IBM z14

Data Protection for the Digital Enterprise

Nick Sardino – sardino@us.ibm.com
IBM Z Offering Management

IBM Z

you IBM

Trademarks

* Registered trademarks of IBM Corporation

CICS*	IBM*	IMS	z14
DB2*	IBM (logo)*	QRadar*	zSecure
Guardium*	IBM Z	z13*	z/OS*

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 Security Leadership

Designed for the next generation of secure, trusted transactions

Privileged Identity Management

Govern, protect, and audit users with elevated privileges to prevent unauthorized access to sensitive data by rogue insiders or external attackers using compromised administrator credentials

81% Less effort required to secure equivalent workloads

Sensitive Data Protection

Defend and protect critical assets with unrivaled encryption and intelligent data monitoring –all without compromising transactional throughput or response time

Greater than **8.5x** more effective at resisting security threats

Integrated Security Intelligence

Correlate huge amounts of security data to uncover patterns of unusual activity, use real-time alerts to immediately focus on critical security threats that matter the most to the business

93% Lower cost for security defense

Source: *Pervasive Encryption, A New Paradigm for Protection* -- https://ibm.biz/BdjjYf

Data protection and compliance are business imperatives

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

28%

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)

$3.6M

Average cost of a data breach in 2017 [2]

Of the **9 Billion** records breached since 2013 only **4%** were encrypted [3]

Health Insurance Portability and Accountability Act (HIPAA)

1, 2 Source: 2017 Ponemon Cost of Data Breach Study: Global Overview -- http://www.ibm.com/security/data-breach/
3 Source: Breach Level Index -- http://breachlevelindex.com/

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.

A Paradigm Shift in Data Protection

From selective encryption to pervasive encryption

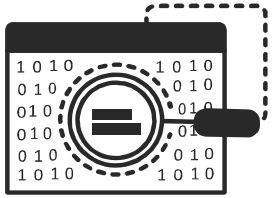
Protecting only the data required to achieve compliance should be viewed as a minimum threshold, not a best practice.

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

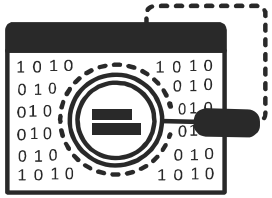
Unrivaled Data Protection

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

No Application Changes

No Impact to SLAs

IBM z14



All application and database data

Protect all application and database data according to enterprise security policy using encryption **without interrupting business applications and operations.**

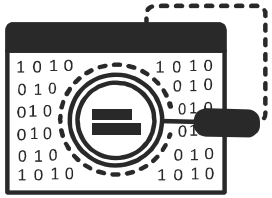
Blazing fast hardware-accelerated encryption on every core is **up to 7x faster than IBM z13® and 2.5x faster than x86.**

Bulk encryption enabled in the Operating System for:

- **Simple implementation**
- **Transparent exploitation**
- **Optimized performance**

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

IBM z14



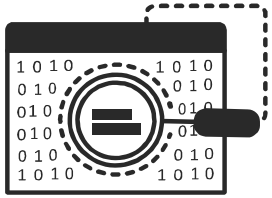
All in-flight network data and APIs

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



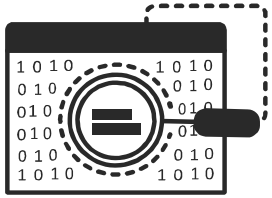
All encryption keys protected

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 ensures **encryption keys are never exposed** to the OS, hypervisor, or application in the clear.

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.

Pervasive Encryption with IBM Z

Enabled through tight platform integration

Integrated Crypto Hardware		Hardware accelerated encryption on every core, CPACF performance improvements of 7x Crypto Express6S – PCIe Hardware Security Module (HSM) & Cryptographic Coprocessor
Data at Rest		Broadly protect Linux file systems and z/OS data sets using policy controlled encryption that is transparent to applications and databases
Clustering		Protect z/OS Coupling Facility 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 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 …

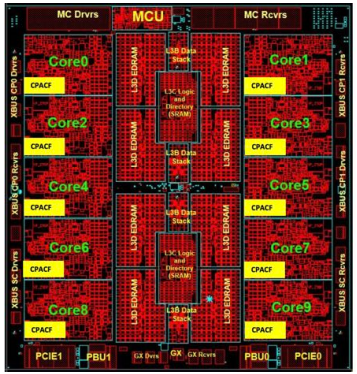
z14 Integrated Cryptographic Hardware

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



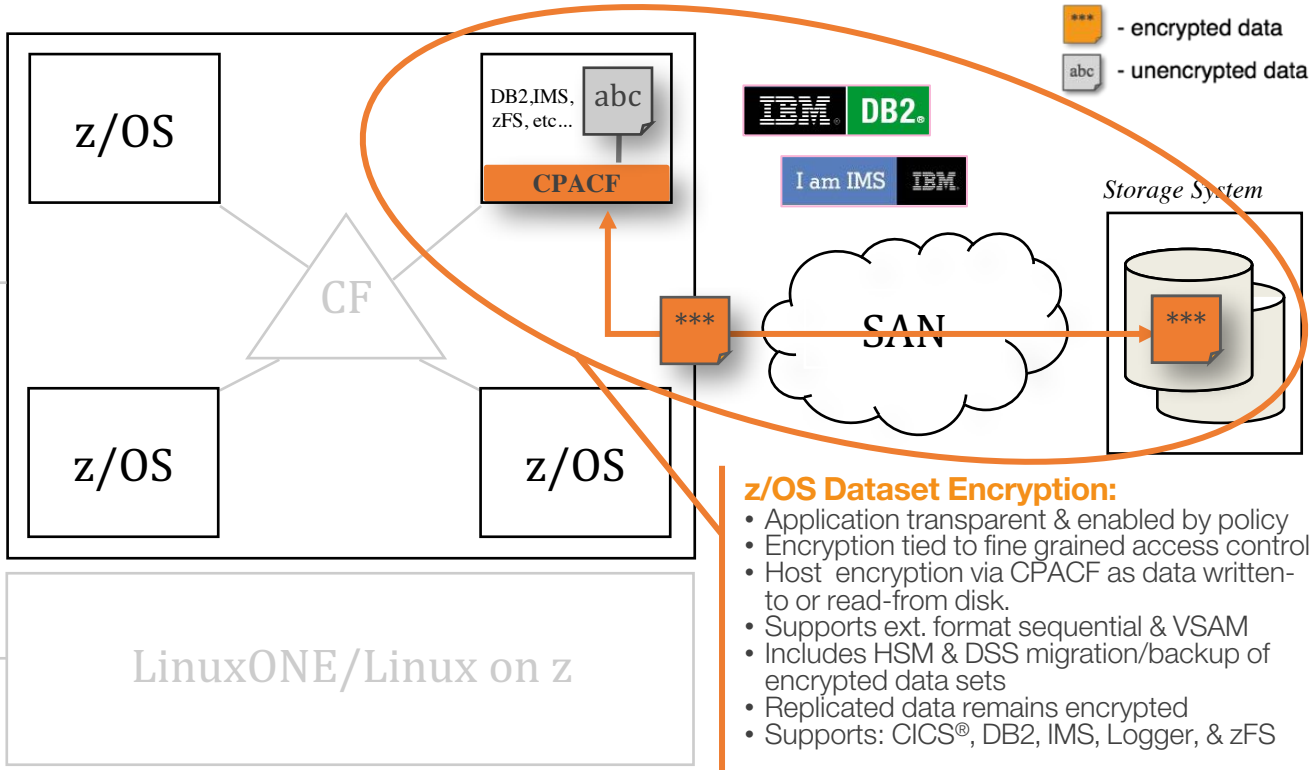
Why is it valuable:

