IBM Z
Pervasive Encryption, unreachable goal or reality?

Pervasive: present or noticeable in every part of a thing or place

Jan Tits
IBM Systems
jantits@be.ibm.com

May 8, 2019 GSE Regional Conference - Zemst

IBM Z

you IBM

Data protection and compliance are business imperatives

28%

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

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

Of the **14 Billion** records breached since 2013 only **4%** were encrypted [3]

$3.86M

Average cost of a data breach in 2018 [2]

European Union General Data Protection Regulation (GDPR)

Payment Card Industry Data Security Standard (PCI-DSS)

Health Insurance Portability and Accountability Act (HIPAA)

1, 2 Source: 2018 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 complex

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

Organizations struggle with questions such as:

What data should be encrypted?

Where should encryption occur?

Who is responsible for encryption?

Pervasive encryption: A paradigm shift in data protection

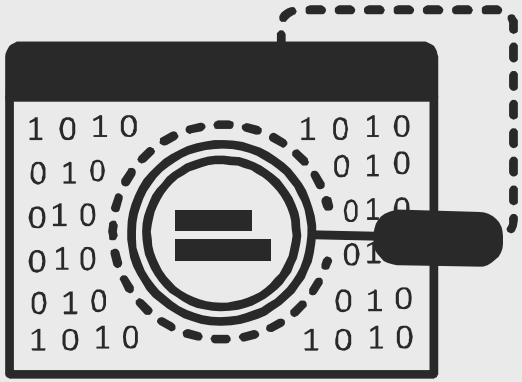
Protecting only enough data to achieve compliance should be the bare minimum, not a best practice.

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

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.

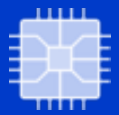
No Application Changes

No Impact to SLAs

IBM z14

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 OS 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

Authenticate and 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 IBM Blockchain platform (Enterprise or IBM Cloud Private).

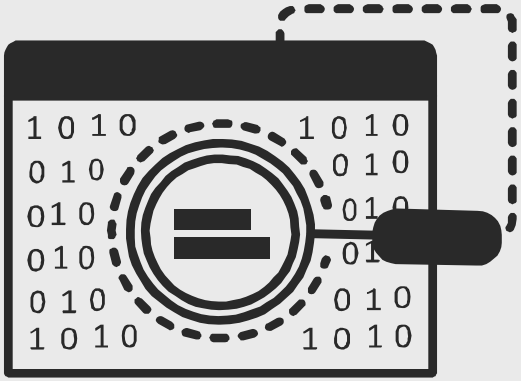
IBM z14

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

keys in memory - industry exclusive CPACF protected key encryption ensures encryption key values are never exposed to the OS, hypervisor, or application.

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

IBM z14



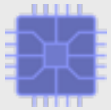
Pervasive encryption on IBM Z significantly reduces the time and effort required to meet compliance obligations and complete audits.

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

Remove entire classes of data and users from compliance scope.

