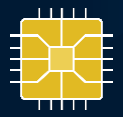
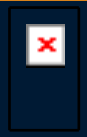
Safeguard encrypted data by protecting encryption keys with industry leading tamper-resistant cryptographic hardware and robust key management .

Enterprises can protect all data according to enterprise security policy using encryption with out interrupting business applications and operations.

Secure deployment of software appliances tamper-resistant installation and runtime, restricted administrator access, encryption of data and code.

Pervasive Encryption with IBM z Systems

Enabled through full-stack platform integration

Integrated Crypto Hardware		Hardware accelerated encryption on every core – CPACF performance improvements of up to 6x Next Gen Crypto Express6S – up to 2x faster than prior generation
Data at Rest		Broadly protect Linux file systems and z/OS data sets[1] using policy controlled encryption that is transparent to applications and databases
Clustering		Protect z/OS Coupling Facility[2] data end-to-end, using encryption that's transparent to applications
Network		Protect network traffic using standards based encryption from end to end, including encryption readiness technology[2] to ensure that z/OS systems meet approved encryption criteria
Secure Service Container		Secure deployment of software appliances including tamper protection during installation and runtime, restricted administrator access, and encryption of data and code in-flight and at-rest
Key Management		The IBM Enterprise Key Management Foundation (EKMF) provides real-time, centralized secure management of keys and certificates with a variety of cryptographic devices and key stores.

And we're just getting started …

A Paradigm Shift

From selective encryption to pervasive encryption

Encrypting only the data required to achieve compliance should be viewed as a minimum threshold, not a best practice …

The practice of pervasive encryption can also:

- Decouple encryption from classification
- Reduce risk associated with undiscovered or misclassified sensitive data
- Make it more difficult for attackers to identify sensitive data
- Help protect *all* of an organization's digital assets
- Significantly reduce the cost of compliance

"Ask most customers, 'Are you 100% sure of all your sensitive data and whether it should have this level of encryption?' Probably 100% would say that no, they don't."

Encrypt data in core business applications

Ensure that sensitive customer data in more than 50 CICS / VSAM applications processing thousands of transactions per second is protected in order to meet compliance requirements.

582.9M

Data records were compromised in 2015, including nearly 20 million financial records.

TODAY

- Organizations in this situation must implement encryption within their applications
- Application changes are costly, complex, and require significant ongoing maintenance

"We know we need to encrypt this…but we can't."

"We don't want to do this, but don't have a choice"

WITH zNEXT

- Encrypt ALL of the application data without making any application changes and no impact to SLAs
- Implement a defense-in -depth encryption strategy for a multi-layered threat defense

"Can you get it to us sooner? Can you make it happen sooner?"

"As soon as the code is available, we want it"

Meet Audit and Compliance Obligations

Comply with numerous Financial Services Sector regulations and endure relentless inspection and audit from internal auditors, external auditors, and their clients.

$4M

Average cost of a data breach in 2016

TODAY

- Experiencing an average of 50 audits per year, a "revolving door" of auditors - internal, external, clients…a state of perpetual audit
- The process is cumbersome and could stagnate for years, holding back teams and bringing unwanted visibility to the organization

"Increasing rules from inside and outside is our biggest security concern for the next 5 years."

WITH zNEXT

- With Pervasive Encryption, organizations no longer have to encrypt only the data required for compliance, they can encrypt ALL of their data
- zNext provides solutions for both application teams and auditors to verify up-to-date compliance stats in near real-time

"It's simple to demonstrate compliance, and we know what's coming well before the audit happens."

Prevent the threat from within

Ensure that that only the people with a need-to-know within the organization have access to data in the clear, while still allowing those who don't to do their jobs efficiently and effectively.

58%

Of security attacks on financial institutions in 2016 were insider attacks.

TODAY

- Organizations have a priority to limit the number of users with access to data in the clear
- The fear of insider threat, either malicious or inadvertent, is a driving force and so is the need to simplify compliance.

"We have to track all our DBA activity to make sure they're not doing what they don't need to be doing."

