IBM brings
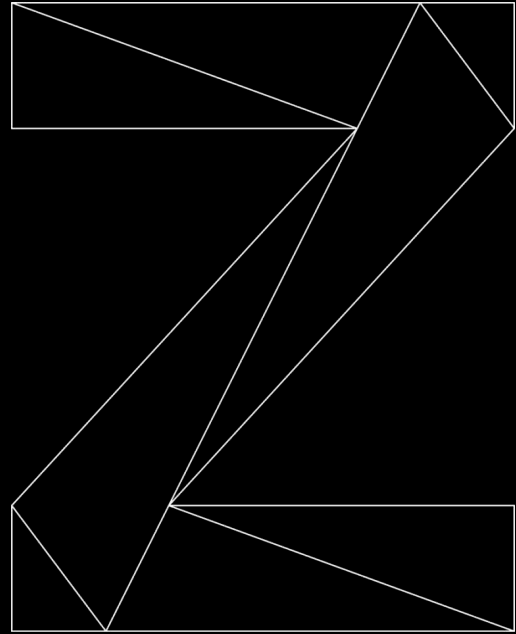# **Pervasive Encryption to the Cloud** with
New System Design

Andreas Thomasch
Platform Leader & Manager
IBM Z & LinuxONE, DACH

Embargoed until April 10th

IBM

Agenda

11:00 **Opening & Strategy remarks**
Andreas Thomasch, Platform Leader & Manager
IBM Z & LinuxONE, DACH

11:15 **Announcement News**
Bodo Hoppe, Distinguished Engineer
Hardware Verification, IBM Labor Böblingen

11:45 **A deeper look at security@IBM Z**
Rita Pleus, Product Manager IBM Z & LinuxONE
Hardware + Operating Systems, DACH

11:55 **Master the Mainframe experience**
Sebastian Wind, Student
Universität Leipzig

12:00 **Q&A**
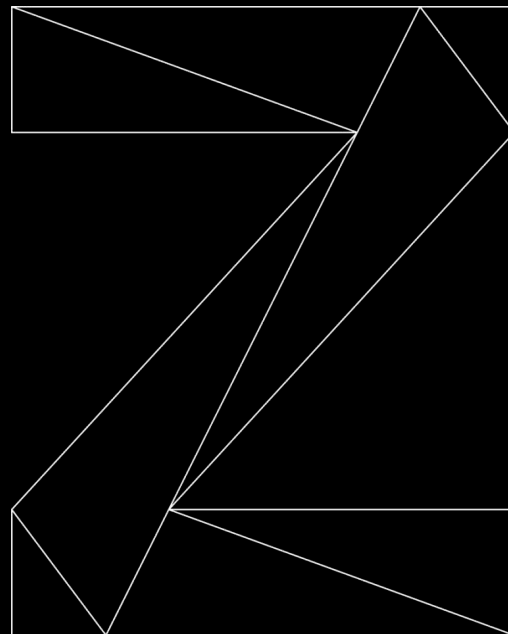
Trademarks

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

BladeCenter*	FICON*	IBM*	LinuxONE	Storwize*	z13s	z/OS*
Db2*	Flash Systems	IBM (logo)*	LinuxONE Emperor II	System Storage*	z14	z/VM*
DFSMSdss	GDPS*	ibm.com	LinuxONE Rockhopper II	WebSphere*	zEnterprise*	z/VSE*
DFSMShsm	HiperSockets	IBMZ*	Power Systems	z13*	zHyperLink	
ECKD	HyperSwap*	InfiniBand*	PR/SM			

* Registered trademarks of IBM Corporation

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.

From our Chairman's Letter of Ginni Rometty to our Annual Report 2017 (see https://www.ibm.com/annualreport/2017/letter.html for full letter):

(…) Our reinvented systems franchises generated strong growth.

Mainframes enjoyed a very strong fourth quarter, thanks to the launch of the new z14, the world's first system that can encrypt data pervasively without requiring changes to applications and with no downtime.
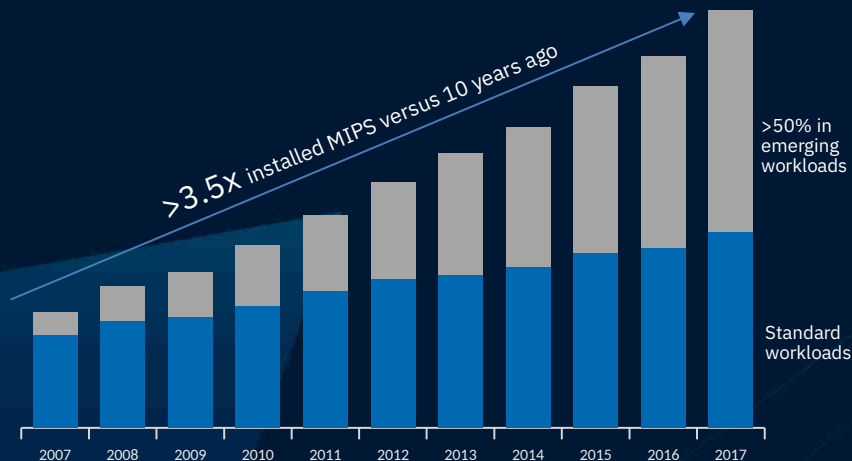
We expect this breakthrough will drive significant expansion of the mainframe's already broad market. (…)

