IBM z14 / Pervasive Encryption

Julie Bergh

Executive Cyber Security Specialist

Trademarks

* Registered trademarks of IBM Corporation

CICS*
DB2*
DFSMS
DS8000*
Guardium
IBM*
IBM (logo)*
IBM Z
IMS
Qradr*
RACF*
z13*
z14
zSecure
z/OS*
z/VM*

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
IT Infrastructure Library is a Registered Trade Mark of AXELOS Limited.
ITIL is a Registered Trade Mark of AXELOS Limited.
Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
UNIX is a registered trademark of The Open Group in the United States and other countries.
VMware, the VMware logo, VMware Cloud Foundation, VMware Cloud Foundation Service, VMware vCenter Server, and VMware vSphere are registered trademarks or trademarks of VMware, Inc. or its subsidiaries in the United States and/or other jurisdictions.
Other product and service names might be trademarks of IBM or other companies.

Notes:
Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.
IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.
All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.
This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.
All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.
Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.
This information provides only general descriptions of the types and portions of workloads that are eligible for execution on Specialty Engines (e.g, zIIPs, zAAPs, and IFLs) ("SEs"). IBM authorizes customers to use IBM SE only to execute the processing of Eligible Workloads of specific Programs expressly authorized by IBM as specified in the “Authorized Use Table for IBM Machines” provided at www.ibm.com/systems/support/machine_warranties/machine_code/aut.html (“AUT”). No other workload processing is authorized for execution on an SE. IBM offers SE at a lower price than General Processors/Central Processors because customers are authorized to use SEs only to process certain types and/or amounts of workloads as specified by IBM in the AUT.

IBM Z: Designed for Trusted Digital Experiences

Pervasive Encryption is the New Standard

Encrypt all data for applications & databases

Zero application changes

Zero impact to service levels

Protect client and corporate from internal and external threats

Analytics & Machine Learning for Continuous Intelligence Across the Enterprise

Anticipate customer needs and embed insight in every business transaction

Dramatically faster lifecycle management of behavioral models with more memory and greater processing capacity

Derive impactful insights by combining z Systems data with other structured and unstructured external data sources

Open Enterprise Cloud to Extend, Connect and Innovate

Cut new service build time by 90% using secure APIs on IBM z and advanced DevOps

Seamlessly connect any service from public and private cloud with transactions and data on IBM Z

Accelerate innovation with an ecosystem of partners to develop and manage enterprise wide applications leveraging 1000’s open source software packages

Container Pricing For IBM Z provides new flexibility for modern digital workloads.

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 **9 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/

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:

- 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

Pervasive encryption is the new standard

IBM z14

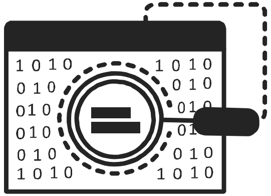
The world's premier system for enabling

Data as the new perimeter

Encrypt IBM Z® data in-flight and at-rest with new capabilities in hardware, OS, and middleware.

No Application Changes

IBM z14



All application and database data

Protect all application and database data according to enterprise security policy using encryption without application changes and no impact to SLAs.

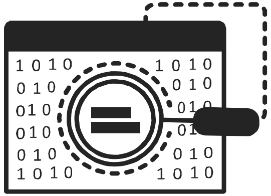
Bulk encryption enabled in the Operating System for:

Simple implementation
Transparent exploitation
Optimized performance

Blazing fast hardware-accelerated encryption on every core is up to 7x faster than IBM z13® and 2.5x faster than x86.

Secure Service Container delivers tamper-resistant installation and runtime, restricted administrator access, encryption of data and code.

IBM z14



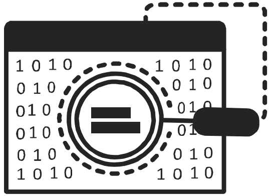
All in-flight network data and APIs

Encrypt all incoming and outgoing network connections for true end-to-end data protection.

Secure the cloud by encrypting APIs 2-3x faster than x86 systems.

Integrate any z/OS® subsystem through API’s with transactions that have occurred in the Blockchain High Security Business Network.

IBM z14



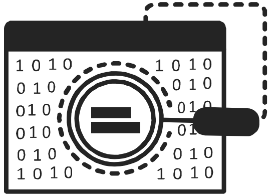
All encryption keys protected

Safeguard encrypted data by protecting encryption keys with tamper-responding cryptographic hardware, designed to meet the certification requirements for FIPS 140-2 Level 4.

Industry-exclusive protected key encryption delivers both high-performance and high-security.

Ensure the availability and security of encrypted data with robust, centralized full-lifecycle encryption key management.

IBM z14



All compliance

Pervasive encryption on IBM Z significantly reduces the time and effort required to meet compliance obligations and complete audits.

Remove entire classes of data and users from compliance scope.

Real-time, self-service audit verification that IBM Z data and infrastructure is protected and encrypted.

IBM Z pervasive encryption
Technical Foundation

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 7x 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 …

[1] Statement of Direction* in the z/OS Announcement Letter (10/4/2016) - http://ibm.co/2ldwKoC

[2] IBM z/OS Version 2 Release 3 Preview Announcement Letter (2/21/2017) - http://ibm.co/2l43ctN

Pervasive Encryption with IBM z Systems

Technical Foundation

IBM z14™ (z14) -- Designed for Pervasive Encryption

- ✦ CPACF – Dramatic advance in bulk symmetric encryption performance
- ✦ Crypto Express6s – Doubling of asymmetric encryption performance for TLS handshakes
- ✦ CFCC – Designed for CF data encryption (wrapped encryption key stored for recovery scenarios)

z/OS -- New approach to encryption in-flight and at-rest data

- ✦ z/OS data set encryption – Transparent encryption of data at-rest
- ✦ z/OS CF encryption –Transparent end-to-end encryption of CF data
- ✦ z/OS Communication Server - Intelligent Network Security discovery & reporting

Linux on z/LinuxONE -- Full Power of Linux Ecosystem combined with z14 Capabilities

- ✦ LUKS dm-crypt – Transparent file and volume encryption using industry unique CPACF protected-keys
- ✦ Network Security – Enterprise scale encryption and handshakes using z14 CPACF and SIMD
- ✦ Secure Service Container – Automatic protection of data and code for virtual appliance

zVM **®– Encrypted paging support**
zTPF - Transparent database encryption (*available 8/2016*)

Software-only elements expected on previous generation of z Systems with differentiated value for z14

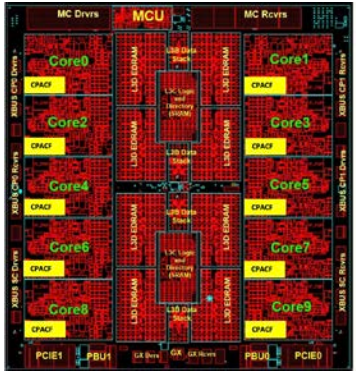
z14 Integrated Cryptographic Hardware

CP Assist for Cryptographic Functions (CPACF)

- Hardware accelerated encryption on every microprocessor core
- Performance improvements of up to 6x for selective encryption modes

Crypto Express6S

- Next generation PCIe Hardware Security Module (HSM)
- Performance improvements up to 2x
- Industry leading FIPS 140-2 Level 4 Certification Design



Why is it valuable:

- More performance = lower latency + less CPU overhead for encryption operations
- Highest level of protection available for encryption keys
- Industry exclusive “protected key” encryption

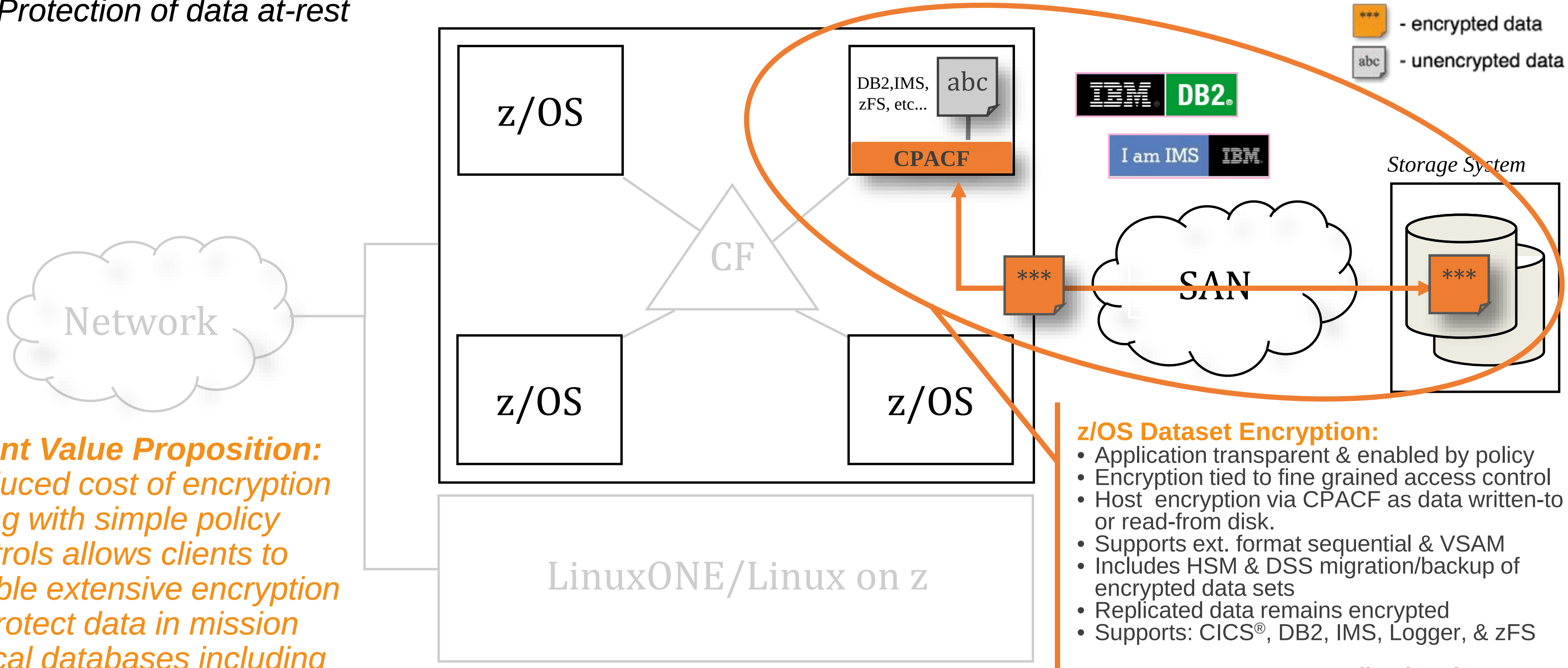
z/OS 2.2 & 2.3

Data Protection // z/OS Dataset Encryption

Protection of data at-rest

Legend:

- *** - encrypted data
- abc - unencrypted data



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
- Replicated data remains encrypted
- Supports: CICS®, DB2, IMS, Logger, & zFS

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

z/OS 2.3

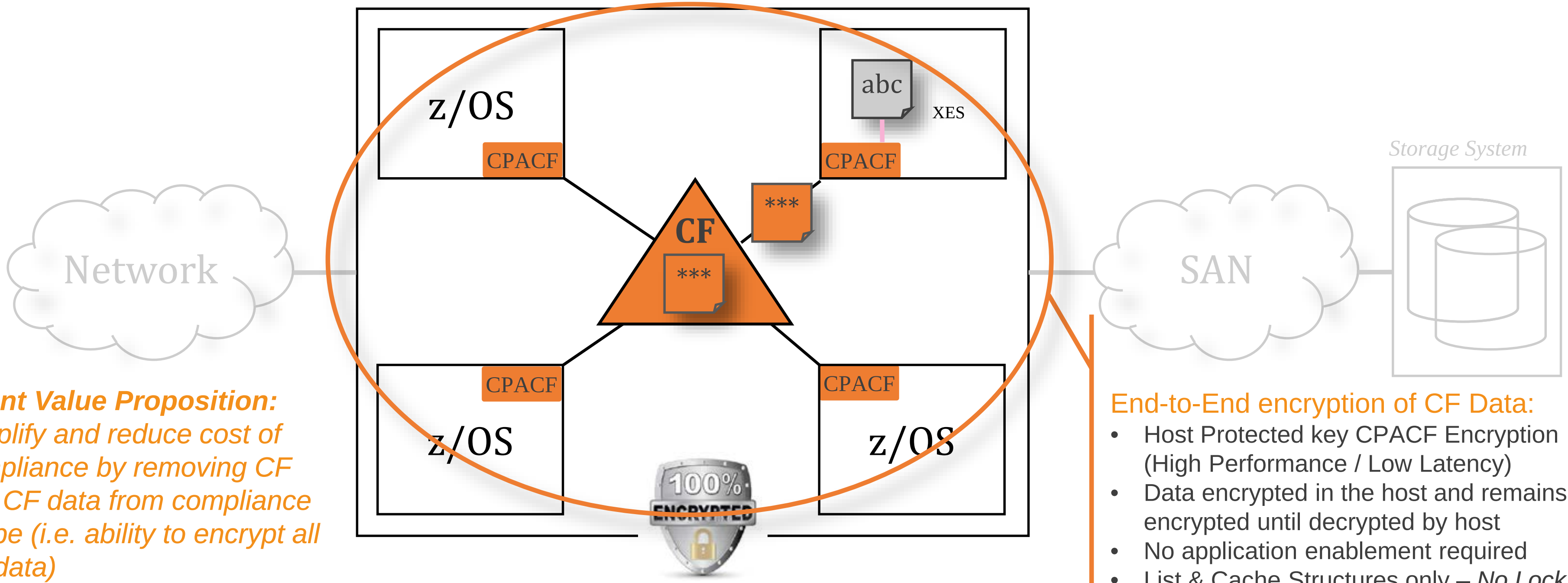
Data Protection // Coupling Facility Encryption