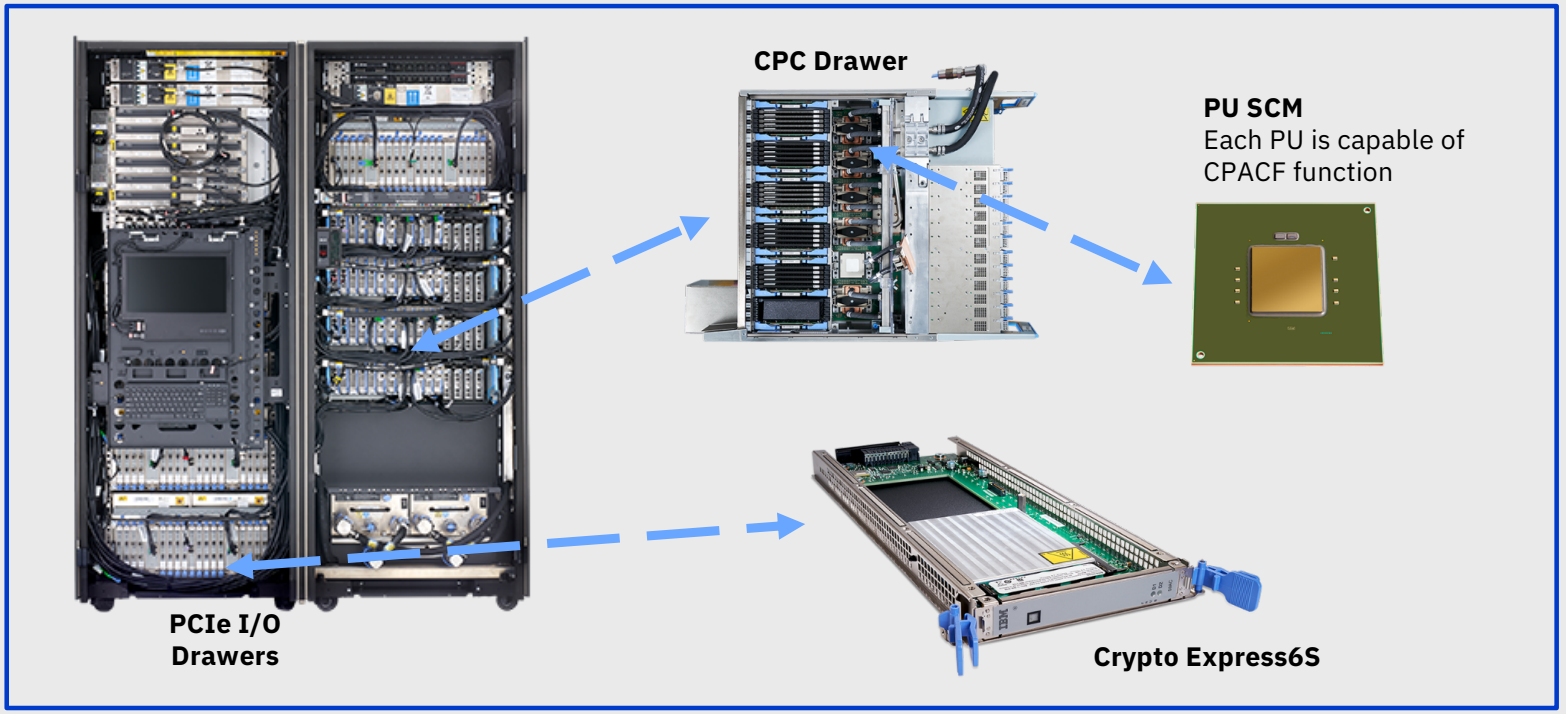
Pervasive Encryption with IBM Z

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 …

How is crypto supported in IBM Z hardware?



z14 Integrated Cryptographic Hardware

CP Assist for Cryptographic Functions (CPACF)

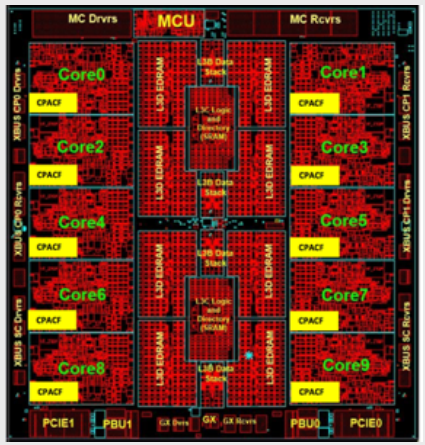
- Hardware accelerated encryption on every microprocessor core
- Performance improvements of up to 6x for selective encryption modes