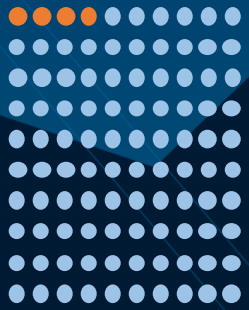
WITH zNEXT

- zNext enables encryption by policy tied to access control
- Separate access control to data sets and encryption keys
- Separation of duties — eliminate entire classes of users from compliance scope

"You covered my storage guys—that was important."

Protect Unstructured Data Objects

Large unstructured data objects that are stored in databases, such as policy documents, billing statements, and medical records in PDF or image format, contain sensitive data.



4%

Out of the 6 billion records breached since 2013, only 4% were encrypted.

TODAY

- The company is held responsible for protecting ALL customer data
- There are many documents with sensitive customer data that reside as objects within the database and there is no way to encrypt them today.

"We recognize this is sensitive, but there are limitations to our technology…"

WITH zNEXT

- Binary large objects can be protected through full database encryption, without any application changes or add-on products
- Easy to set up and maintain

"We're excited to finally be reducing this risk."

Protect Archived Transactional Logs

Historical financial transactional logs contain sensitive information that must be protected, and must be retained for long periods of time for research and compliance purposes.

48% of financial institutions are putting more sensitive data in the cloud

TODAY

- Historical logs are accessed infrequently and should be transferred to lower cost cloud storage to reduce costs
- Current encryption provided by cloud storage solutions has gaps, does not protect data end-to-end, and introduces additional complexities with management of encryption keys

"We generate a lot of log files that we have to store each year…"

WITH zNEXT

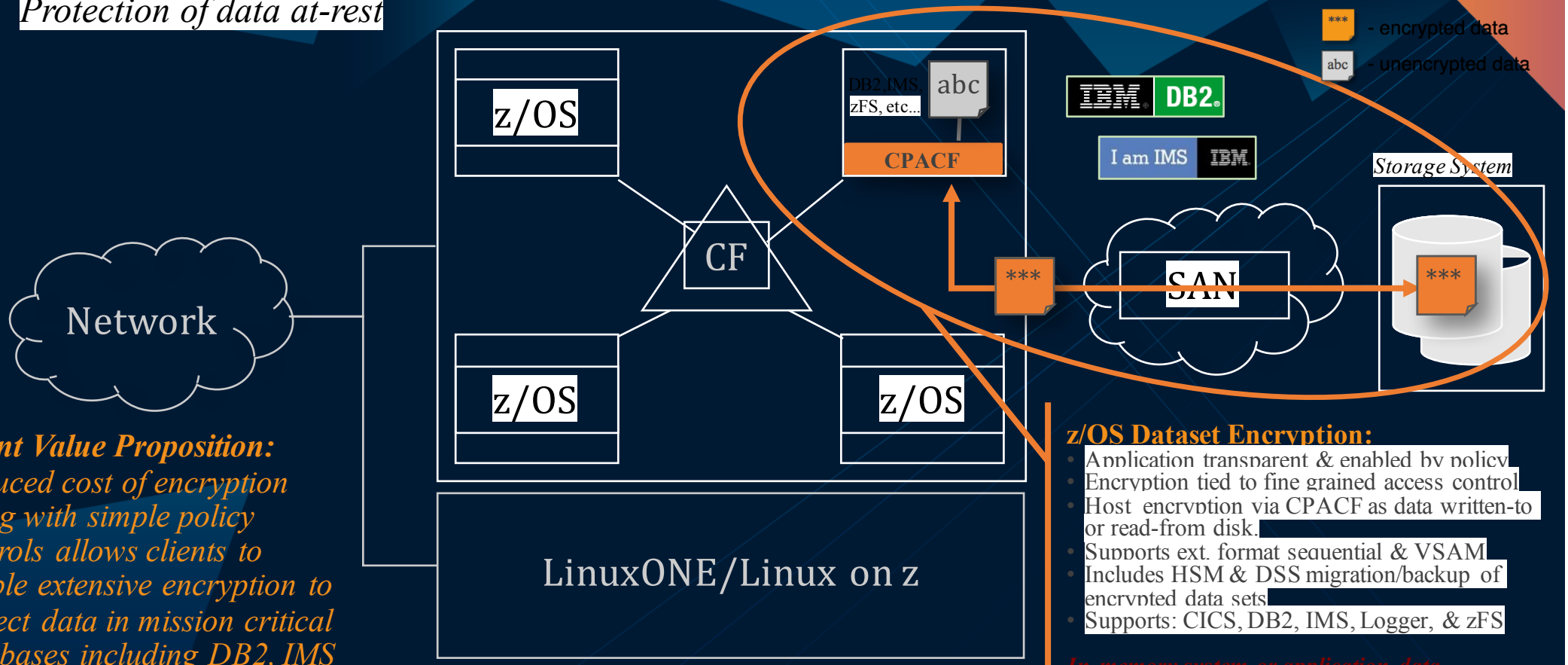
- z/OS data set encryption, z/OS storage automation, and Transparent Cloud Tiering provide the ability to automatically transfer and encrypt data end-to-end in the cloud
- Encryption is centrally managed and controlled by the z Systems host, reducing the risk of a data breach