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

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

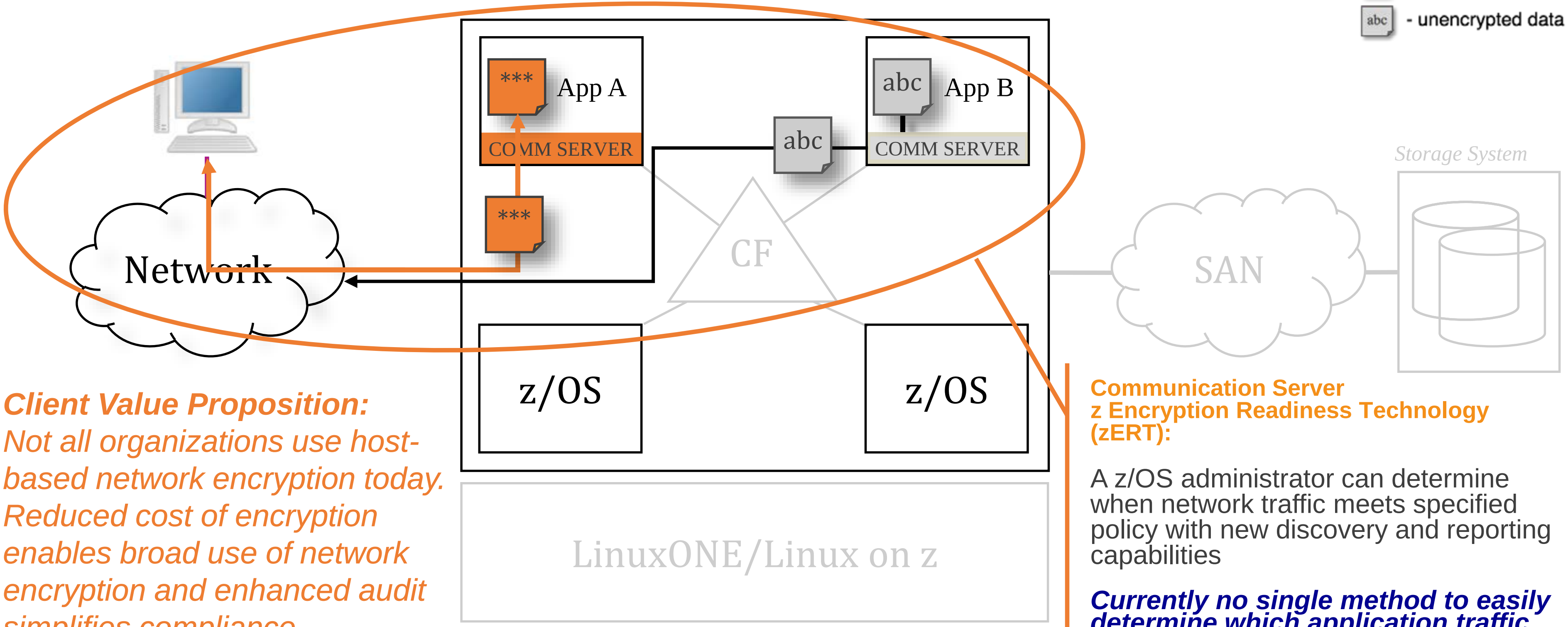
Protection of data in-flight

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

Data Protection // Linux on z File Encryption

Protection of data at-rest

Submitted Upstream

Legend:

*** - encrypted data

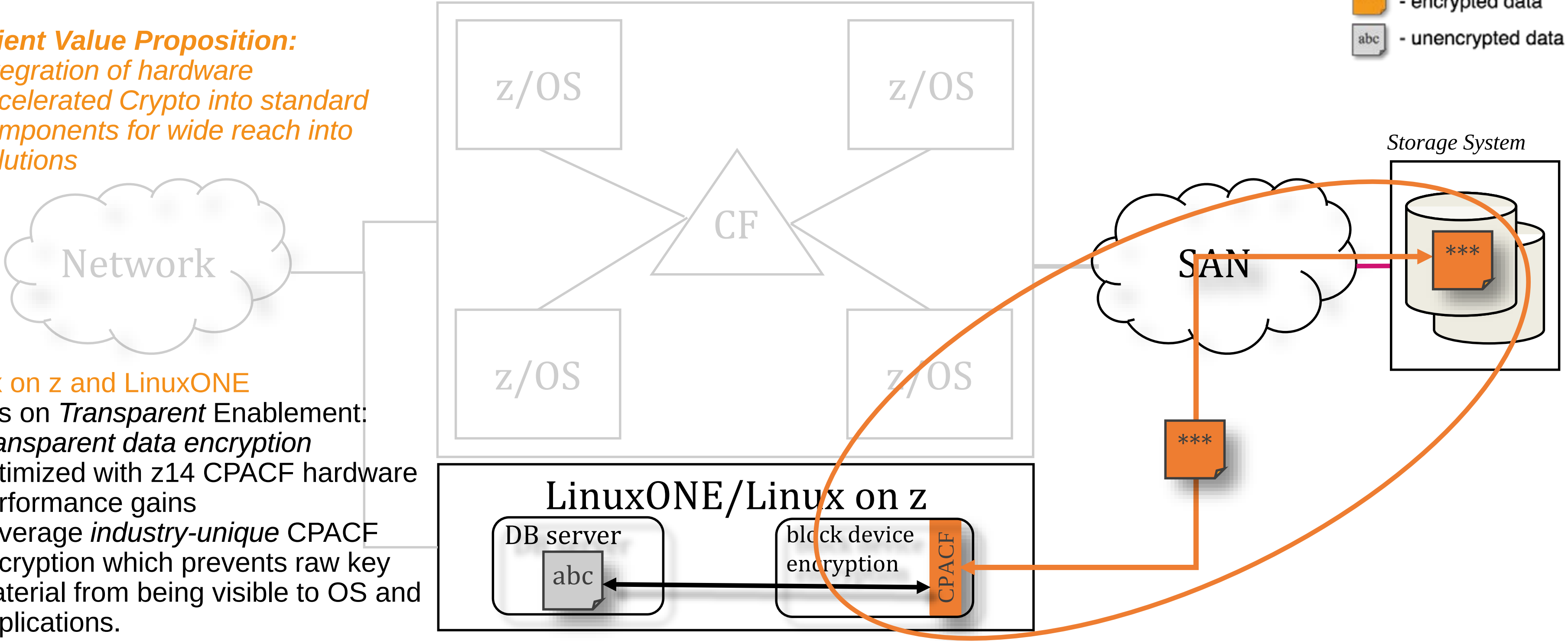
abc - unencrypted data

Client Value Proposition: *Integration of hardware accelerated Crypto into standard components for wide reach into solutions*

Linux on z and LinuxONE

Focus on *Transparent* Enablement:

- *Transparent data encryption* optimized with z14 CPACF hardware performance gains
- Leverage *industry-unique* CPACF encryption which prevents raw key material from being visible to OS and applications.



Status: dm-crypt enhancements for CPACF protected-key submitted upstream

Data Protection // Linux on z Network Security

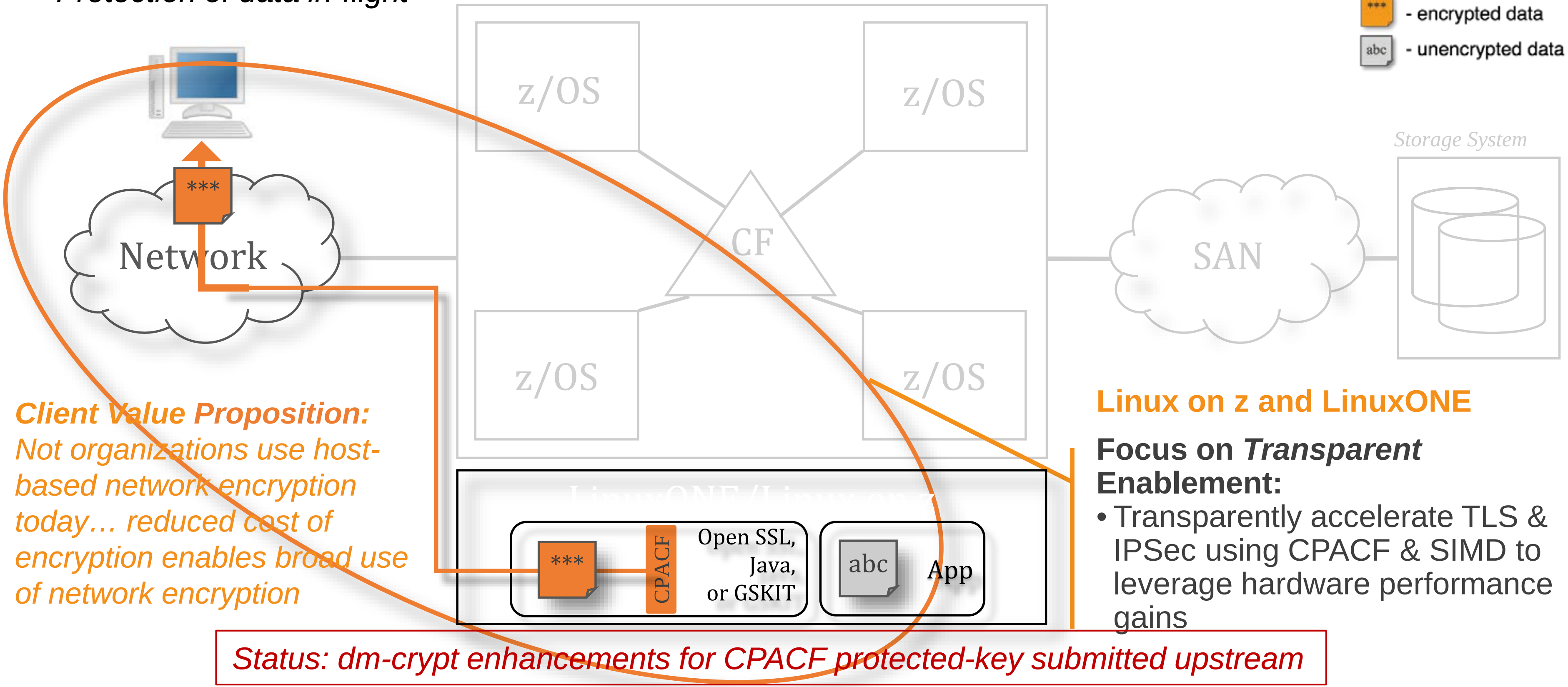
Protection of data in-flight

Submitted Upstream

Legend:

*** - encrypted data

abc - unencrypted data



Client Value Proposition:

Not organizations use host-based network encryption today… reduced cost of encryption enables broad use of network encryption

Linux on z and LinuxONE

Focus on *Transparent* Enablement:

- Transparently accelerate TLS & IPSec using CPACF & SIMD to leverage hardware performance gains

Status: dm-crypt enhancements for CPACF protected-key submitted upstream

Data Protection // Secure Service Container

Extending the value of Z hardware crypto

Client Value Proposition:

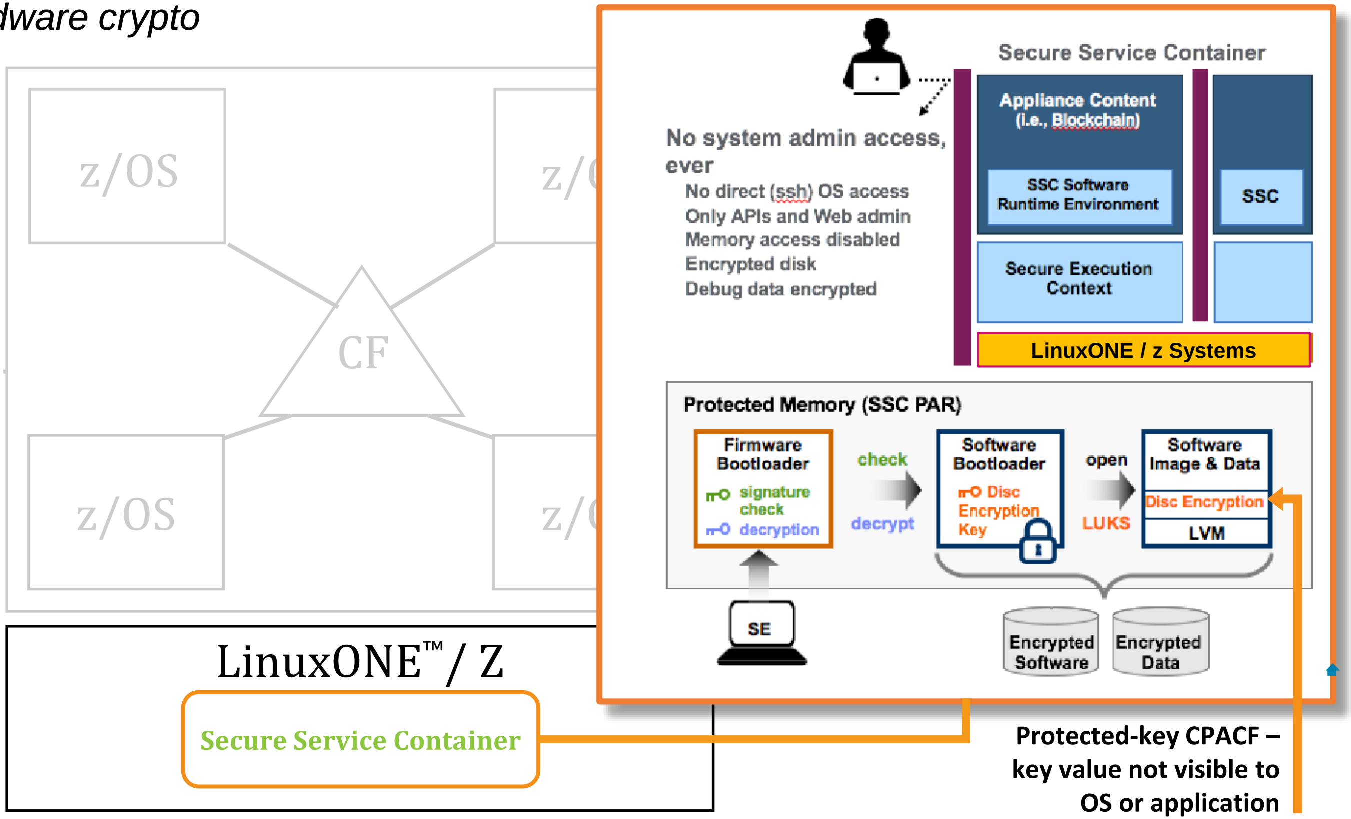
Simplified, fast deployment and management of packaged solutions

Tamper protection during Appliance installation and runtime

Confidentiality of data and code running within the Appliance both at flight and at rest

Restricts administrator access to workload and data

Secure Service Container architecture builds on the value z systems hardware crypto using a runtime environment designed to help clients reduce risk.

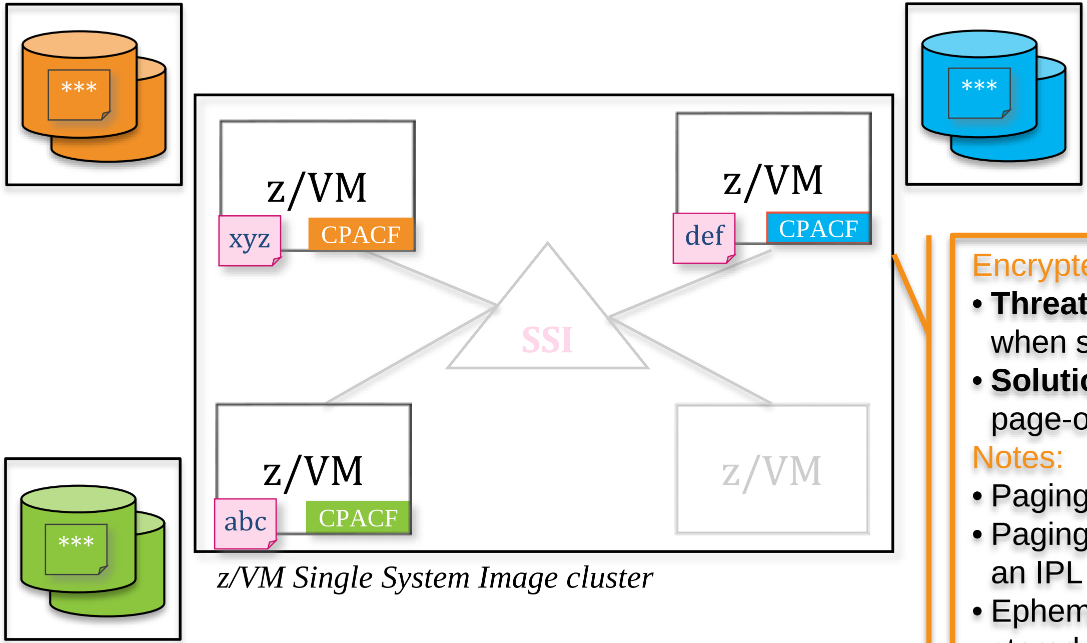


No system admin access, ever

No direct (ssh) OS access
Only APIs and Web admin
Memory access disabled
Encrypted disk
Debug data encrypted

Protected-key CPACF – key value not visible to OS or application z/VM 6.4

Data Protection // z/VM Encrypted Paging



z/VM Single System Image cluster

Encrypted Paging

- **Threat**: access to sensitive data when stored on CP owned disk
- **Solution**: encrypt guest data on page-out.

Notes:

- Paging is not SSI-relevant
- Paging data does not need to survive an IPL
- Ephemeral CPACF protected-key stored in CP (not on disk somewhere)
- AES encryption
- Very low overhead via CPACF

Client Value Proposition:

Protect guest paging data from administrators and/or users with access to volumes z/TPF 1.1.0.13

Data Protection // z/TPF Transparent Database Encryption

Technical Foundation

z/TPF at-rest Data Encryption

- Automatic encryption of at-rest data
- No application changes required
- Database level encryption using highly efficient CPACF HW crypto
- Includes data on disk and cached in memory
- Optionally can include data integrity checking to detect accidental or malicious data corruption

Client Value Proposition:

Transparent encryption of TPF database data plus reduced cost of encryption allows clients to enable extensive encryption of TPF data.

Additional Information

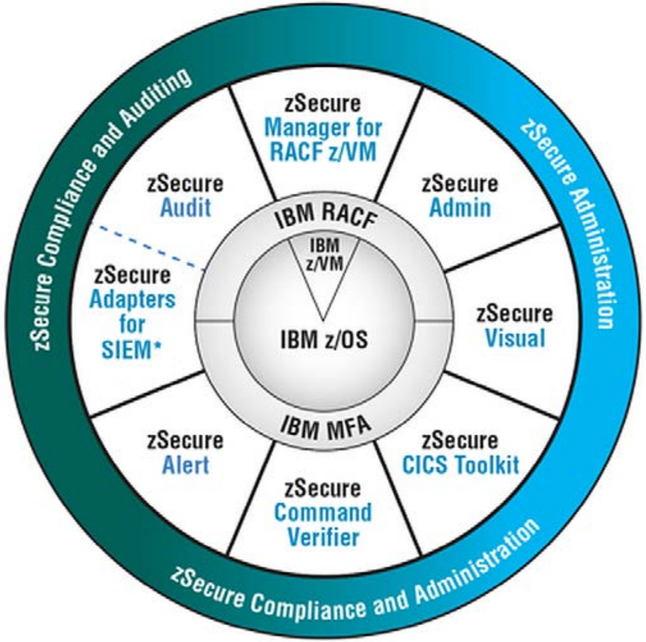
- Data encrypted using AES CBC (128 or 256)
- Optional integrity checking uses SHA-256
- Includes tools to migrate an existing DB from unencrypted to encrypted state or change the encryption key/algorithm for a given DB while transactions are flowing (no DB downtime)

Support shipped August 2016

(APAR PI56476)

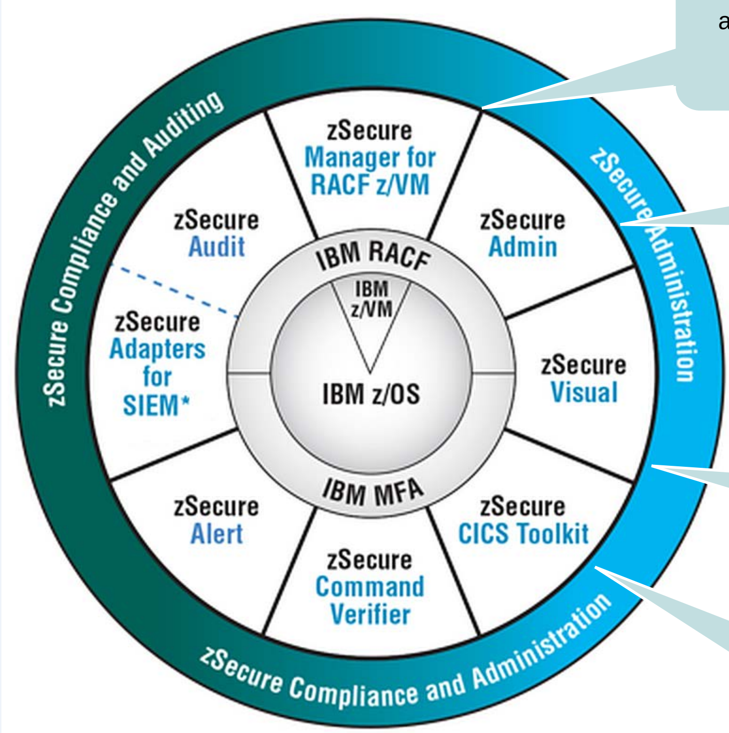
IBM Security zSecure Suite

IBM Security zSecure suite



* Product offers a subset of the capabilities provided by zSecure Audit

IBM Security zSecure ion



* Product offers a subset of the capabilities provided by zSecure Audit

Combined audit and administration for RACF in the VM environment including auditing Linux on System z

Enables more efficient and effective RACF administration, using significantly fewer resources

Helps reduce the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration

Provides access RACF command & APIs from a CICS environment, allowing additional administrative flexibility

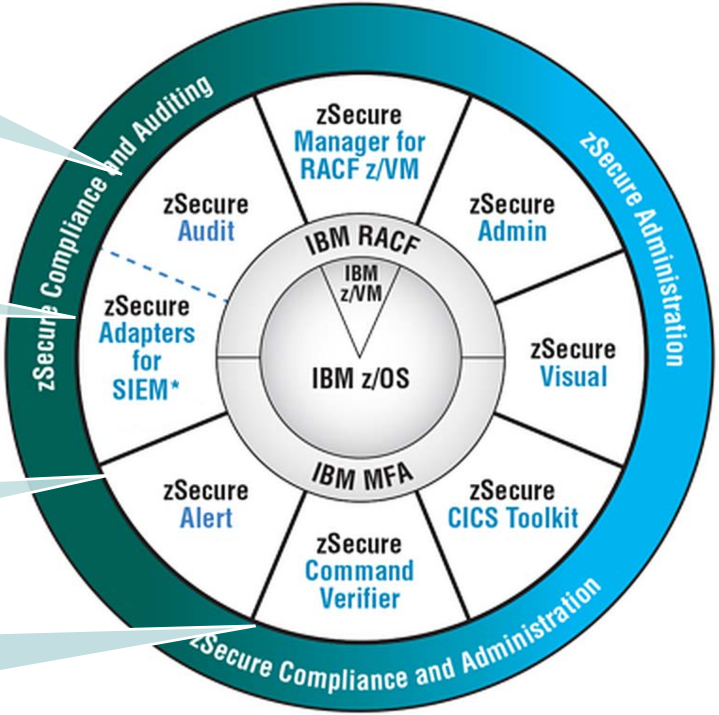
IBM Security zSecure suite – Compliance and Auditing