Suited for high speed bulk symmetric encryption

Crypto Express6S

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

Suited for high value transactions, key protection and asymmetric acceleration

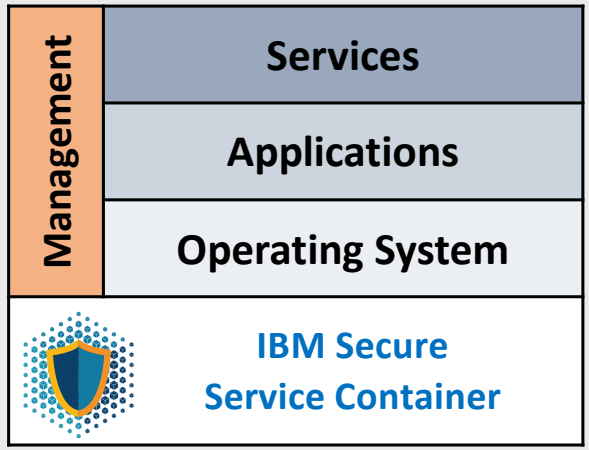


Why is it valuable:

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

IBM Secure Service Container
The Base Infrastructure to Host and Build Software Appliances

- Simplified, fast deployment and management of packaged solutions
- Tamper protection during appliance installation and runtime
- Automatic protection of data and code running in appliance – at flight and at rest
- Management via Remote APIs (RESTful) and web interfaces
- Enables appliances to be delivered via distribution channels