"That would be perfect. That's what we would like to be able to do."

Data Protection // z/OS Dataset Encryption

Protection of data at-rest

z/OS 2.2 & 2.3



Client Value Proposition:
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

z/OS Dataset Encryption:

- Application transparent & enabled by policy
- Encryption tied to fine grained access control
- Host encryption via CPACF as data written-to or read-from disk.
- Supports ext. format sequential & VSAM
- Includes HSM & DSS migration/backup of encrypted data sets
- Supports: CICS, DB2, IMS, Logger, & zFS

In-memory system or application data buffers will not be encrypted

Data Protection // Coupling Facility Encryption

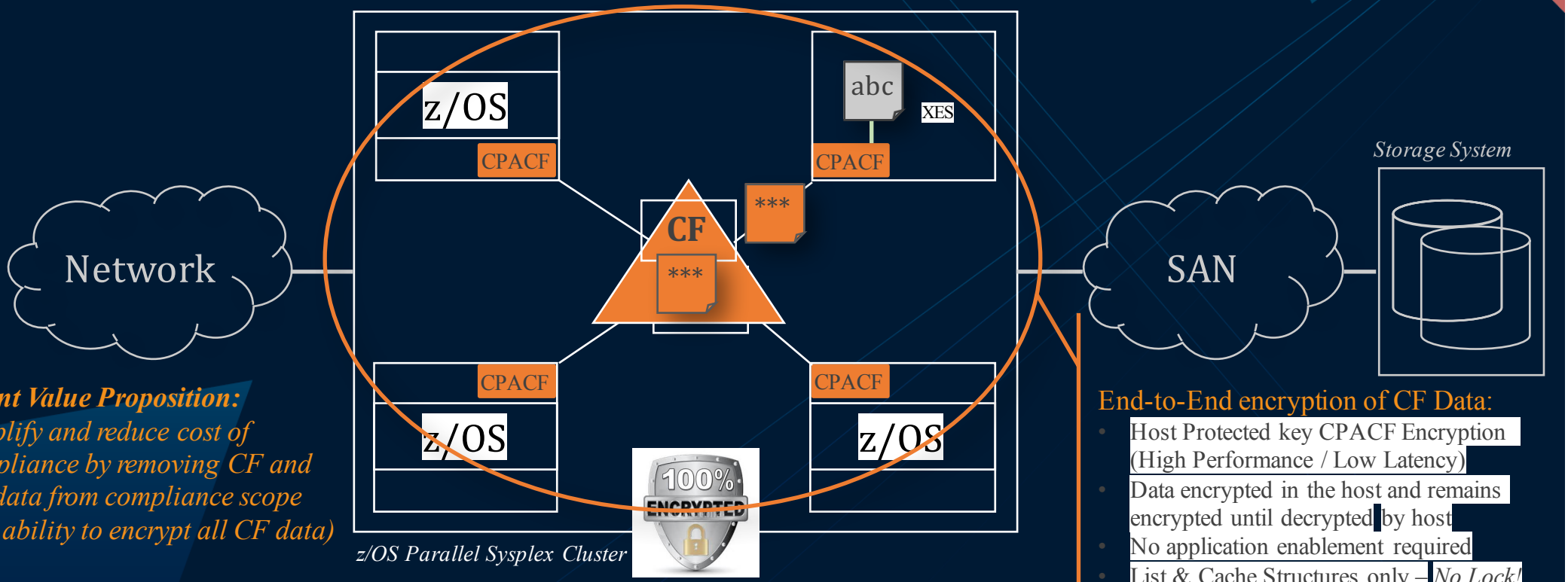
Protection of data in-flight and in-use (CF)

z/OS 2.3

Legend:

*** - encrypted data

abc - unencrypted data



Client Value Proposition:
Simplify and reduce cost of compliance by removing CF and CF data from compliance scope (i.e. ability to encrypt all CF data)

End-to-End encryption of CF Data:

- Host Protected key CPACF Encryption (High Performance / Low Latency)
- Data encrypted in the host and remains encrypted until decrypted by host
- No application enablement required
- List & Cache Structures only – *No Lock!*

Data Protection // z/OS Network Security

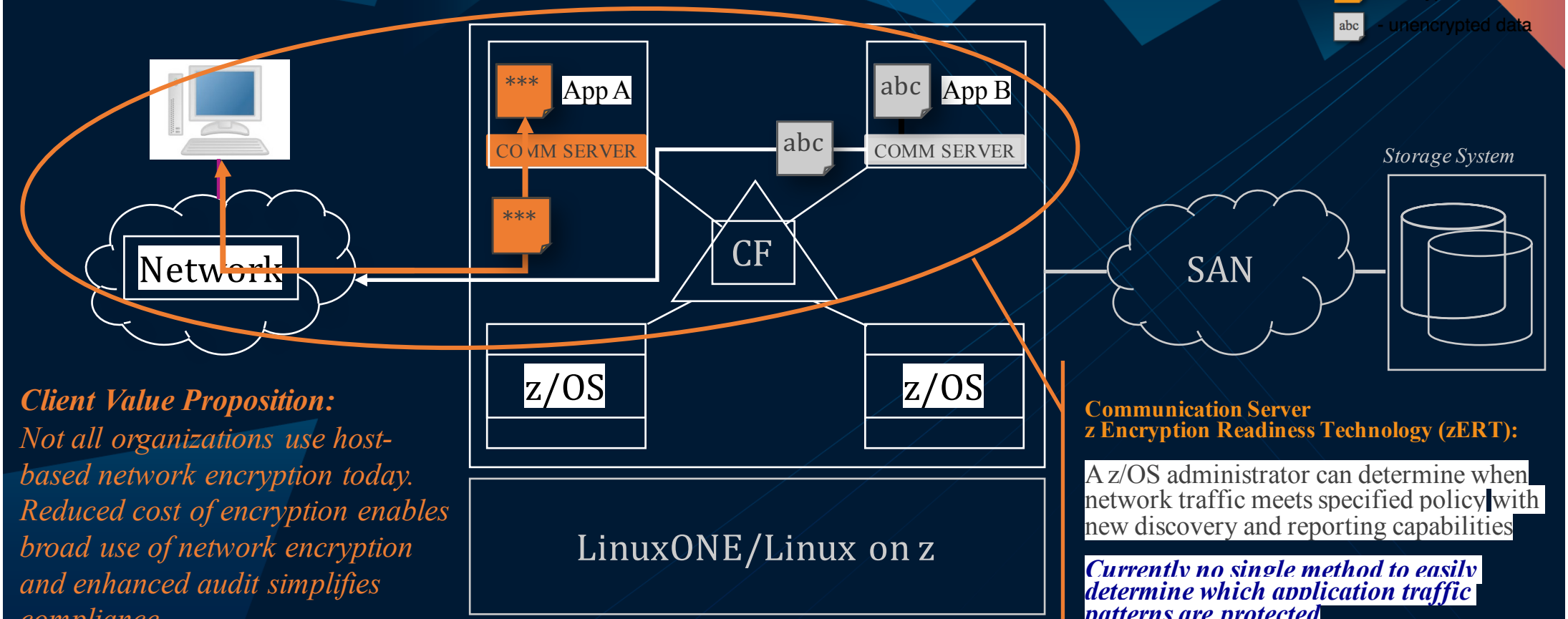
Protection of data in-flight

z/OS 2.3

Legend:

*** - encrypted data

abc - unencrypted data



Client Value Proposition:

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

Communication Server
z Encryption Readiness Technology (zERT):

A z/OS administrator can determine when network traffic meets specified policy with new discovery and reporting capabilities

Currently no single method to easily determine which application traffic patterns are protected

Thank you!