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

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

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

Data Protection // Coupling Facility Encryption

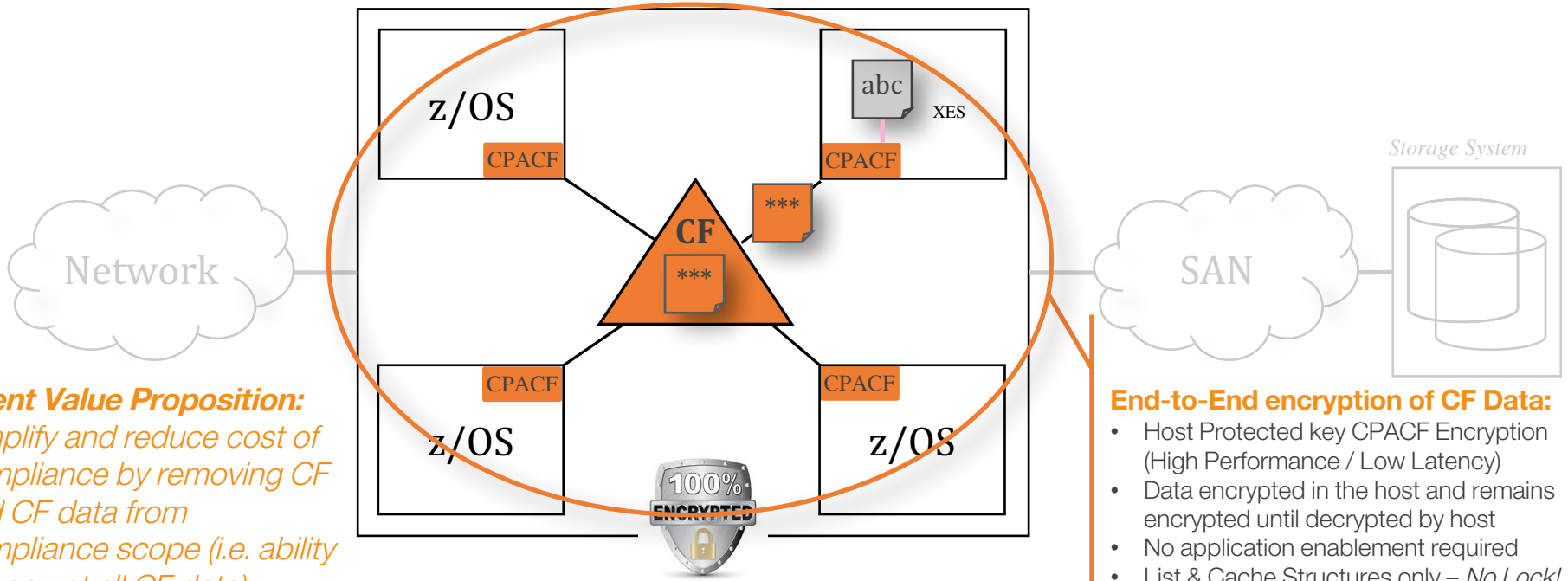
Protection of data in-flight and in-use (CF)

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

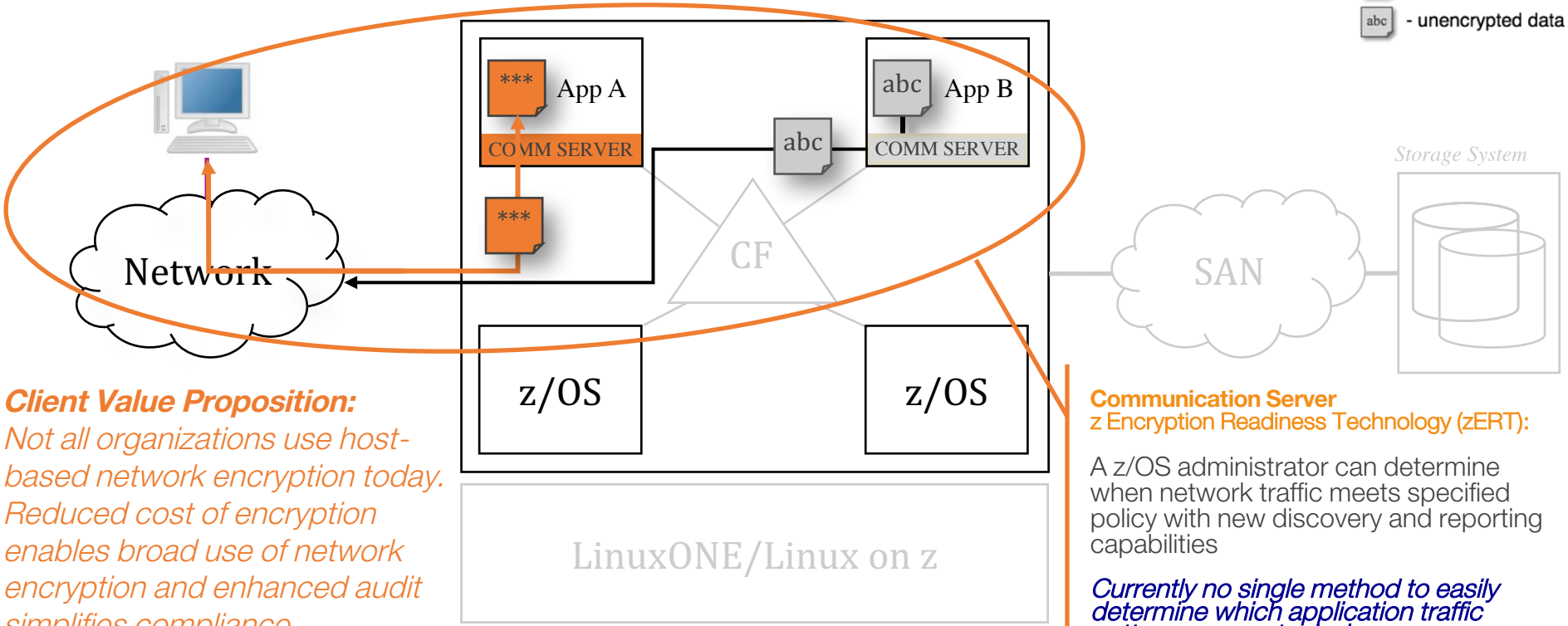
Protection of data in-flight

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

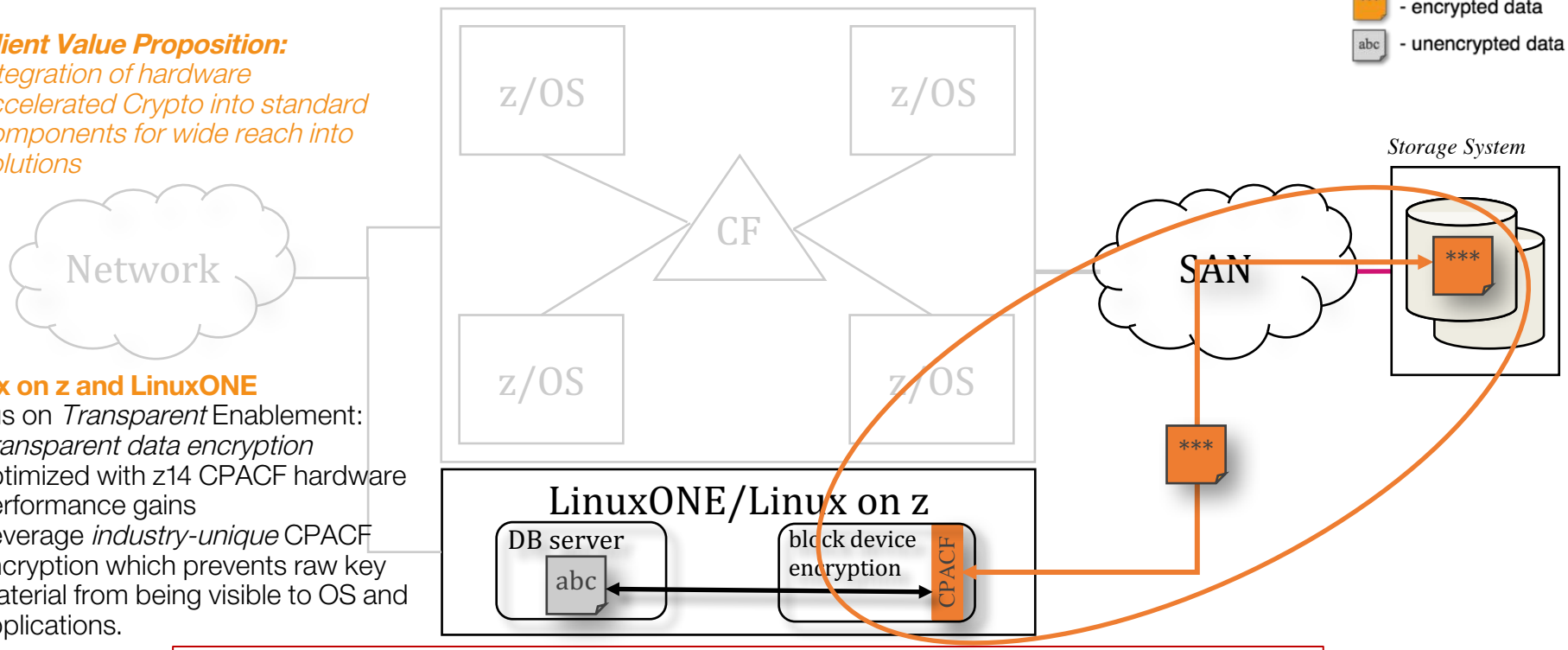
Currently no single method to easily determine which application traffic patterns are protected