Vulnerability analysis for the mainframe infrastructure. Automatically analyze and report on security events & detect security exposures

Collects, formats and sends enriched mainframe System Management Facility (SMF) audit records to supported SIEM

Real-time mainframe threat monitoring permits you to monitor intruders and identify misconfigurations that could hamper your compliance efforts

Policy enforcement solution that helps enforce compliance to company and regulatory policies by preventing erroneous commands



* Product offers a subset of the capabilities provided by zSecure Audit

zSecure 2.3 Pervasive Encryption Support

Command Verifier: Command Verifier policy for DATAKEY

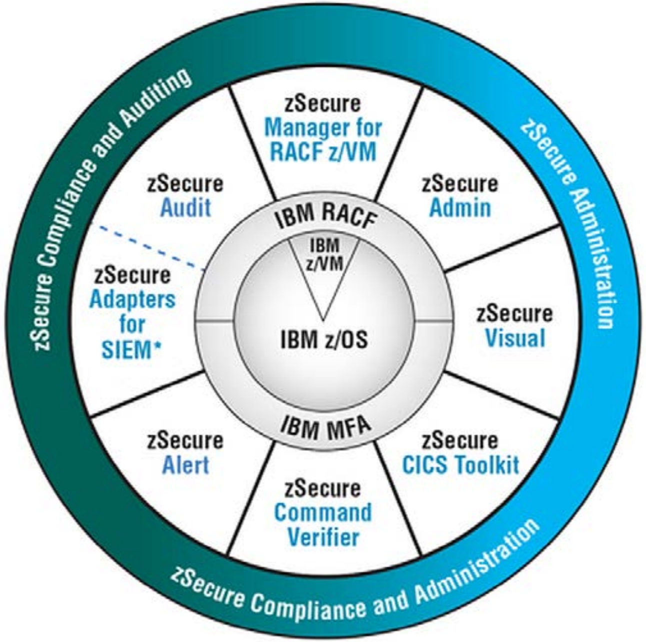
Admin: Easy administration DATAKEY on DFP segment

Audit: Report on non-VSAM and VSAM data sets key labels
- Extend existing report types DSN / SENSDSN

Audit: Report key protection CSFKEYS
- New report types ICSF_SYMKEY, ICSF_PUBKEY

Audit: Report which systems sharing DASD can decrypt ds

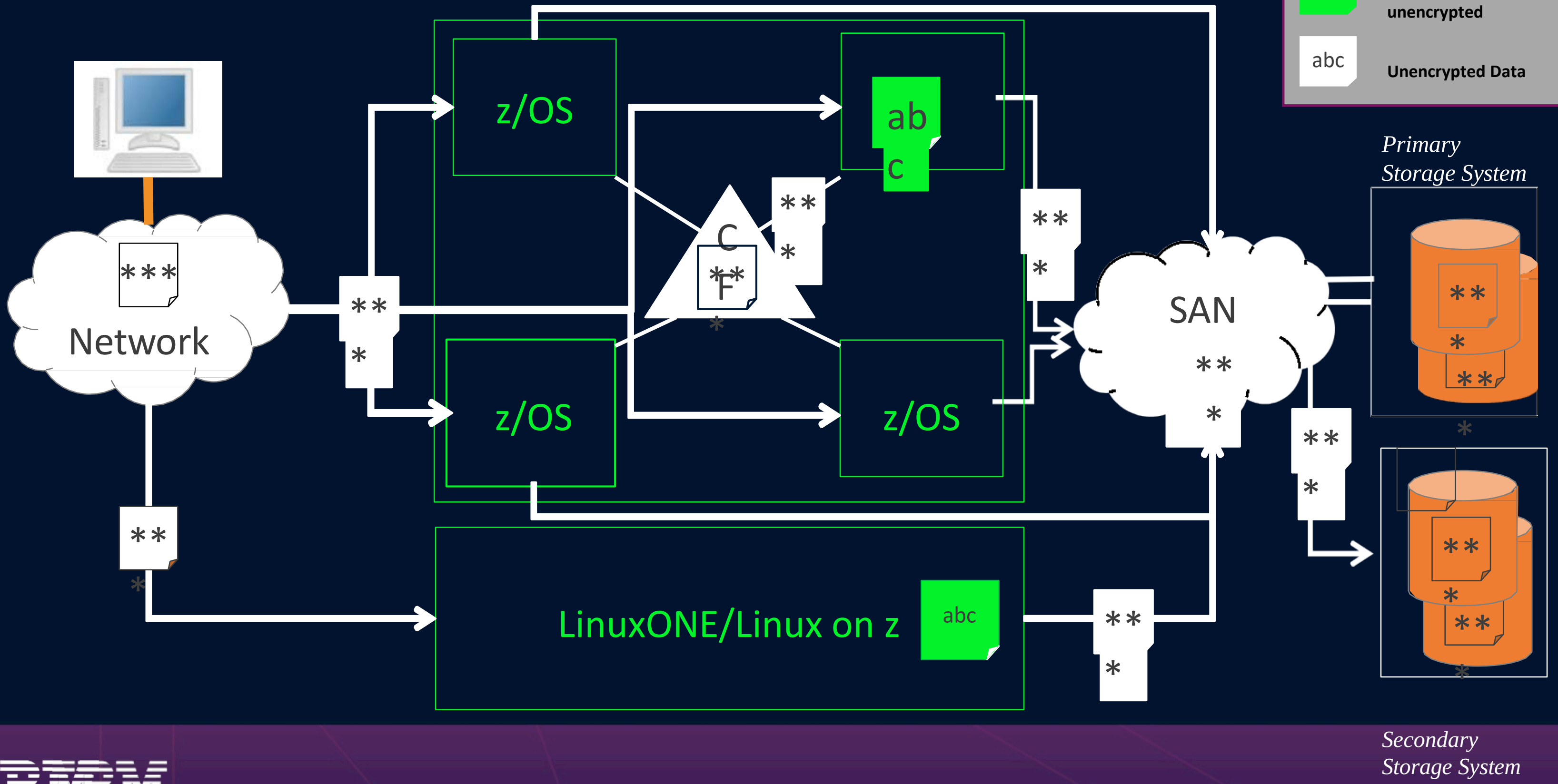
Audit: Extend report type SMF
- Type 14/15 non-VSAM and Type 62 VSAM keylabel use
- ICSF
- zERT records to show encryption strengths



Data Protection // Encryption Today

Legend:

**	**Encrypted Data**
abc	**Secured by RACF, unencrypted**
abc	**Unencrypted Data**



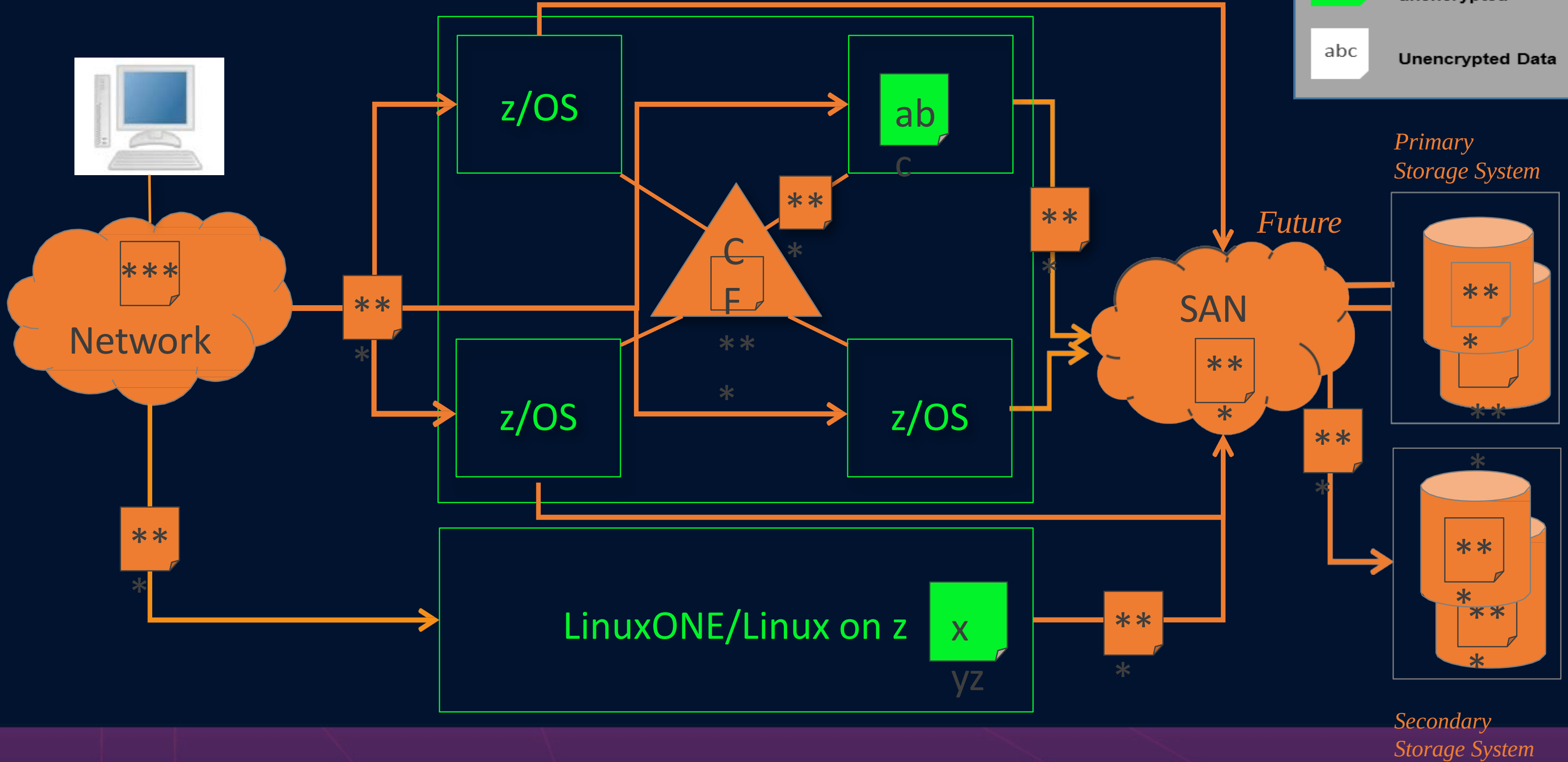
© 2017 IBM Corporation

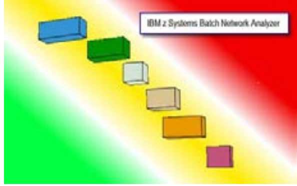
Data Protection // Encrypt Everything

Protection of data at-rest and in-flight

Legend:

- *** Encrypted Data
- abc Secured by RACF, unencrypted
- abc Unencrypted Data





Estimating CPU Cost of Data Protection

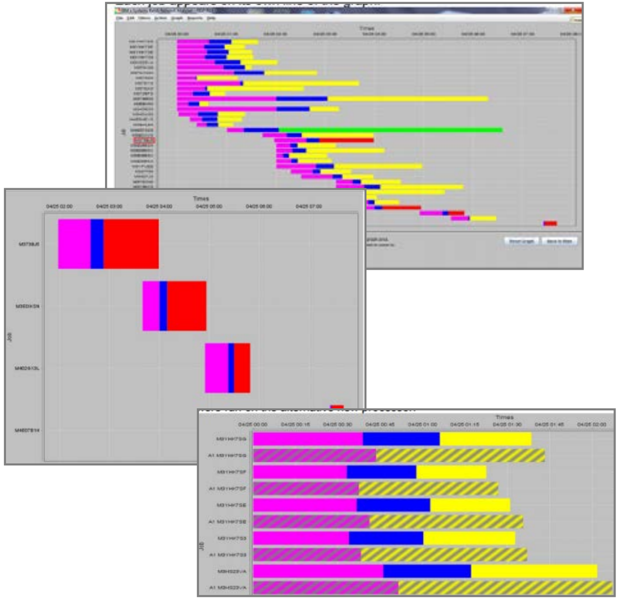
z Batch Network Analyzer (zBNA)

Background:

- A no charge, “as is” tool originally designed to analyze batch windows
- PC based, and provides graphical and text reports
- Available on techdocs for customers, business partners, and IBMers http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132
- Previously enhanced for zEDC to identify & evaluate compression candidates