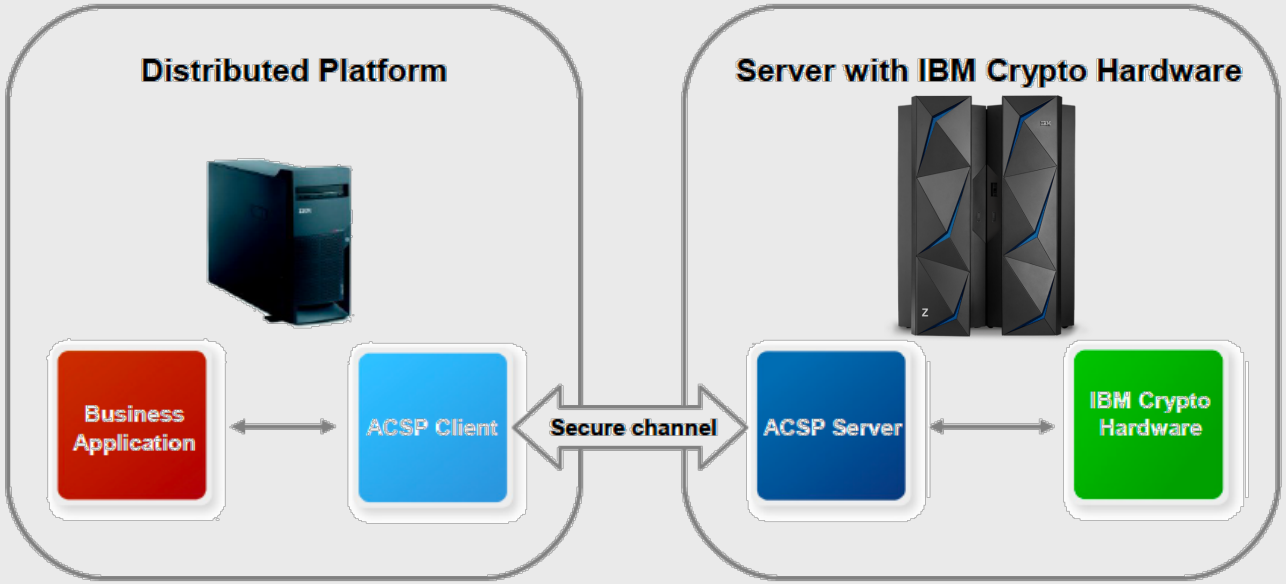


Protects Against Misuse of Privileged User Credentials

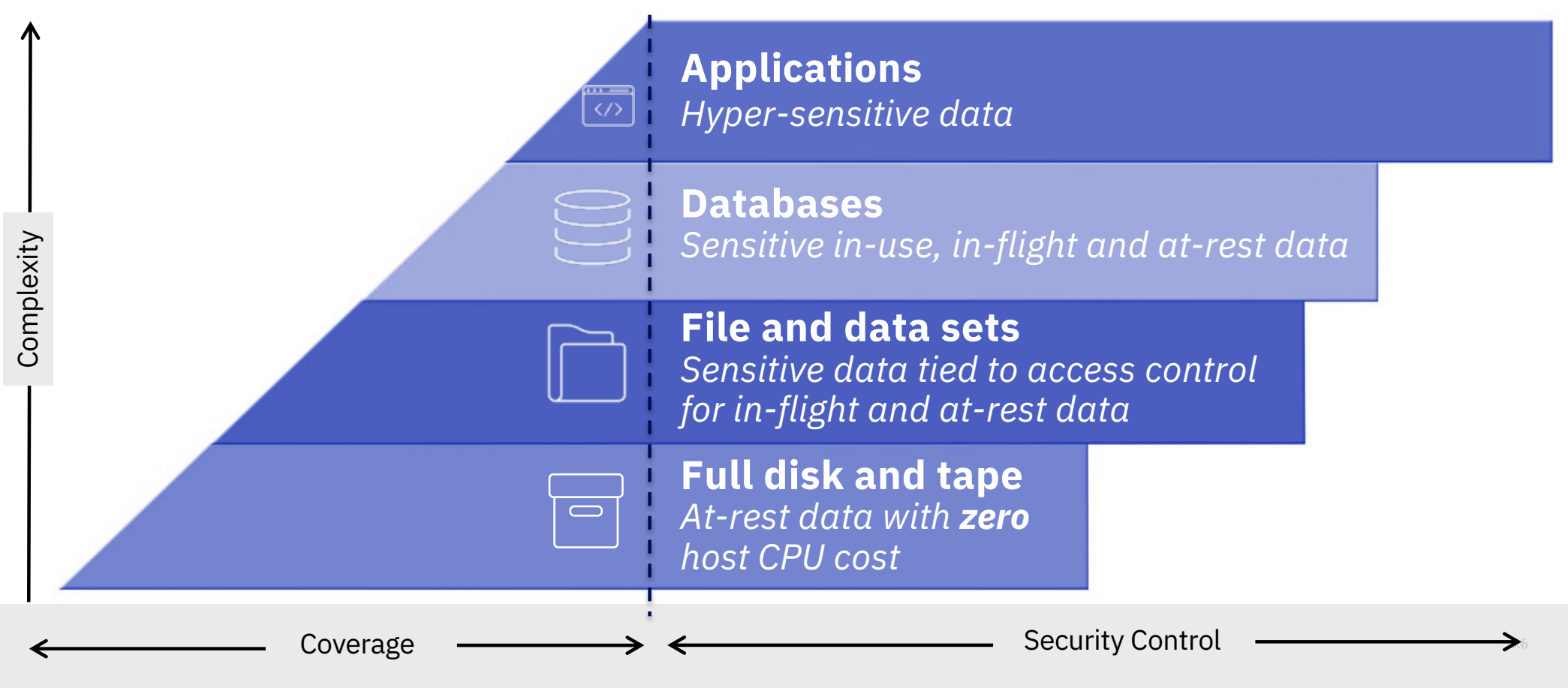
Operating environments and data are protected against access and abuse by root users, system administrator credentials, and other privileged user access

Advanced Crypto Service Provider

- Use existing scalable infrastructure to add security to new applications and platforms
- EKMF can be used to manage keys



Multi-layered encryption is essential for data at-rest



Market Response to IBM Z pervasive encryption

- Pervasive encryption recognized as a pillar of compliance (including GDPR), limiting risk at low cost
- Organizations recognize synergy with other encryption solutions like Full Disk Encryption
- Organizations discovering the true cost of application encryption may be prohibitive
- Organizations recognize pervasive encryption technical value (application transparency, performance, easy to implement ,..)
- There is a pervasive encryption story for LinuxONE & Linux on Z!!!

Let’s get started!