Data Protection // Linux on z File Encryption

Protection of data at-rest

Submitted Upstream

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

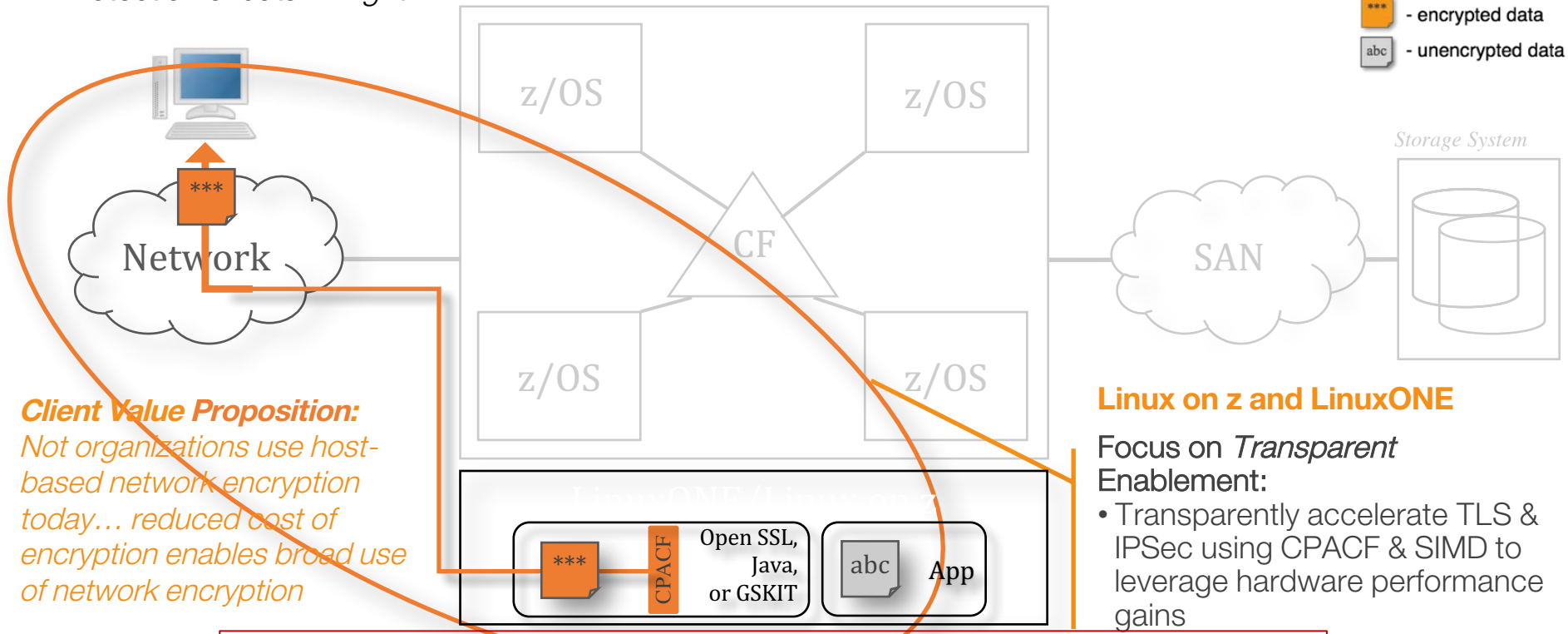
Protection of data in-flight

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:

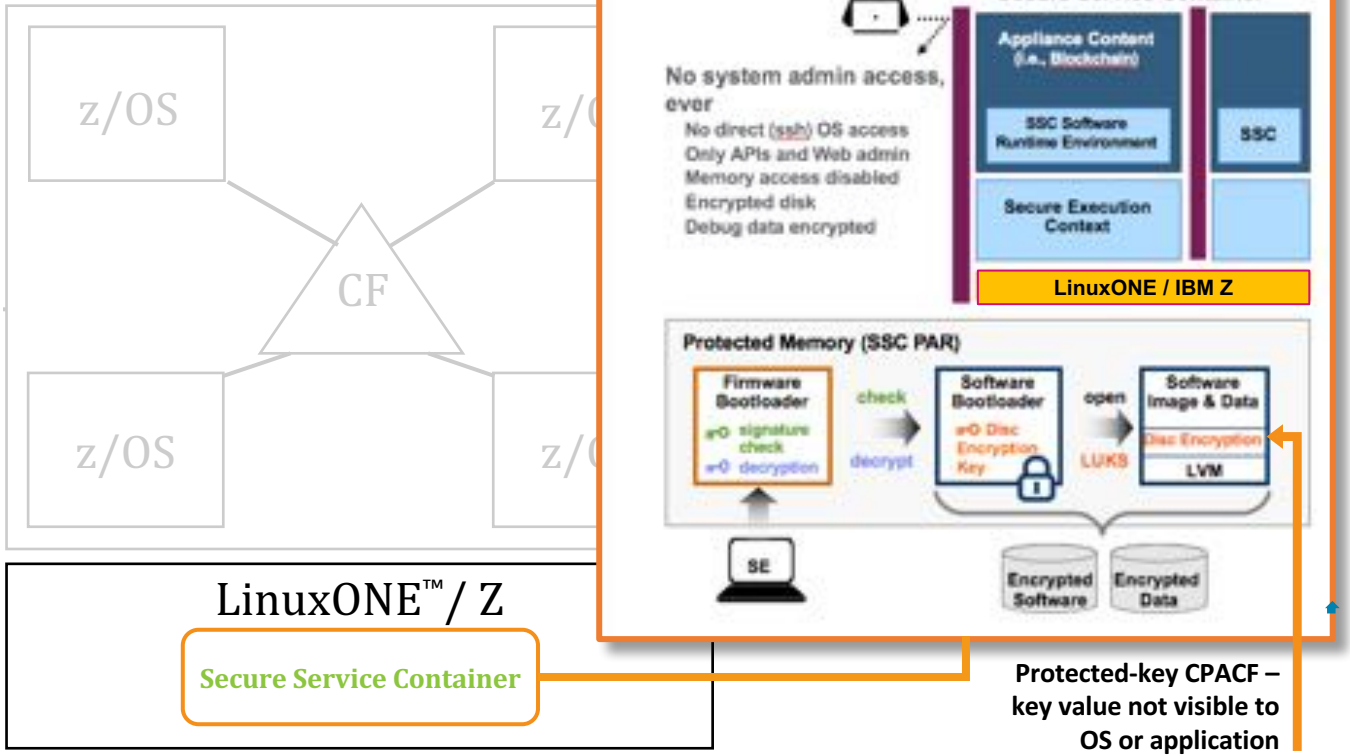
Simplified, fast deployment and management of packaged solutions