Encryption Enhancements:

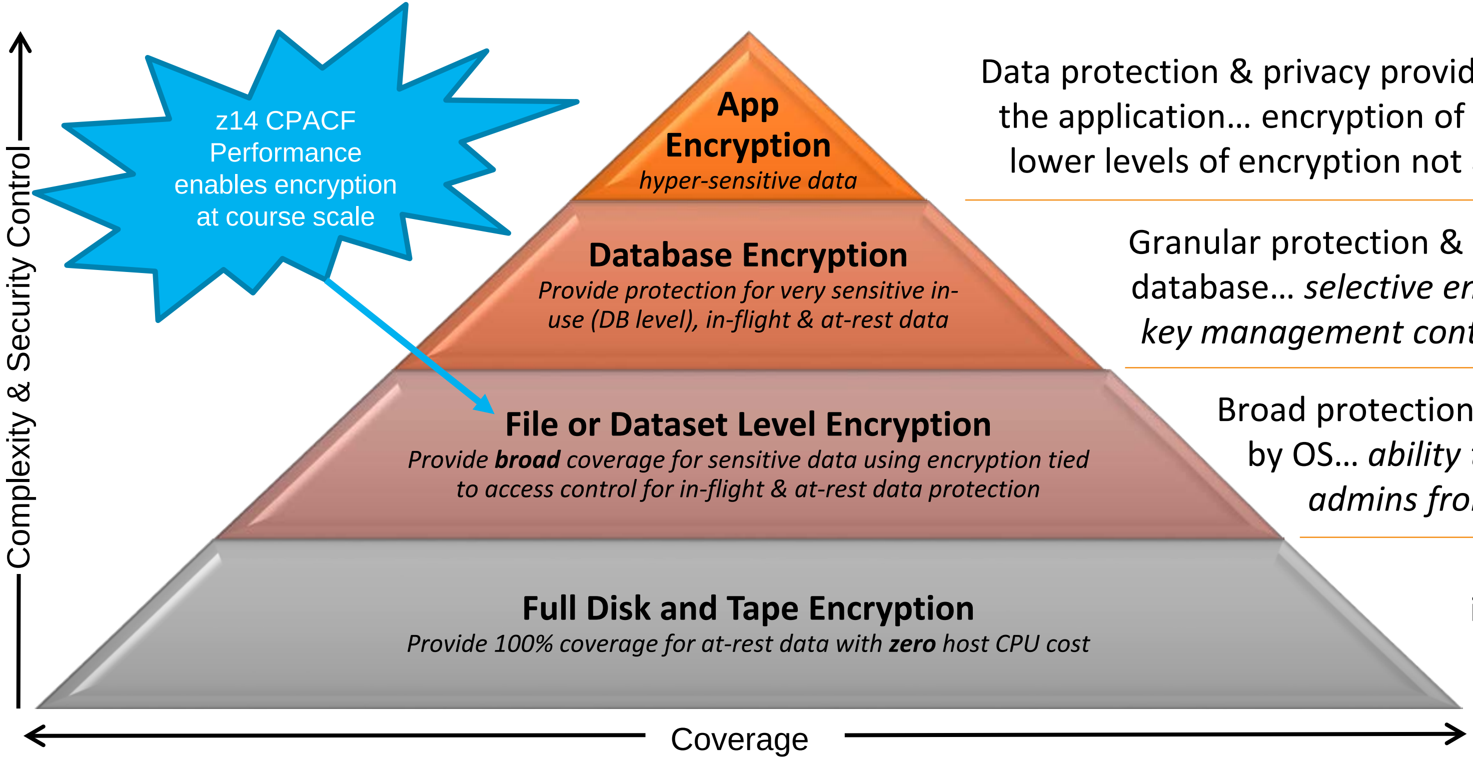
- zBNA will be further enhanced to help clients estimate encryption CPU overhead based on actual client workload SMF data
- Ability to select z13 or z14 as target machine
- Support will be provided for
  - z/OS data set encryption
  - Coupling Facility encryption



IBM Z pervasive encryption Considerations

Multiple Layers of Encryption

Robust data protection



z14 CPACF Performance enables encryption at course scale
App Encryption
hyper-sensitive data
Database Encryption
Provide protection for very sensitive in-use (DB level), in-flight & at-rest data
File or Dataset Level Encryption
*Provide **broad** coverage for sensitive data using encryption tied to access control for in-flight & at-rest data protection*
Full Disk and Tape Encryption
*Provide 100% coverage for at-rest data with **zero** host CPU cost*
Complexity & Security Control
Coverage

Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

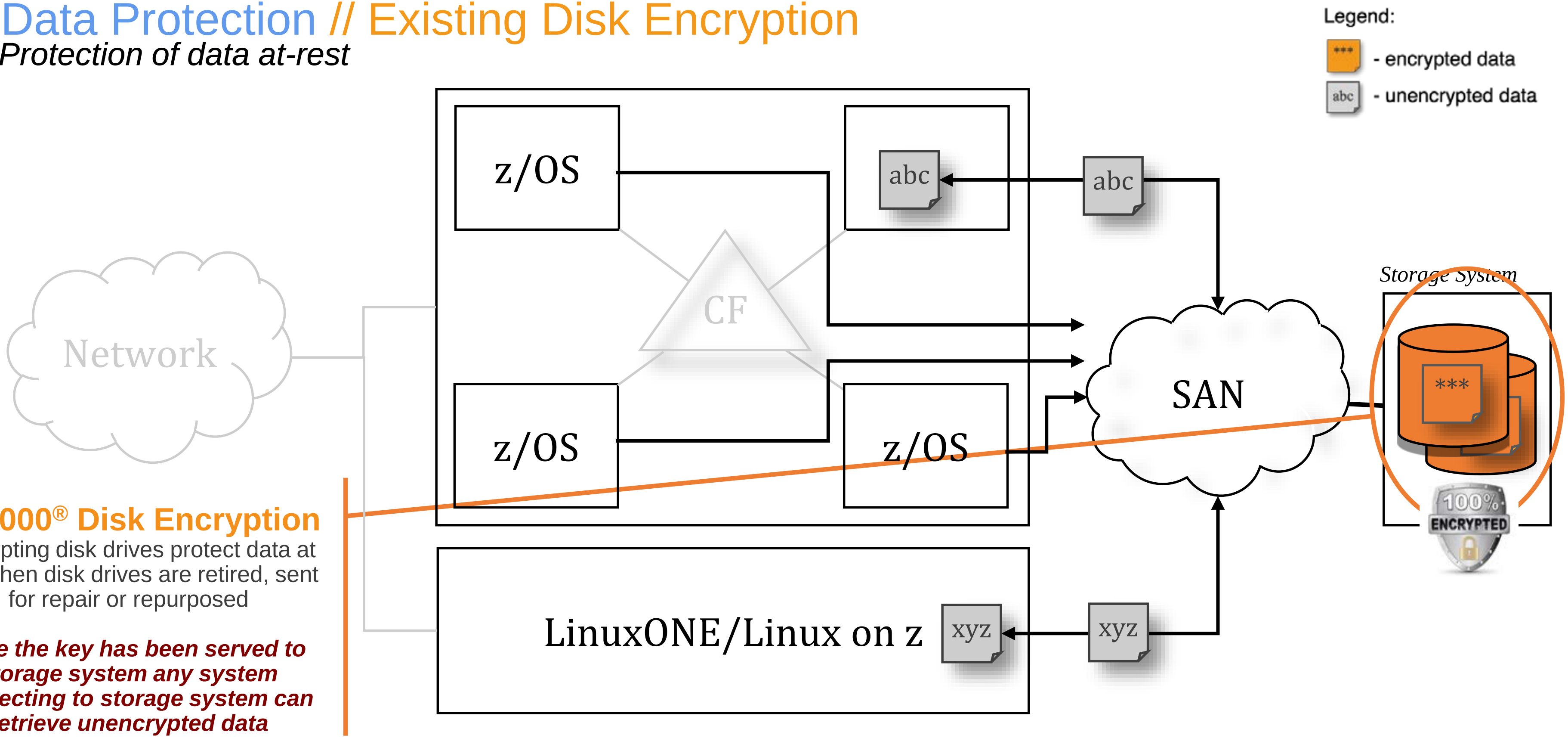
Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

Protection against intrusion, tamper or removal of *physical* infrastructure

Data Protection // Existing Disk Encryption

Protection of data at-rest



DS8000® Disk Encryption

Encrypting disk drives protect data at rest when disk drives are retired, sent for repair or repurposed

Once the key has been served to storage system any system connecting to storage system can retrieve unencrypted data

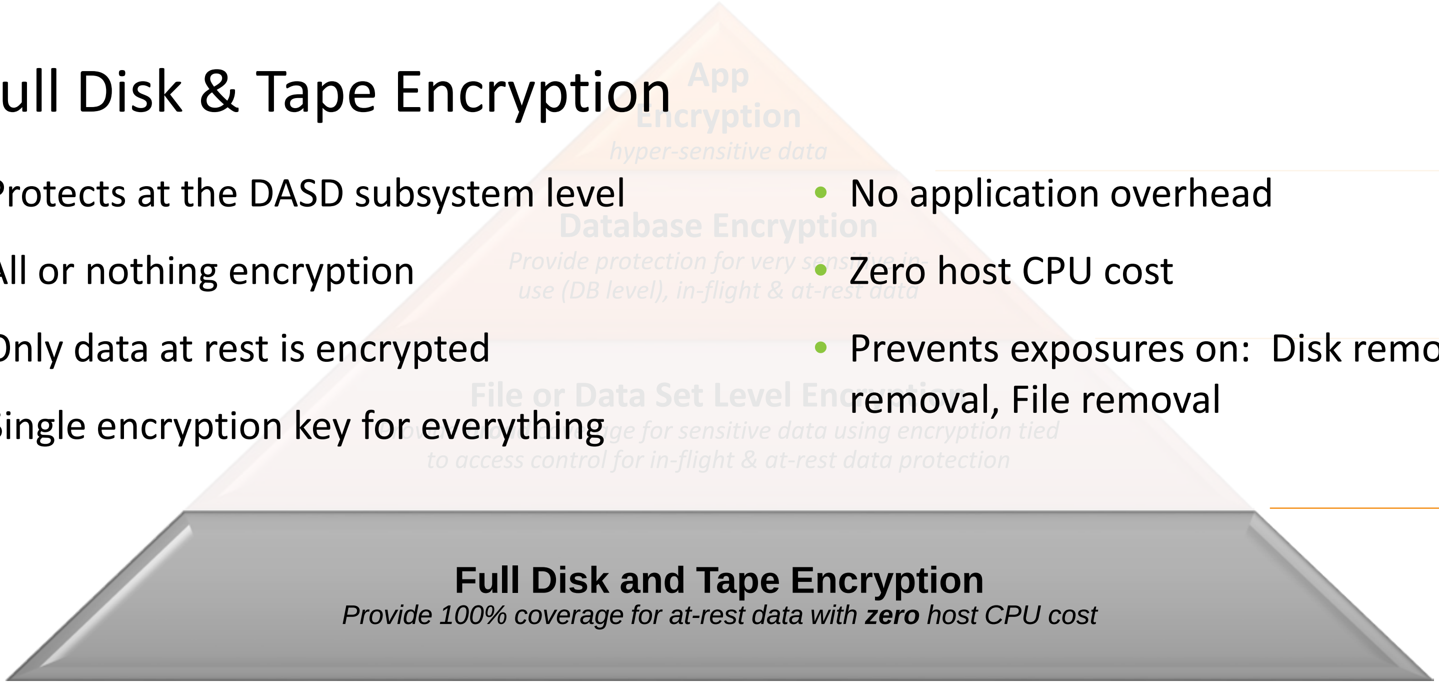
Multiple layers of encryption for data at-rest

Robust data protection

Full Disk & Tape Encryption

- Protects at the DASD subsystem level
- All or nothing encryption
- Only data at rest is encrypted
- Single encryption key for everything

- No application overhead
- Zero host CPU cost
- Prevents exposures on: Disk removal, Box removal, File removal



App Encryption
hyper-sensitive data
Database Encryption
Provide protection for very sensitive in-use (DB level), in-flight & at-rest data
File or Data Set Level Encryption
Provide broad coverage for sensitive data using encryption tied to access control for in-flight & at-rest data protection