Schedule your workshop at the IBM Client Experience Center

Watch some videos

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

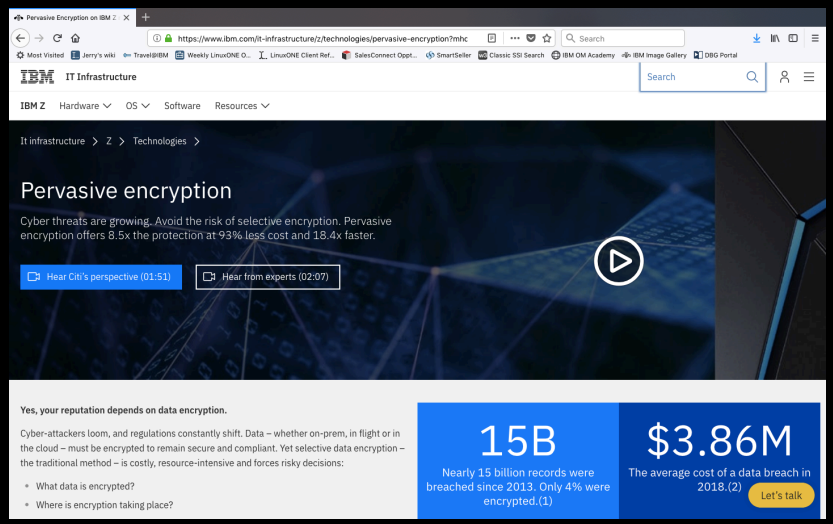
CF Encryption:
https://www.youtube.com/watch?v=ITmsFWuJwJU

zERT:
https://www.youtube.com/watch?v=1CgEcCTX_o8

MOP MPL Bank:
https://www.youtube.com/watch?v=EP488nLdGts

Visit the IBM Z Pervasive Encryption landing page

https://www.ibm.com/it-infrastructure/z/technologies/pervasive-encryption



Get ready

Redbook: Getting Started with z/OS Data Set Encryption Redbook
http://www.redbooks.ibm.com/redpieces/abstracts/sg248410.html?Open

Redbook: Security and Linux on z Systems
http://www.redbooks.ibm.com/abstracts/redp5464.html?Open

New: IBM Z pervasive encryption landing page
https://www.ibm.com/it-infrastructure/z/technologies/pervasive-encryption

IBM Z pervasive encryption solution guide (Knowledge Center)
https://www.ibm.com/support/knowledgecenter/en/SSLTBW_2.3.0/com.ibm.zos.v2r3.izs/izs.htm

IBM Z pervasive encryption FAQ:
https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=ZSQ03116USEN

IBM Crypto Education page: https://ibm.biz/BdiAah

zPET Test Reports:
https://www.ibm.com/developerworks/community/groups/service/html/communitystart?communityUuid=43ea8e78-acbe-49f5-9290-379e4f4569cb

MOP demo white paper:
http://www-03.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/WP102734

Don’t forget!