Tamper protection during Appliance installation and runtime

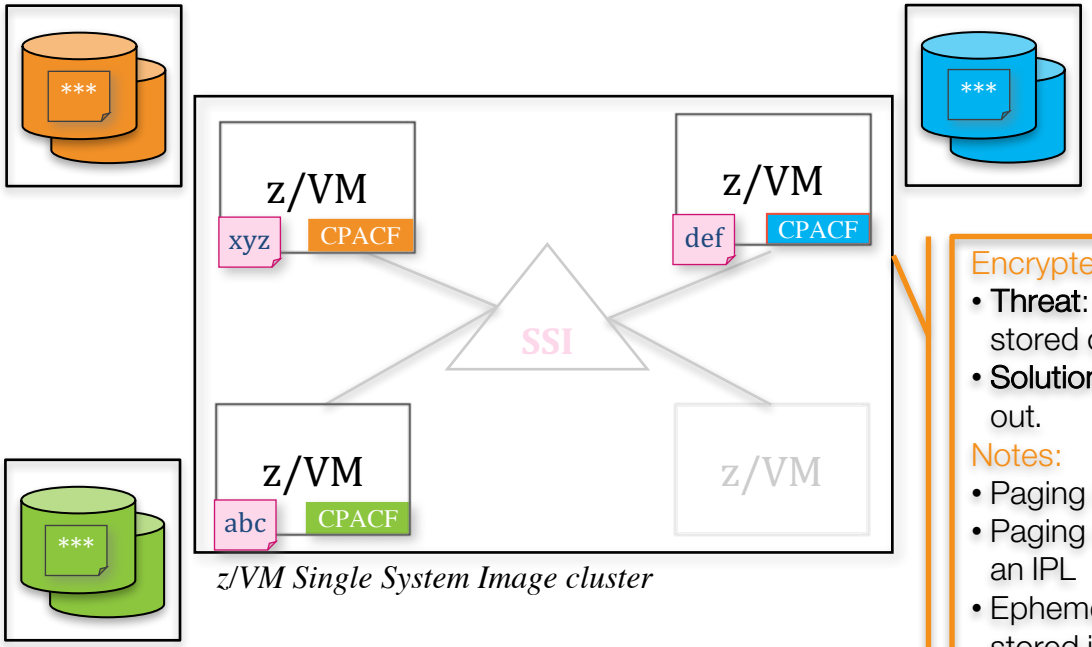
Confidentiality of data and code running within the Appliance both at flight and at rest

Restricts administrator access to workload and data

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



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

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)

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

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

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

- Broadly encrypt data at rest
- Covers VSAM, DB2, IMS, Middleware, Logs, Batch, & ISV solutions[1]
- Encrypt in bulk for low-overhead
- Utilizes IBM Z integrated cryptographic hardware

1 Applications or middleware making use of VSAM, QSAM, BSAM access methods. Refer to individual ISV documentation to confirm support of z/OS data set encryption.

Multiple layers of encryption for data at rest

Robust data protection

IBM Security Guardium Data Encryption for DB2 and IMS Databases

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 integrated cryptographic hardware