Full Disk and Tape Encryption

*Provide 100% coverage for at-rest data with **zero** host CPU cost*

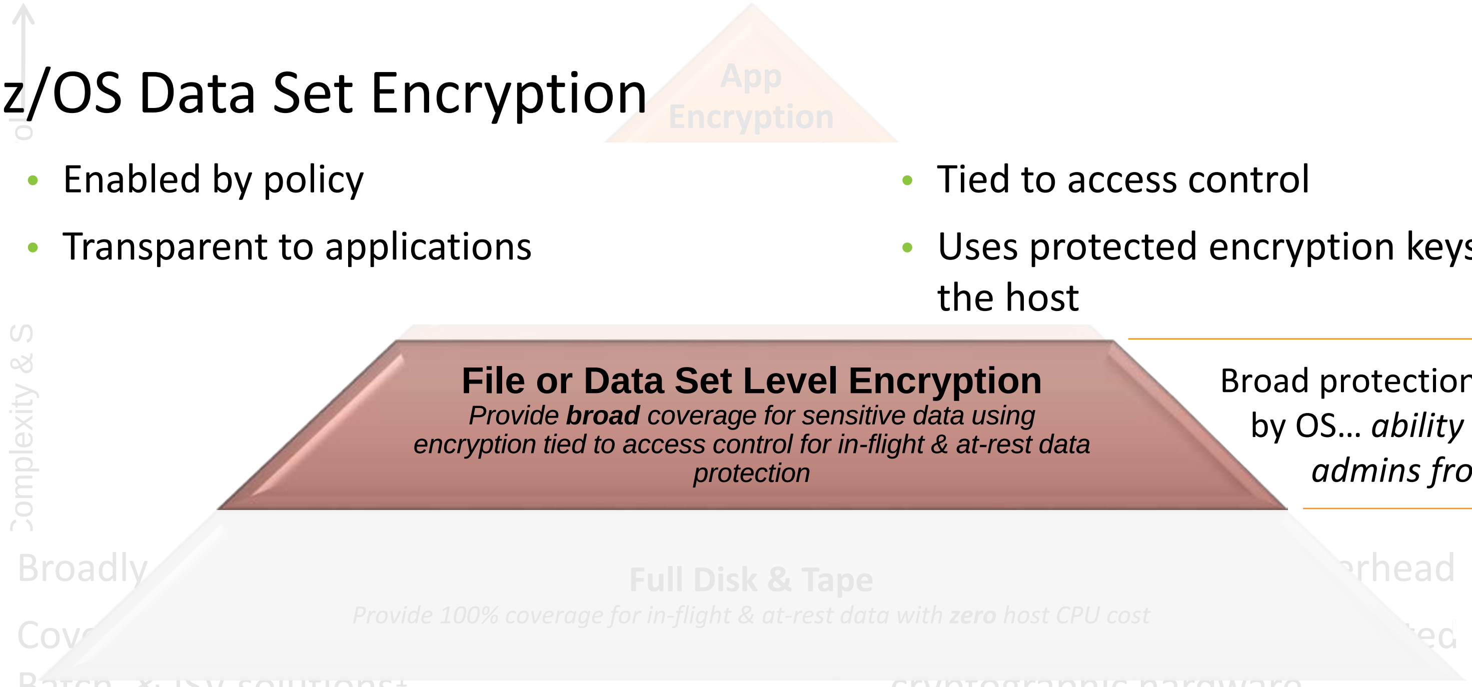
Protection against intrusion, tamper or removal of *physical* infrastructure

Multiple layers of encryption for data at-rest

Robust data protection

z/OS Data Set Encryption

- Enabled by policy
- Transparent to applications
- Tied to access control
- Uses protected encryption keys managed by the host



App Encryption
Complexity & S

File or Data Set Level Encryption

*Provide **broad** coverage for sensitive data using encryption tied to access control for in-flight & at-rest data protection*

Broad protection & privacy managed by OS… *ability to eliminate storage admins from compliance scope*

Full Disk & Tape
Provide 100% coverage for in-flight & at-rest data with zero host CPU cost

- Broadly
- Cov
Batch, & ISV solutions¹

erhead

ted

cryptographic hardware

of

to

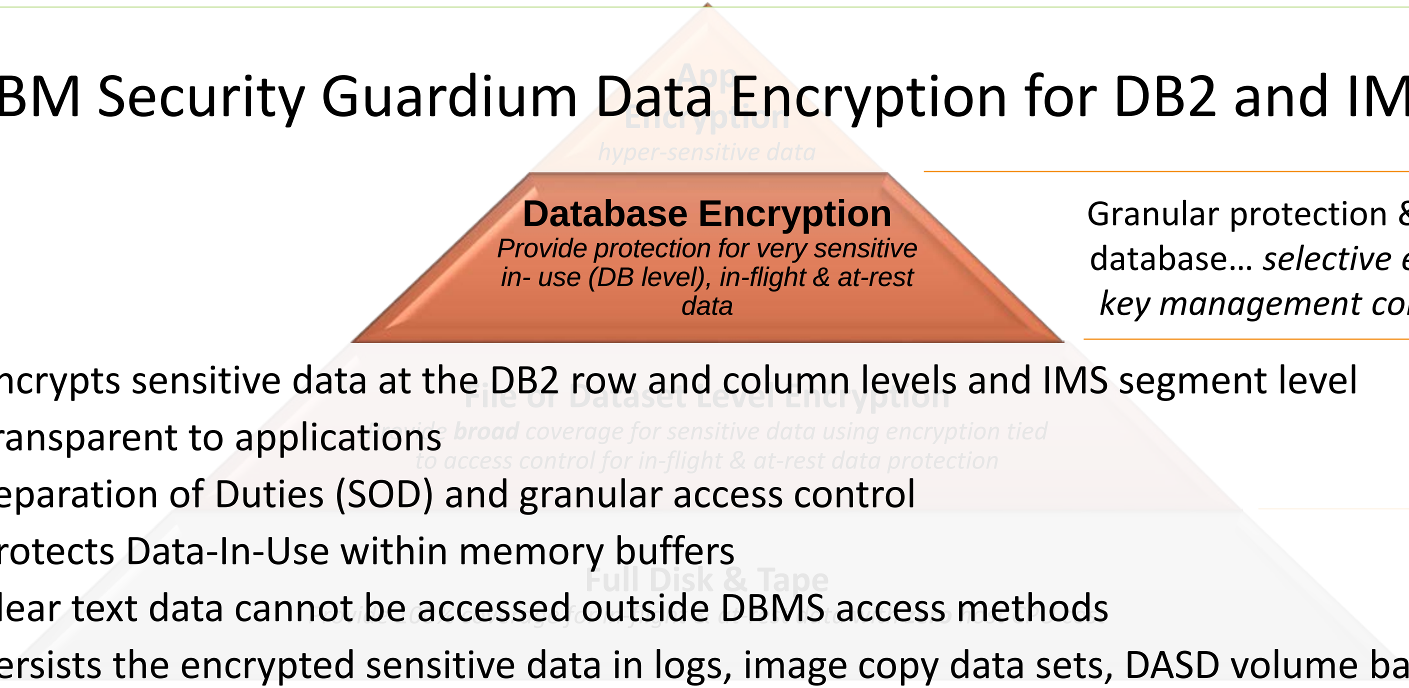
individual ISV documentation to confirm support

encryption.

Multiple layers of encryption for data at-rest

Robust data protection

IBM Security Guardium Data Encryption for DB2 and IMS Databases


App Encryption
hyper-sensitive data
File or Dataset Level Encryption
broad coverage for sensitive data using encryption tied to access control for in-flight & at-rest data protection
Full Disk & Tape

Database Encryption

Provide protection for very sensitive in- use (DB level), in-flight & at-rest data

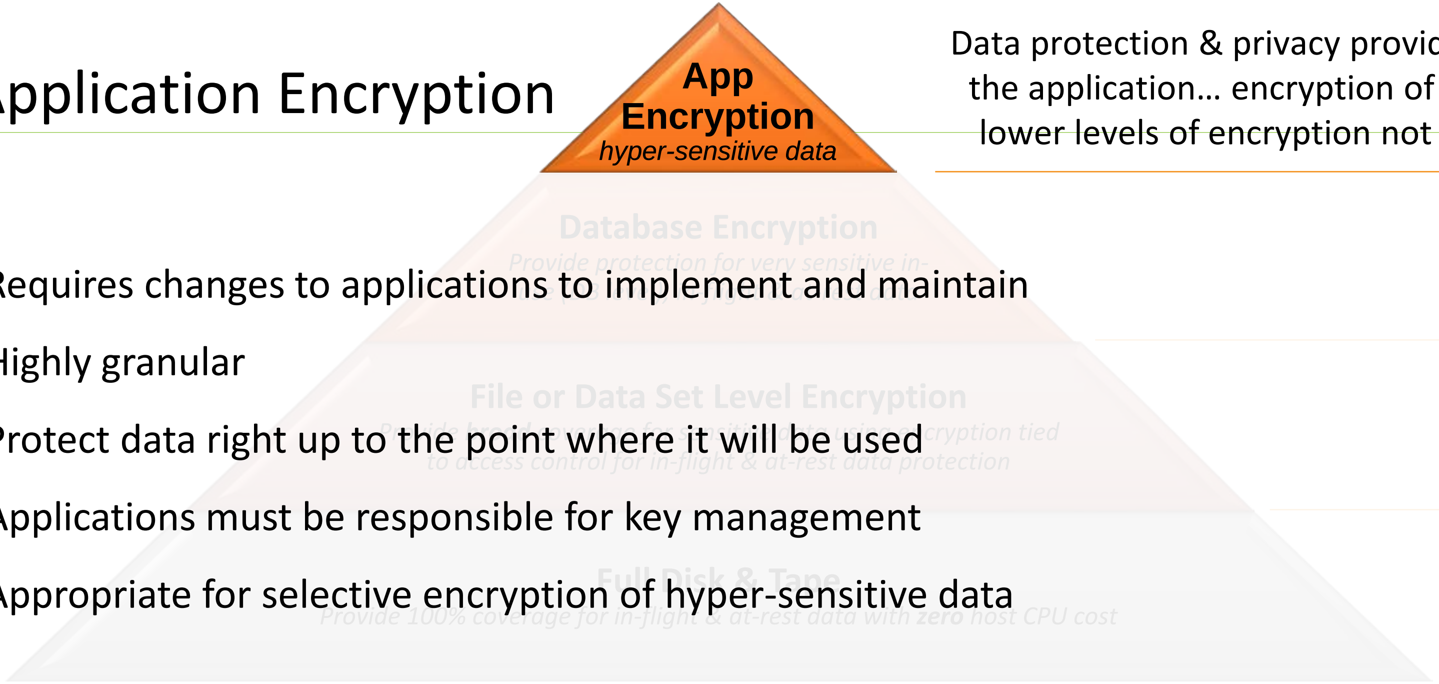
Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

- Encrypts sensitive data at the DB2 row and column levels and IMS segment level
- Transparent to applications
- Separation of Duties (SOD) and granular access control
- Protects Data-In-Use within memory buffers
- Clear text data cannot be accessed outside DBMS access methods
- Persists the encrypted sensitive data in logs, image copy data sets, DASD volume backups
- Utilizes IBM z Systems integrated cryptographic hardware

Multiple layers of encryption for data at-rest

Robust data protection

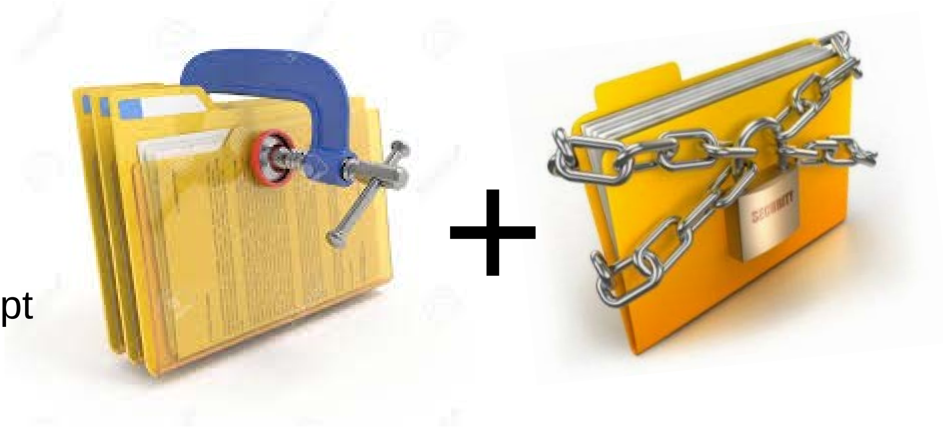
Application Encryption


App
Encryption
hyper-sensitive data
Database Encryption
Provide protection for very sensitive in-use (DB level), in-flight & at-rest data
File or Data Set Level Encryption
Provide broad coverage for sensitive data using encryption tied to access control for in-flight & at-rest data protection
Full Disk & Tape
Provide 100% coverage for in-flight & at-rest data with zero host CPU cost

Data protection & privacy provided and managed by the application… encryption of sensitive data when lower levels of encryption not available or suitable

- Requires changes to applications to implement and maintain
- Highly granular
- Protect data right up to the point where it will be used
- Applications must be responsible for key management
- Appropriate for selective encryption of hyper-sensitive data

Compression and Encryption



Encrypted data does not compress!