2019

IBM Systems Technical University

IBM Z • IBM Storage

20 – 24 May | Berlin, Germany
Vienna House Andel’s Berlin

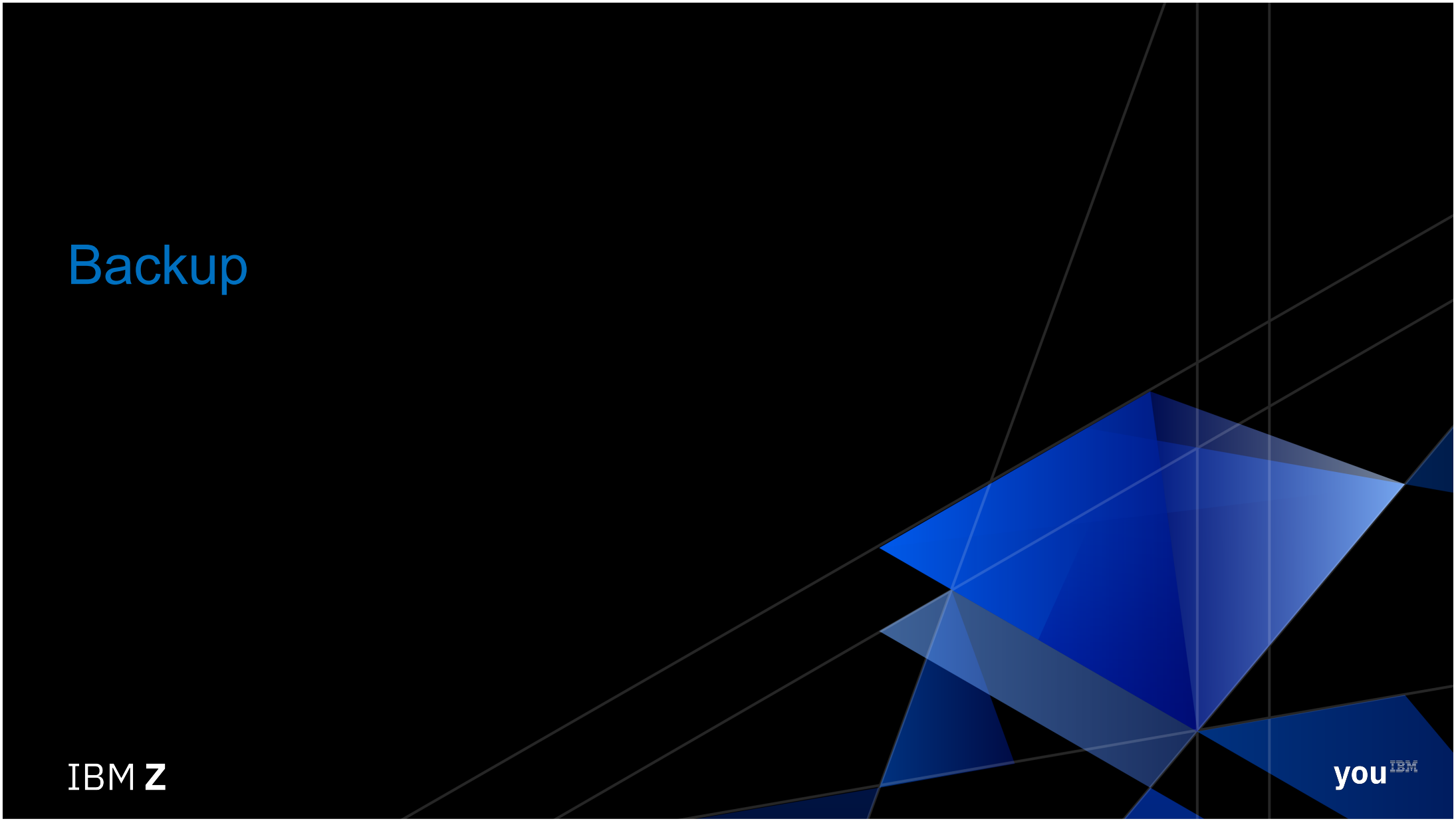
https://www-03.ibm.com/services/learning/ites.wss/zz-en?pageType=page&c=FBAW9ITQV7TWW9TF