Multiple layers of encryption for data at rest

Robust data protection

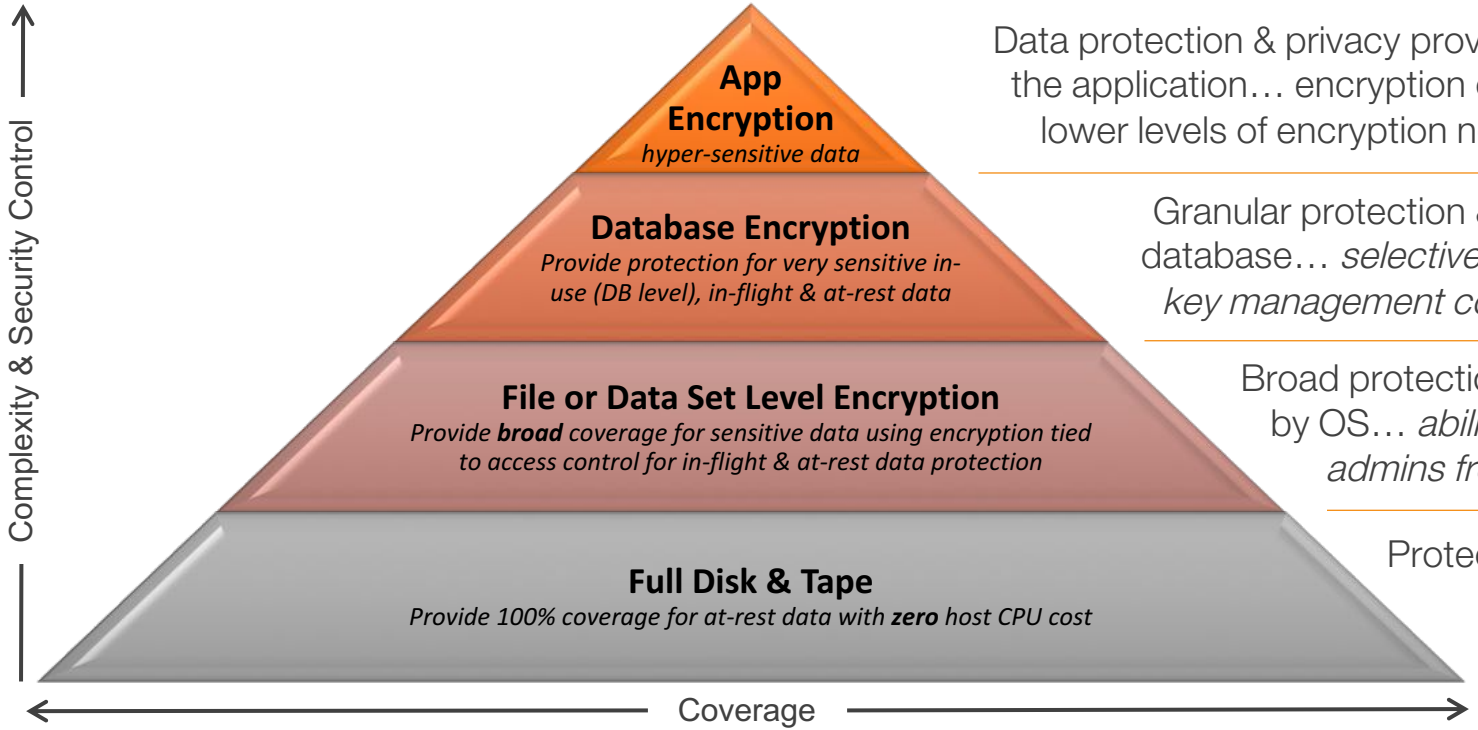
Application Encryption

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

Multiple layers of encryption for data at rest

Robust data protection



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

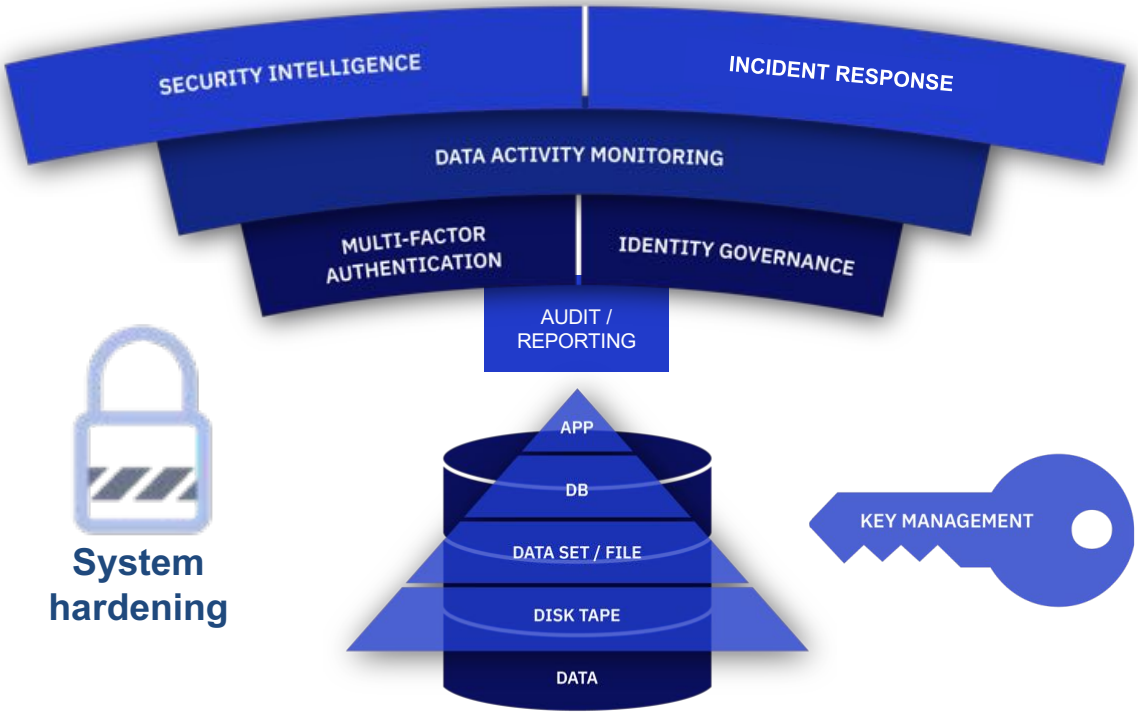
Granular protection & privacy managed by database… *selective encryption & granular key management control of sensitive data*

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

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

Protecting data at the core of the enterprise

Encryption is the solid foundation of a layered cybersecurity strategy



Traditional workloads and APIs:

- DB2
- IMS
- CICS / VSAM
- MQ

Relevant IBM Security Solutions:

- IBM Security zSecure Suite
- IBM Security QRadar
- IBM Security Guardium Family
- IBM Multi-factor Authentication
- IBM Security Identity Governance
- Enterprise Key Management

Enterprise key management

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.

zSecure 2.3 Pervasive Encryption Support

Command Verifier: Command Verifier policy for DATAKEY

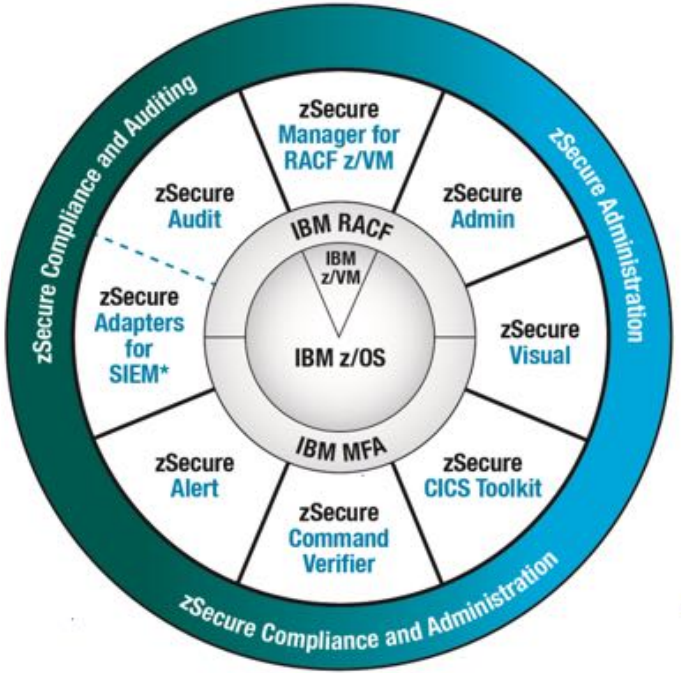
Admin: Easy administration DATAKEY on DFP segment

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



IBM Multi-Factor Authentication for z/OS

Higher assurance authentication for IBM z/OS systems that use RACF

IBM Multi-Factor Authentication on z/OS provides a way to **raise the assurance level** of z/OS, applications, and hosting environments by extending RACF to authenticate users with multiple factors.

- Support for third-party authentication systems
  - RSA® Ready supporting RSA SecurID® Tokens (hardware & software based)
  - IBM TouchToken – Timed One Time use Password (TOTP) generator token
  - PIV/CAC and Smart cards – Commonly used to authenticate in Public Sector enterprises
- Tightly integrated with SAF & RACF

TECHNOLOGY RSA READY PARTNER

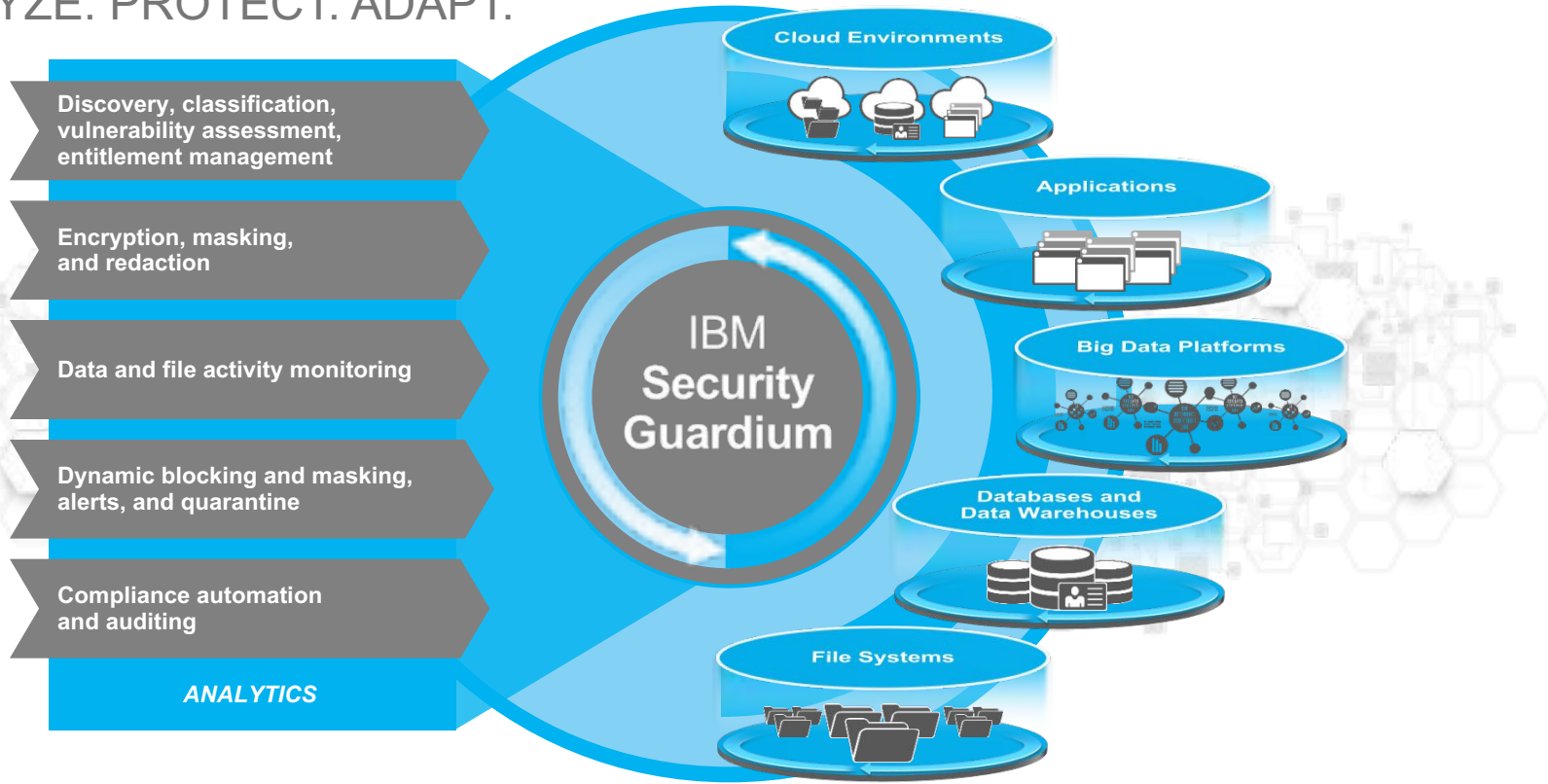
Fast, flexible, deeply integrated, easy to deploy, easy to manage, and easy to use