- Any compression downstream from encryption will be ineffective
- Where possible compress first, and then encrypt

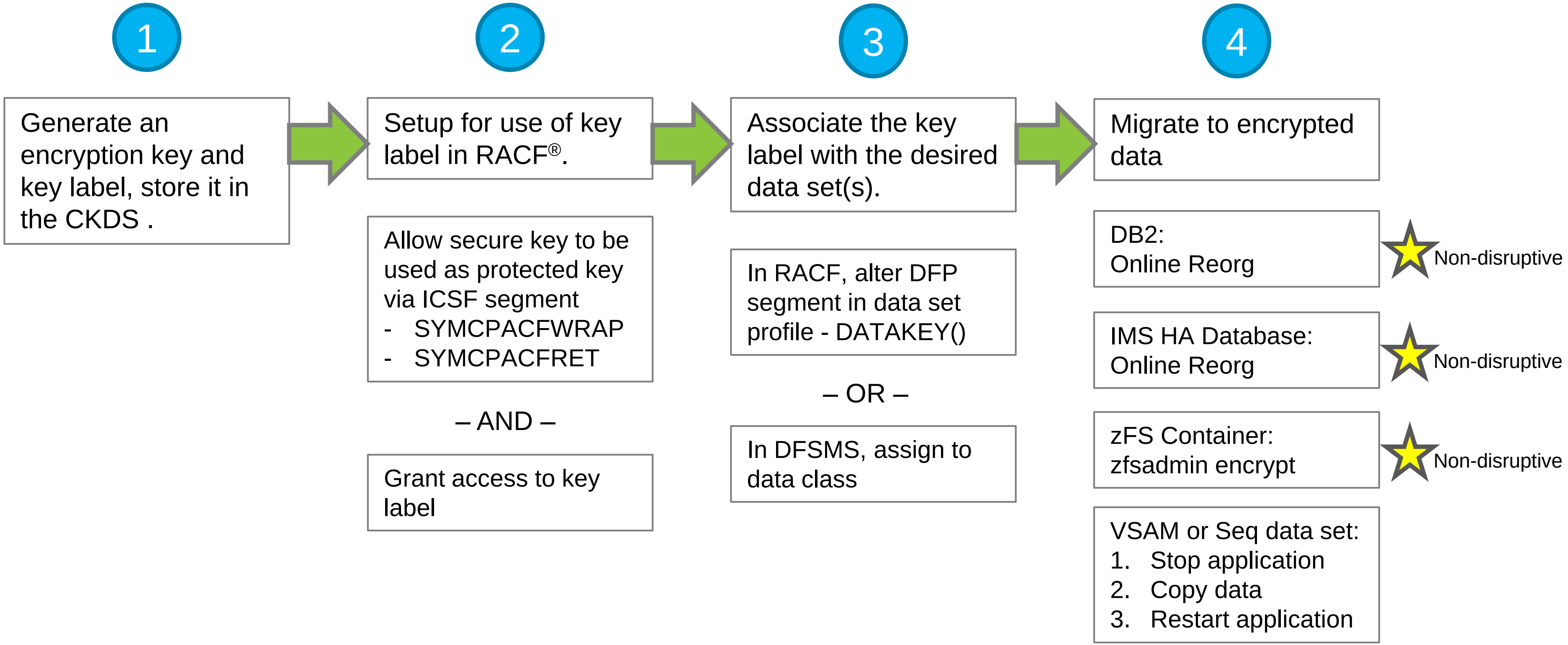
z/OS data set encryption

- DFSMS™ will compress first (generic, tailored, enhanced, and zEDC) then encrypt
- Data sets will remain encrypted during HSM and DSS migration and backup processing
- Data sets will remain encrypted during hardware based data replication services

zEDC is expected to significantly reduce the CPU cost of encryption

- Great compression ratios (5X or more for most files)
- Less data to encrypt means lower encryption costs
- Compressed data sets use large block size for IO (57K)
- Applicable to QSAM, and BSAM access methods

z/OS data set encryption – High Level Steps



1

Generate an encryption key and key label, store it in the CKDS .

2

Setup for use of key label in RACF®.

Allow secure key to be used as protected key via ICSF segment
- SYMCPACFWRAP
- SYMCPACFRET

– AND –

Grant access to key label

3

Associate the key label with the desired data set(s).

In RACF, alter DFP segment in data set profile - DATAKEY()

– OR –

In DFSMS, assign to data class

4

Migrate to encrypted data

DB2:
Online Reorg

★ Non-disruptive

IMS HA Database:
Online Reorg

★ Non-disruptive

zFS Container:
zfsadmin encrypt

★ Non-disruptive

VSAM or Seq data set:
1. Stop application
2. Copy data
3. Restart application

CF Data Encryption – High Level Steps

1. Run the policy utility (IXCMIAPU) to define a CFRM policy and specify ENCRYPT(YES) for the structures to be encrypted

2. SETXCF START the policy

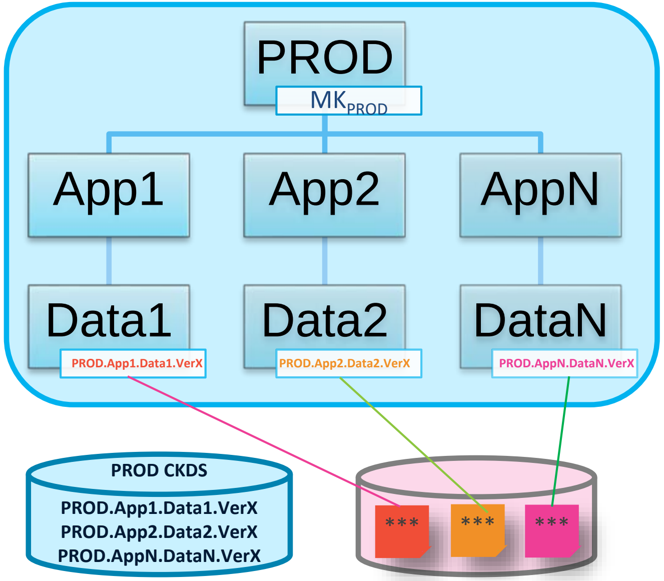
3. SETXCF REALLOCATE to get structures encrypted

4. D XCF,STR to see current encryption state of a structure

5. SETXCF MODIFY,STRNAME=strname,ENCRYPTKEY to change encryption key for selected structure(s) defined in the active CFRM policy

Naming Conventions & Granular Access Control

Leveraging naming conventions & z Security to enforce separation across application instances



- Naming conventions can be used to segment applications, data, and keys, e.g.
  – Environment: PROD, QA, TEST, DEV
  – Application: App1, App2,…, AppN
  – Data-Type: Account, Payroll, Log
- Recommend use of version # to support key rotation
  – Version: Ver1, Ver2,…,VerX
- Application resources (data sets, encryption keys) can be assigned names based on naming conventions, e.g.
  – PROD.APP2.LOG.VER10
  – PROD.APP1.PAYROLL.KEY.VER7
- Security rules can be used to enforce separation with granular access control for application resources and encryption keys

Enterprise Key Management Considerations

Encryption of data at enterprise scale requires robust key management

The current key management landscape can be characterized by clients who have …

- … already deployed an enterprise key management solution
- … developed a self-built key management solution
- … not deployed an enterprise key management solution

Key management for pervasive encryption must provide …

- Policy based key generation
- Policy based key rotation
- Key usage tracking
- Key backup & recovery

EKMF

The IBM Enterprise Key Management Foundation (EKMF) provides real-time, centralized secure management of keys and certificates in an enterprise with a variety of cryptographic devices and key stores.

IBM Key Management Landscape…

ICSF

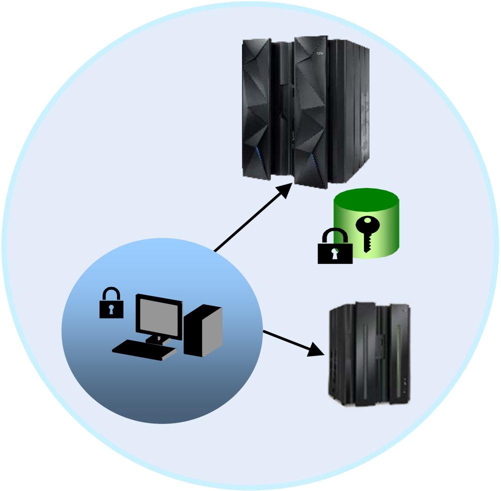
- Provides secure key storage with HSM protected keys (CKDS, PKDS, TKDS)
- Integrated with High Availability and Disaster Recovery Solutions
- Basic key *administration* primitives
- New ICSF CKDS Browser (HCR77C1)

ISKLM - IBM Security Key Lifecycle Manager

- Primarily used for serving keys to storage devices (e.g. disk, tape)
- Supports IBM Proprietary Protocol (IPP) and OASIS Key Management Interoperability Protocol (KMIP)
- Available on z and distributed platforms
- Limited ability to manage keys in z Systems hardware key stores

EKMF – IBM Enterprise Key Management Foundation

- Geared toward Banks, payment processors and other financial services
- Provides Multi-platform, multi-site & multivendor support key management
- Rich integration with Z hardware cryptography and key stores
- Robust backup and recovery capabilities
- Supports proprietary protocol for key distribution
- Delivered as a services offering

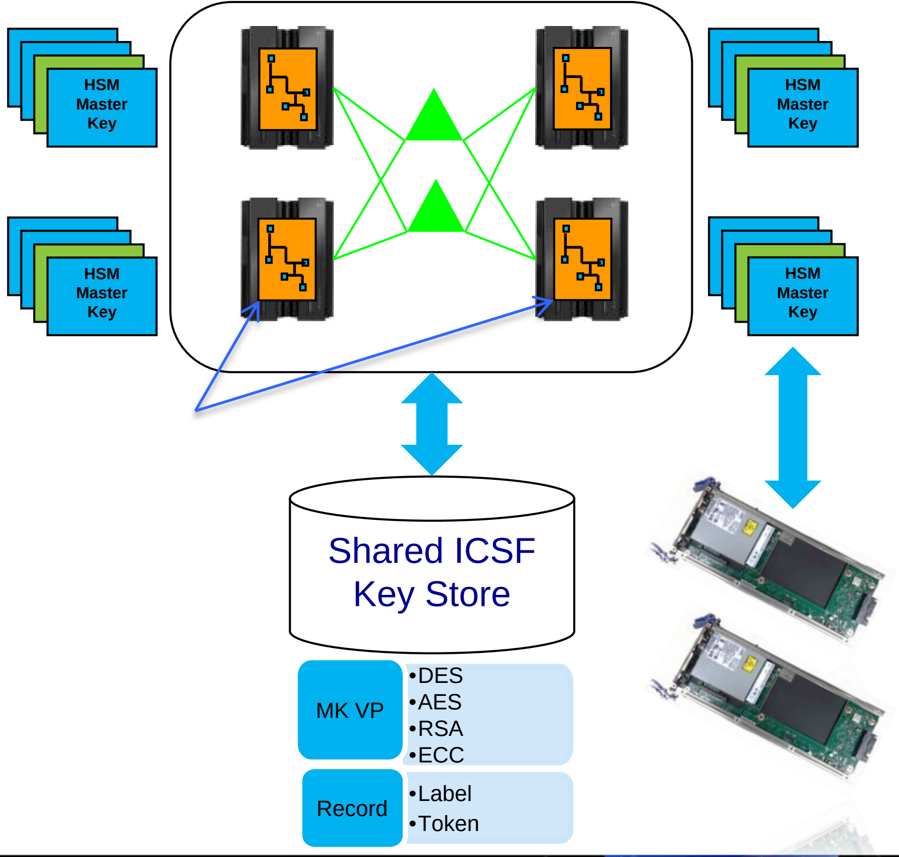


High Availability Key Management Considerations

ICSF Parallel Sysplex Enablement

z/OS ICSF can provide a *Single System Image* view by allowing key stores to be shared by all members of the sysplex.