Thank you

IBM Z

you IBM

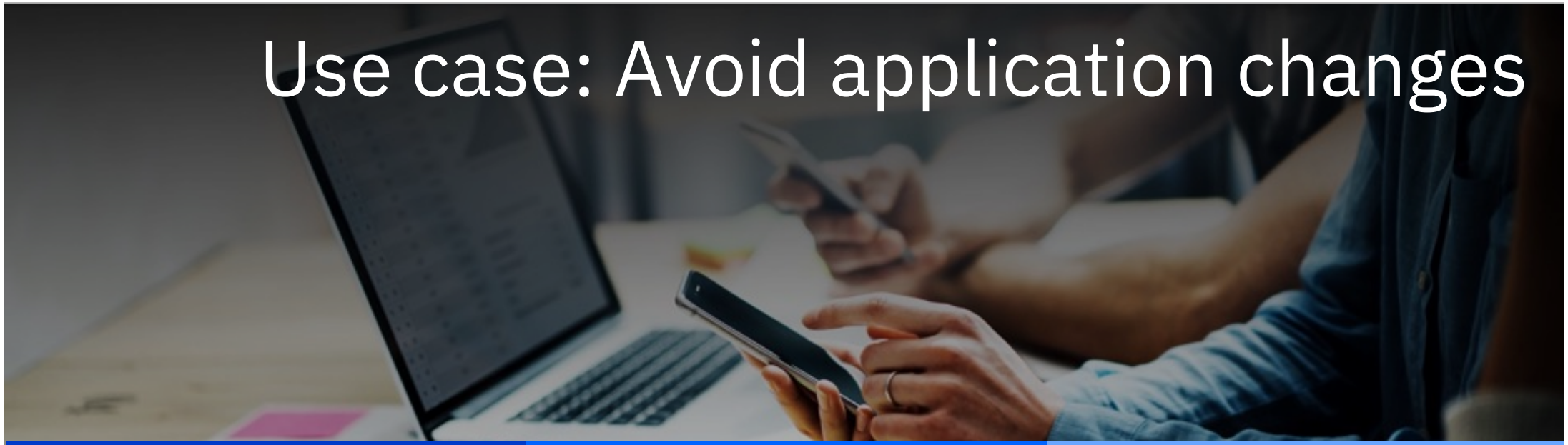
Backup



IBM Z

you IBM

Use case: Avoid application changes



Challenge

Faced significant expense to protect data by changing thousands of applications to add field level encryption

IBM approach

Keep app developers focused on adding business value. IBM Z encryption designed to protect data transparent to applications.

Outcome

Protect business critical data at core of enterprise without costly application changes using z/OS data set encryption.

Use case: Reduce CPU cost

Challenge

Observed significant processor cost after initial benchmark test of field level encryption added to application.

IBM approach

Full stack integration - IBM z14 on core hardware crypto acceleration combined with operating system encryption exploitation.

Outcome

Encrypt data in “bulk” to protect data with minimal processor overhead.

Use case: Easy, secure deployment

Challenge

IBM Blockchain Network using Hyperledger fabric has key focus on performance, data privacy and security.

IBM approach

Deploy Blockchain in a Secure Service Container (SSC) on a LinuxONE server with Crypto Express coprocessors.

Outcome

Hardened container with all data and code encrypted using high performance and scalable IBM Z encryption hardware.

Use case: data in-flight and at-rest

Challenge

Business imperatives driving need for data protection in response to government and GDPR regulations.

IBM approach

Linux on z and LinuxONE designed to leverage z14 encryption hardware transparent to software and applications.

Outcome

Protect data in-flight and at-rest with benefit of z14 crypto performance using open source solutions including OpenSSL and dm-crypt .

Use case: Intelligent Network Discovery

Challenge

Corporate directive to encrypt all data in-flight. Identifying where and how network traffic protected was manual labor intensive

IBM approach

z/OS Comm Server z Encryption Readiness Technology designed to provide a single view of security attributes for all z/OS network sessions.

Outcome

Auditors and network administrators can easily determine where and how network session are protected using single dashboard view.

Use case: Achieve cryptographic isolation

Challenge

Audit findings due to lack of crypto key isolation between prod, dev, & test sharing same physical resources (processor & disk)

IBM approach

IBM Z pervasive encryption uses crypto domains to achieve cryptographic separation between prod, dev and test environments.

Outcome

Deploy z14 and z/OS data set encryption in combination with full disk encryption to meet audit requirements.

Use case: Simplify compliance

Challenge

Storage administrators have access to massive amounts of data and pose significant risk to business.

IBM approach

Encryption designed to allow storage administrators to manage data containers without needing access to encryption key.

Outcome

Remove storage administrators from risk and scope using IBM Z pervasive encryption.