PCI-DSS
Achieve regulatory compliance, reduce risk to critical applications and data

Architecture supports multiple third-party authentication systems at the same time

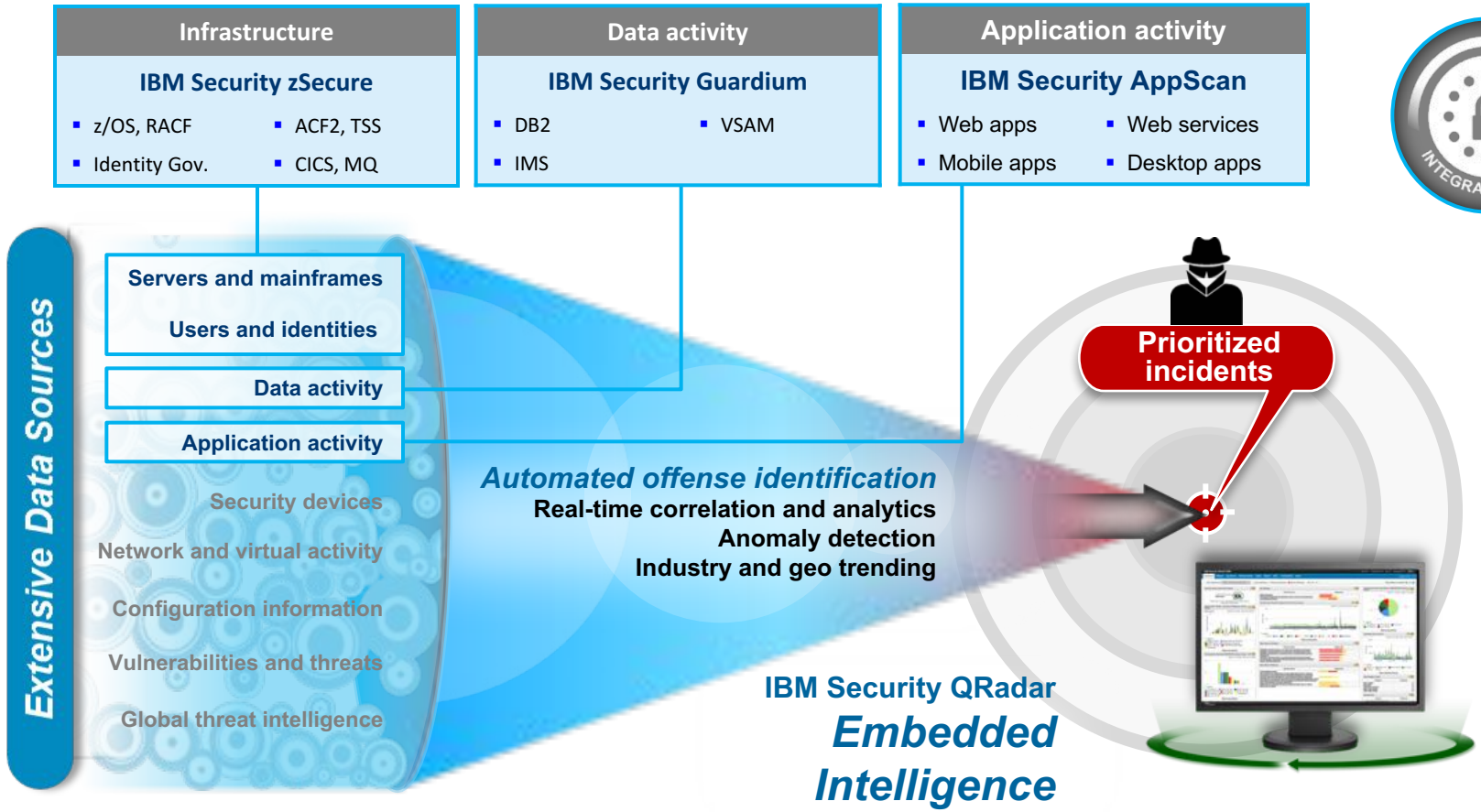
IBM Security Guardium

ANALYZE. PROTECT. ADAPT.



Highly optimized for IBM Z to meet the aggressive transactional throughput and SLAs of enterprise applications

Integrated Security Intelligence with IBM z



Use cases

Protect 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 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 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

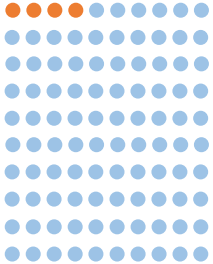
"We know we need to encrypt this, …but we can't."
"We don't want to do this, …but don't have a choice"

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

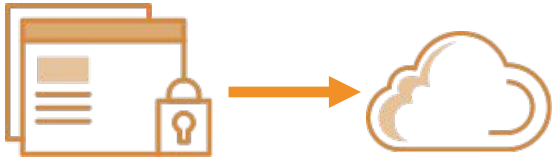
"We recognize this is sensitive, but there are limitations to our technology…"

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 IBM Z host, reducing the risk

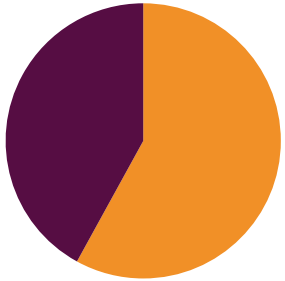
"We generate a lot of log files that we have to store each year…"

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.



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.

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.

$3.6M

Average cost of a data breach in 2017

TODAY

- Experiencing an average of 50 audits per year, a "revolving door" of auditors - internal, external, clients…a state of perpetual 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."

Thank you

Nick Sardino
IBM Z Offering Management

Michael Jordan
IBM Distinguished Engineer, IBM Z Security

IBM Z

you IBM

z/OS Data Set Encryption - Getting Started

- Choose an application
- Prepare test environment
- Enable encryption (4 steps)
- Test & verify
- Plan for production rollout

Pervasive encryption client advocacy program

z/OS Data Set Encryption – Choose an application

Questions:

- Is your enterprise driving a tops down encryption initiative?
  - e.g. GDPR, PCI DSS, etc..
- What do you expect to be the first use case for data set encryption?

- CICS/VSAM application
- DB2 database
- IMS database
- Batch workload
- Log data sets (system logger)

z/OS Data Set Encryption – Prepare test environment

- Hardware
  - CPACF protected key (z196 or later for AES-XTS mode)
  - Crypto Express3 or later required for secure key
  - Recommend use of Crypto Express in test to validate crypto operational procedures (e.g. master key loading, master key change, etc…)
- Setup & Configure ICSF
  - Load AES master key
  - Recommend installing latest ICSF web deliverable (HCR77C1)
    (Can generate AES DATA keys using CKDS Browser)
- Install/Update Base Software
  - DFSMS - z/OS 2.2 + service or z/OS 2.3
  - RACF – z/OS 2.2 + service or z/OS 2.3
  - ICSF – HCR77A0-B1 + service or HCR77C0-C1
- Install/Update Exploitation Software
  - DB2, IMS, logger… vendor products?