- Enabled via SYSPLEXCKDS(YES), SYSPLEXPKDS, SYSPLEXTKDS
- Wrapped keys cached in-memory for fast access.
- Updates are automatically propagated across the sysplex (via signaling) to maintain cache coherency.
- Key store management operations are coordinated across the sysplex
- Same Master Key must be loaded into all HSMs



HSM Master Key

HSM Master Key

HSM Master Key

HSM Master Key

Shared ICSF Key Store

MK VP
- DES
- AES
- RSA
- ECC

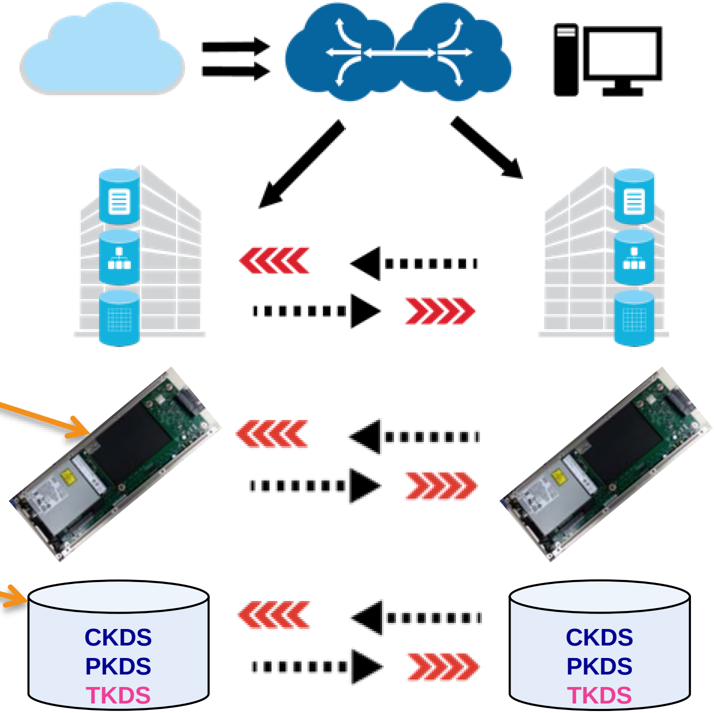
Record
- Label
- Token

Disaster Recovery Key Management Considerations

Replication of Cryptographic Key Material for Multi-Site DR Solutions

Configure and maintain both sites to run the same cryptographic workload

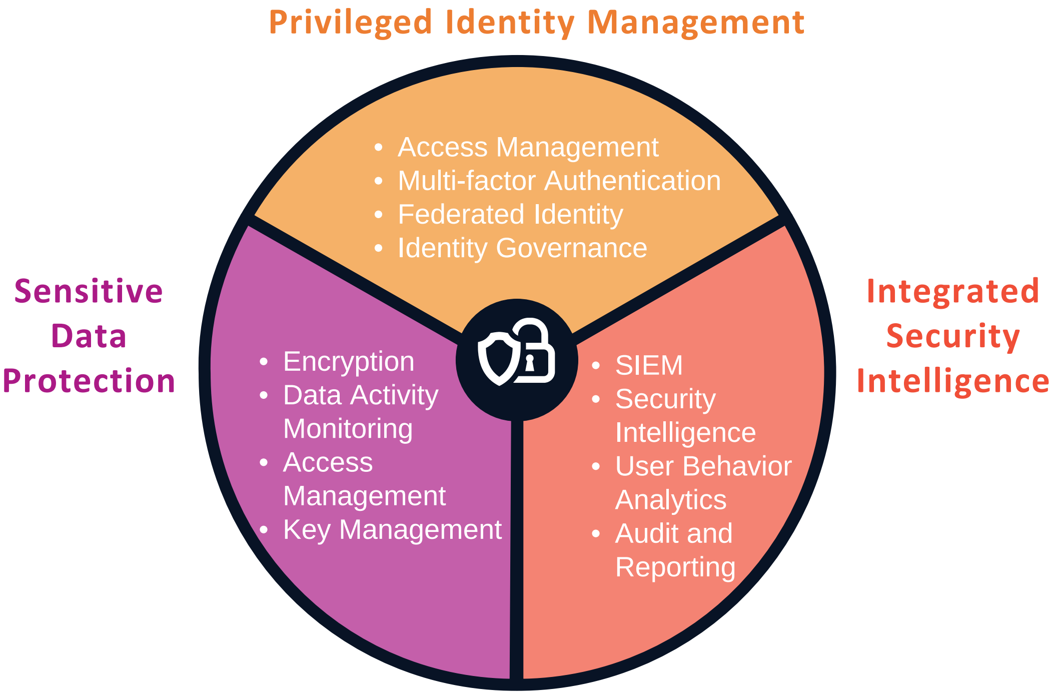
- Replicated copies of encrypted z/OS data sets will also be encrypted/protected.
- Replicate cryptographic coprocessor configurations across both sites:
  - Master Keys, access control points, etc…
  - Done at initial setup & periodic MK change
  - Can be simplified with TKE domain groups
- Replicate cryptographic key material across both sites:
  - Define ICSF Key Store datasets on replicated volumes



Supports Multi-site ***Disaster Recovery*** Solutions. *e.g. GDPS PPRC, XRC, GM, MGM, etc...*

Protecting data at the core of the enterprise

Encryption is the solid foundation of a layered cybersecurity strategy



Privileged Identity Management

- Access Management
- Multi-factor Authentication
- Federated Identity
- Identity Governance

Sensitive Data Protection

- Encryption
- Data Activity Monitoring
- Access Management
- Key Management

Integrated Security Intelligence

- SIEM
- Security Intelligence
- User Behavior Analytics
- Audit and Reporting

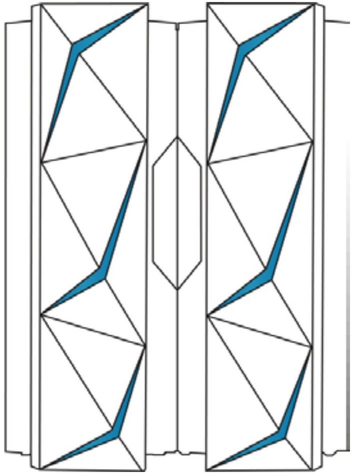
Traditional workloads and APIs:

- DB2
- IMS
- CICS / VSAM
- MQ

Key Security Solutions:

- IBM Security zSecure™ Suite
- IBM Security Qradar®
- IBM Security Guardium® Family
- IBM Multi-factor Authentication
- IBM Security Identity Governance
- Enterprise Key Management

IBM z14: Designed for Trusted Digital Experiences



Pervasive Encryption is the new standard

Analytics & Machine Learning for Continuous Intelligence Across the Enterprise

Open Enterprise Cloud to Extend, Connect and Innovate

Container Pricing For IBM Z provides new flexibility for modern digital workloads

IBM Z pervasive encryption Backup - Use Cases

Encrypt data in core business applications

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

NEWS

582.9M

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

TODAY

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

WITH z14

- Encrypt 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

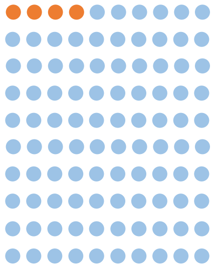
"We know we need to encrypt this,
...but we can't."
"We don't want to do this,
...but don't have a choice"

User Feedback

"Can you get it to us sooner? Can you make it happen sooner?"
"As soon as the code is available, we want it"

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 9 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.

WITH z14

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

User Feedback

"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 reside on lower cost cloud storage
- Gaps in current encryption via cloud storage solutions has gaps, does not protect data end-to-end, and introduces additional complexities with management of encryption keys

WITH z14

- 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

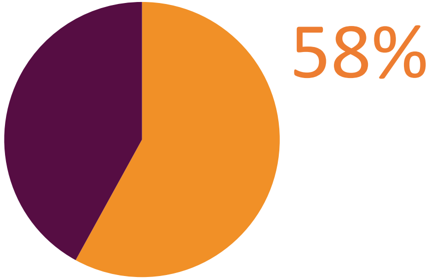
“We generate a lot of log files that we have to store each year…”

User Feedback

“That would be perfect. That’s what we would like to be able to do.”

Reduce 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.



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.

WITH z14

- z14 enables encryption by policy tied to access control
- Separate access control to data sets and encryption keys providing separation of duties — *eliminate entire classes of users from compliance scope*

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

User Feedback

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

Meet audit and compliance obligations

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

$4M

Average cost of a data breach in 2016

TODAY

- Organizations are faced with multiple audits per year - internal, external, client…a state of near continuous audit

WITH z14

- With Pervasive Encryption, organizations no longer have to encrypt only data for compliance, and can encrypt all application/database data
- z14 provides solutions for both application teams and auditors to verify up-to-date compliance stats in near real-time

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

User Feedback

“It’s simple to demonstrate compliance, and we know what’s coming well before the audit happens.”

IBM Z pervasive encryption
Backup - Software Rollout

z/OS Data Set Encryption

Hardware and Operating System Support

Product/Feature	Required Level	Description
Hardware		
Minimum HW	z196 CPACF	Minimum HW for AES-XTS (MSA-4)
	Crypto Express3	Minimum HW for Secure-key/Protected-key CPACF[1]
Recommended HW	z14 CPACF	AES-XTS CPACF performance improvements
	z14 Crypto Express6s	Crypto express performance improvements
Operating System – Base Support		
DFSMS	z/OS 2.3	Full support
	z/OS 2.2 + OA50569 PTFs	
	z/OS 2.1 + OA50569 PTFs	*Toleration only –read/write, cannot create encrypted data sets.*
RACF	z/OS 2.3	DFP segment key label and conditional access checking
	z/OS 2.1, 2.2 + OA50512 PTFs	
ICSF	HCR77C0 or HCR77C1	Protected-Key Read
	HCR77A0–B1 + OA50450 PTFs	

[1] *– Secure-key is STRONGLY RECOMMENDED for production environments. Clear-key may be used for dev/test.*

z/OS Data Set Encryption

Exploitation

Product/Feature	Required Level	Description
Software Exploitation		
DB2	DB2 v12 + PTFs	Base exploitation + user interface enablement
	DB2 v11 + PTFs	Base exploitation
IMS	IMS v14	FF VSAM DB & OLDS - *test only no code changes expected*
	IMS v15	FP DEDB VSAM & WADS enablement support
CICS	*Supported CICS versions*	Test-only for user, CICS TS, and TD data sets
MQ	*NA*	*Recommendation for MQ - Advanced Message Security*
zSecure	zSecure 2.3	zSecure Audit & Admin support for z/OS data set encryption
zBNA	zBNA x.y.z	zBatch Network Analyzer support for z/OS data set encryption
z/OS Exploitation		
zFS	z/OS 2.1 & 2.2	Toleration support
	z/OS 2.3	User Interface & data conversion support
System Logger	z/OS 2.3 w/RB 2.2 & 2.1	Media Manager enablement for logger data sets

CF Encryption

Hardware and Operating System Support

Product/Feature	Required Level	Description
	Hardware	
z/OS: Minimum HW	zEC12	Minimum supported for z/OS 2.3
	Crypto Express3	Required for Protected-key CPACF
z/OS: Recommended HW	z14 CPACF	AES-CBC CPACF performance improvements
CF: Recommended HW	z14 CF	Simplified recovery for specific sysplex-wide recovery scenarios
	Operating System – Base Support	
z/OS	z/OS 2.3	z/OS support for CF encryption
	Exploitation	
zSecure	zSecure 2.3	zSecure Audit support for CF encryption
zBNA	zBNA x.y.z	zBatch Network Analyzer support for CF encryption

z/OS Communications Server

Hardware and Operating System Support

Product/Feature	Required Level	Description
Hardware		
Recommended HW	z14 CPACF	AES-GCM CPACF performance improvements
Operating System – Base Support		
z/OS Comm Server	z/OS 2.3	Provides zERT function
z/OS Exploitation		
System SSL	z/OS 2.3	zERT-enabled cryptographic protocol provider
OpenSSH	z/OS 2.3	zERT-enabled cryptographic protocol provider
Software Exploitation		
Connect:Direct	z/OS 2.3 + PTFs	Exploits SIOCSHSNOTIFY ioctl
zSecure	*TBD*	*Working with zSecure to be a consumer of zERT SMF records*
ISV Support		
ISVs	*As required by ISV*	*ISV enablement/compatibility support*

Thank you

ZSP04731USEN-00