Questions:

- Do you currently have Crypto Express feature in your environment?
  - prod? dev? test?
- Do you have Master Keys loaded in Crypto Express?
- Is anyone still running z/OS 2.1 or earlier?

z/OS data set encryption – Enable Encryption (4 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

https://www.youtube.com/watch?v=zdSXRUSmkb4

Hands On PoT

https://ibm.biz/client-experience-portal

z/OS Data Set Encryption – Plan for production rollout

Questions:

- Is ICSF environment configured for Parallel Sysplex?
- Is ICSF environment configured for DR?
- Is an Enterprise Key Management system deployed?

- Configure ICSF & key store for high availability
- Configure ICSF & key store for DR
- Configure periodic logical back up of key store
- Deploy Enterprise Key Management system for backup & recovery
- Consider use of host based compression
- Plan key label naming convention and access control
- Evaluate encryption overhead

Recommended z14 Features for Pervasive Encryption

1. zEDC
   - Compression for sequential data
2. Crypto Express6s
   - Protection of keys stored in CKDS
3. Trusted Key Entry Workstation (TKE)
   - Secure Master Key loading – root of trust

---

4. Enterprise Key Management Foundation (EKMF)
   - Robust key management

Pervasive Encryption Readiness Assessment

IBM Systems Lab Services

Overview

The vision of Pervasive Encryption is to provide a simple, transparent, and consumable approach to enable extensive encryption of data in-flight and at-rest to substantially reduce the costs associated with protecting data and achieving compliance mandates. All clients, when time comes to implementation, will have a lot of questions, like about the different components involved or how to manage the encryption keys and will need deep insights to prepare their environment to this critical step into the best of IBM Z or LinuxONE security. This offering will help them to assess their current state, and give them the path and deep insights to prepare their environment.

Target Audience

All clients who envision to enable pervasive encryption on their IBM Z or LinuxONE environments.

Benefits

Based on a short interview about their current z Systems enabled features and pervasive encryption objectives, the client will know what are the steps they still have to take to be ready for pervasive encryption. They will get deep insights by the IBM Lab Services consultant, from the components they will need to configure to what are the best practices in terms of key management on z systems.

Qualifying Questions

- Do you have clients who are planning to implement pervasive encryption ?
- Do you have clients who don't know where to start and what to do for pervasive encryption ?
- Do you have clients who don't know how to manager their keys on IBM Z ?

Key Features

- Review of the current state toward pervasive encryption.
- Identification of the steps to take to start pervasive encryption.
- Overview of the best practices in key management on IBM Z and LinuxONE

Deliverables

Summary presentation about readiness and key management best practices.

Duration

24-60 hours depending on the complexity of the client environment.

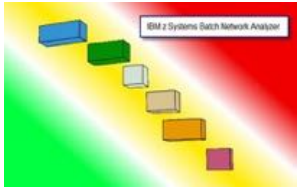
Team Contacts

Owner: Didier Andre (dandre@us.ibm.com)
IBM Sellers can find a Lab Services Opportunity Manager in your area ->
http://ibm.biz/LabServicesOM
IBM Business Partners contact us at
https://www-03.ibm.com/systems/services/labservices/contact.html

Estimating CPU Cost of Data Protection

z Batch Network Analyzer (zBNA)

zBNA 1.8.1

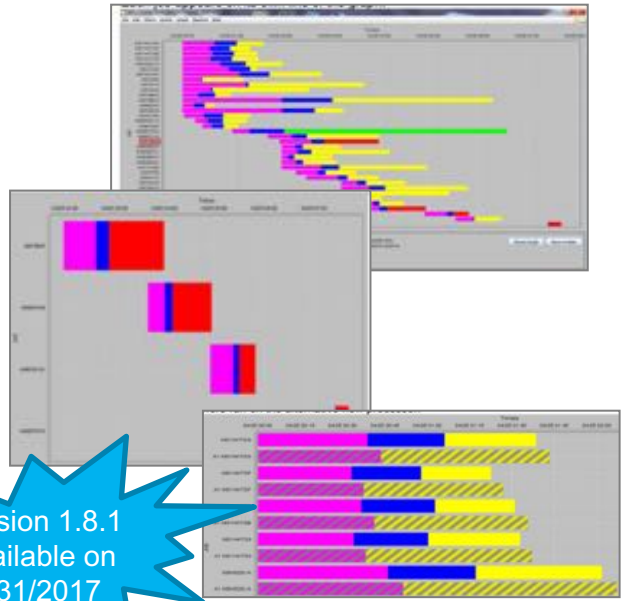


zBNA Background:

- 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

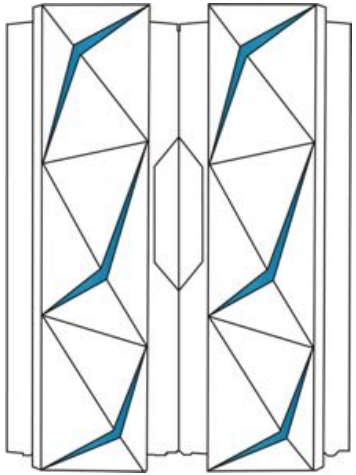
zBNA Encryption Enhancements:

- 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



Version 1.8.1 Available on 8/31/2017

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

World’s leading businesses run on the mainframe

30 billion business transactions per day

$6 trillion in card payments annually

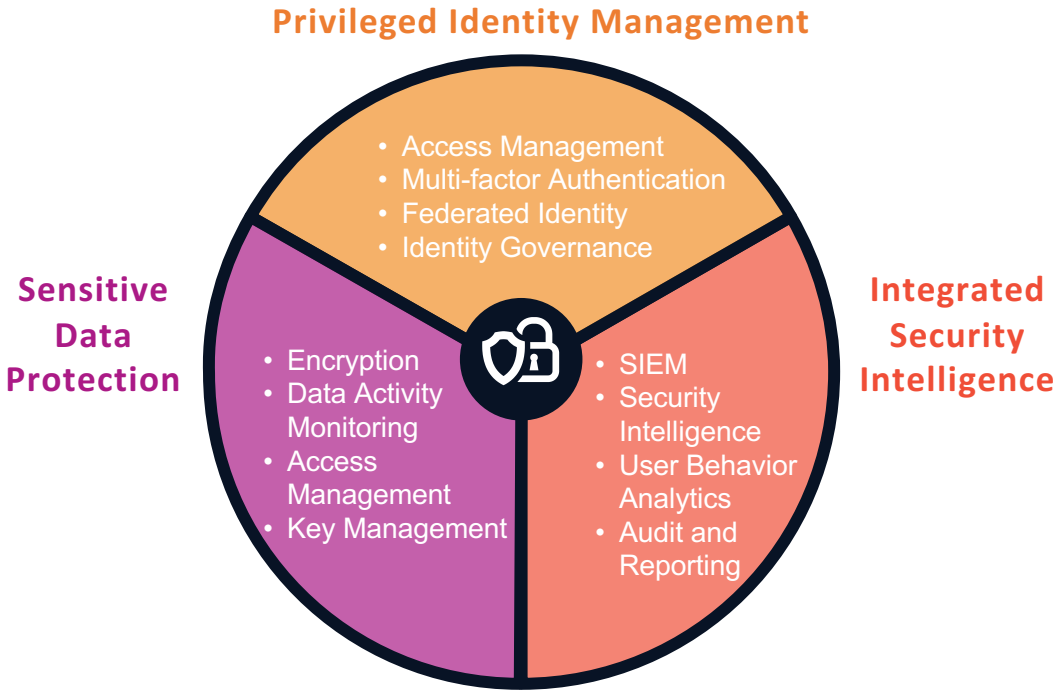
80 percent of the world’s corporate data

91 percent of CIOs said new customer-facing apps are accessing the mainframe

Mainframes account for 68% of production workloads, but only 6% of IT spend

Protecting data at the core of the enterprise

Encryption is the solid foundation of a layered cybersecurity strategy



Traditional workloads and APIs:

- DB2®
- CICS® / VSAM
- IMS™
- MQ

Relevant Security Solutions:

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

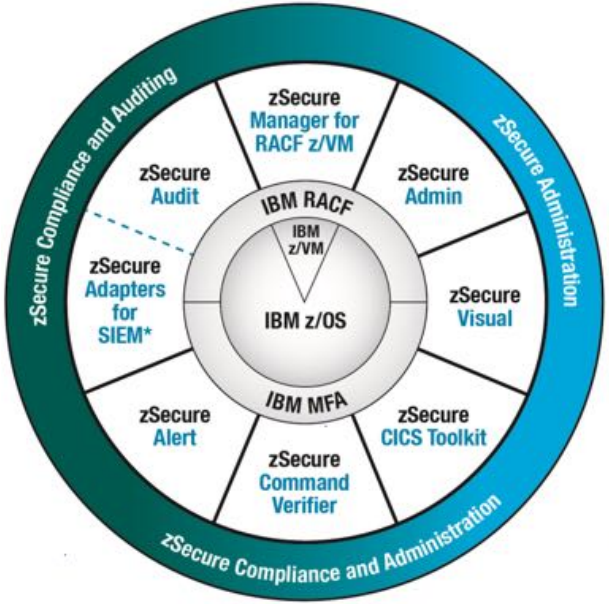
IBM Security zSecure Suite: A comprehensive suite of products

zSecure Audit
Vulnerability analysis for the mainframe infrastructure; automatically analyze and report on security events and monitor compliance

zSecure Adapters for QRadar
Collects, formats and sends enriched mainframe System Management Facility (SMF) audit records to SIEMs including IBM QRadar SIEM

zSecure Alert
Real-time mainframe threat monitoring of intruders and alerting to identify misconfigurations that could hamper compliance

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



Note:
- zSecure Audit also available for ACF2™ and Top Secret®
- zSecure Adapters for QRadar SIEM is a capability of zSecure Audit and is also available for ACF2™ and Top Secret®
- zSecure Alert also available for ACF2™

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

zSecure Admin
Enables more efficient and effective RACF administration, identity governance, tracking and statistics using significantly fewer resources

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

zSecure CICS Toolkit
Provides access RACF command and APIs from a CICS environment, allowing additional administrative flexibility

zSecure suite integrates with . . .

IBM Security Identity Governance and Intelligence

Guardium®

QRadar

Comparison of data at rest encryption

Full Disk 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
- Prevents exposures on
  - Disk removal
  - Box removal
  - File removal

z/OS Data Set Encryption

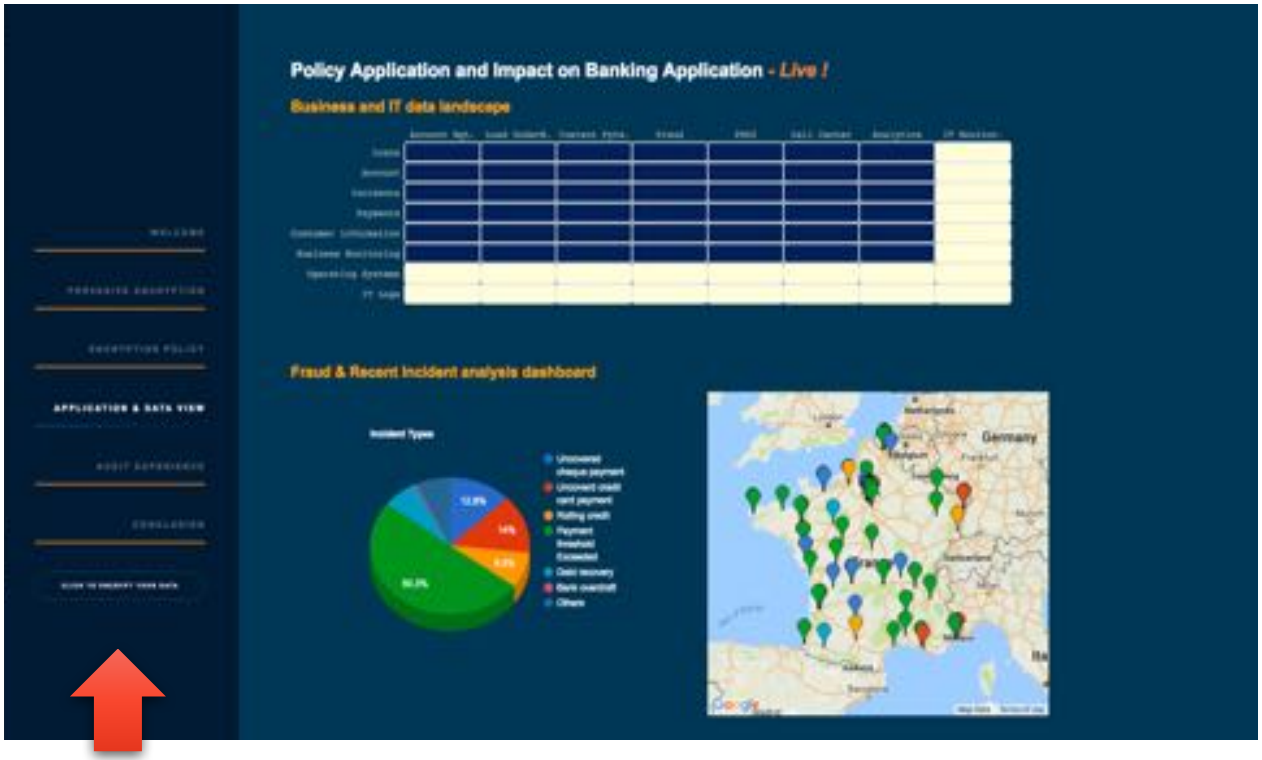
- Broadly encrypt data at rest
- Covers VSAM, DB2, IMS, Middleware, Logs, Batch, & ISV Solutions[1]
- Transparent to applications
- Encryption …
  - By policy
  - Tied to access control
  - Keys controlled by host
- Encrypt in bulk for low-overhead
- Prevents exposures on
  - Mis-identification or mis-classification of sensitive data
  - Compliance findings related to unencrypted data

z/OS Database Encryption

- Data remains encrypted inside the database
- Data in memory buffers is also protected
- Very flexible key granularity
  - Down to the row and column level for DB2
  - Segment level for IMS
- Excellent separation of duties
- Transparent to applications
- Prevents exposures on
  - Unauthorized viewing of encrypted sensitive data
  - Non-DBMS data access
  - Unauthorized access to DBMS generated datasets (i.e. logs)

1 Any applications or middleware making use of VSAM, QSAM, BSAM access methods. Refer to individual ISV documentation to confirm support of z/OS data set encryption.

Policy Application and Impact on a Real Banking Application



3-4 Minutes: Practical example for Banking application

Live Enterprise Data added to policy
Encryption enabled in sec's according to policy
No Application Changes is required

- **Policy scope:** all business (no technical data) and authorizing this application
- **Policy enforcement** (1-time action) is applied on M's of records
- Authorized machine now still runs, on protected data with no Service Level degradation

- Touch to apply the Encryption Policy
- Touch to go NEXT


IBM Security QRadar SIEM
Dataset Encryption
Encryption Status
PCI-DSS
Not Encrypted
Encrypted
Sensitivity Type
% Encryption
Encrypted
Not Encrypted
Mar 26
Apr 9
Apr 23
May 7
May 21

IBM QRadar