Embargoed until April 10th

IBM **Z**

IBM Z Continues to evolve & grow with our clients and the market through multiple technology eras

Continuous Reinvention of Enduring Platforms for Business

Workload as measured by installed Million Instructions Per Second (MIPS)

>3.5x installed MIPS versus 10 years ago

>50% in emerging workloads

Standard workloads

2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017

IBM Z Value Drivers

+ Industry first pervasive encryption capabilities
+ Open and connected to public and private cloud environments
+ Optimized for machine learning and real time insights
+ Transparent and predictable container pricing for new workloads
+ Unmatched reliability, security, and availability

92
of top 100 banks in the world

10
of 10 largest insurers in the world

30B
Transactions processed per day

~$7T
Annual credit card payments

>3.5x
installed MIPS versus 10yrs ago

>50%
of installed MIPS in emerging workloads

>50%
Strategic Imperatives revenue mix

Embargoed until April 10th

IBM **Z**

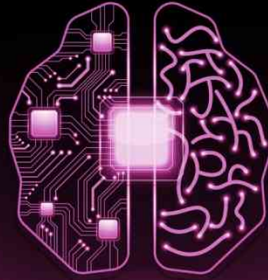# IBM Z: Designed for trusted digital experiences

The world's premier system for enabling data as the new security perimeter

- Pervasive encryption
- No application changes
- Protect from internal and external threats

Designed for data serving in a cognitive world

- Speed, scale and reduced latency
- Efficiency for managing data
- Secure and flexible access to data

The best infrastructure to support an open and connected world

- 'From anywhere' mobile access
- Simplified sys admin of z/OS®
- Standardization for skills transfer

Embargoed until April 10th

Extending the IBM z14 Family

Built on the same technology of IBM z14	Addressing new markets	Standardization and Simplicity	One strong platform and family for the future

Embargoed until April 10th

What is launching on April 10?

- IBM Z is launching a single-frame z14 model **ZR1** (industry standard 19" rack)
- LinuxONE is launching the **Rockhopper II**

Key dates:
- April 10 – Announcement
- 2Q (TBD) – General Availability

Early Support Program - Customer in DACH

- Contract Signed
- Customer Environment
  - zBC12 ⭢ z14 ZR1
  - z/OS
  - z/VM
  - z/VSE
  - Linux on Z
  - KIDICAP NEO (HR application)
- Will become IBM reference customer

One of the leading IT service providers for the churches in Germany

Embargoed until April 10th

IBM z14

Extending the IBM z14 Family

Breakthrough technologies

Designed for the Secure Cloud

Embargoed until April 10th

IBM **z14**
Model ZR1

IBM **LinuxONE**
Rockhopper II

Bodo Hoppe
Distinguished Engineer
IBM Z Development

IBM

Introducing the new IBM z14 Model ZR1 & IBM LinuxONE Rockhopper II

with key technologies engineered in the **Böblingen Development Lab**

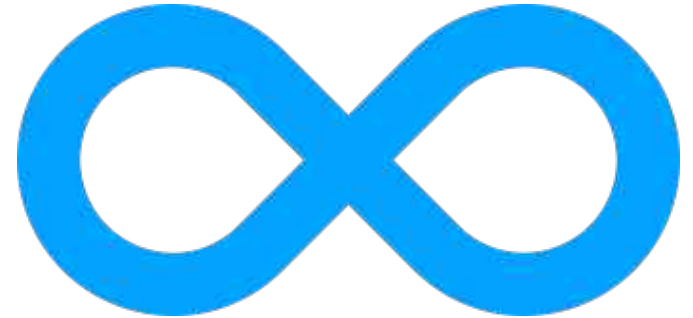# Designed and developed, using IBM Design Thinking

Co-created with stakeholders and sponsor users from clients of all sizes, applications users, business partners and geographies

Collaborated with more than 150 clients for IBM z14 and additional 80 clients for IBM ZR1 and IBM LinuxONE Rockhopper II

Observe   Reflect   Make

New Cloud Ready: All in One

Platform Simplification
- Standardization across many components
  - including industry standard 19" single frame rack*
- 16U free space in frame
- Data Center in a Box
  - Low-latency connectivity (IBM zHyperlink Express)
- 40% less space

*Processor Board & Cards
developed in the Böblingen
Development Lab

IBM z14 Model ZR1 & IBM LinuxONE Rockhopper II
10-core processor chip

- Same chip technology as the z14 Models M01-M05

- Up to ten cores (PUs) per chip

- 4.5 GHz versus 5.2 GHz for the IBM z14 M01-M05

- Improved instructions per cycle (IPC) with microarchitecture enhancements
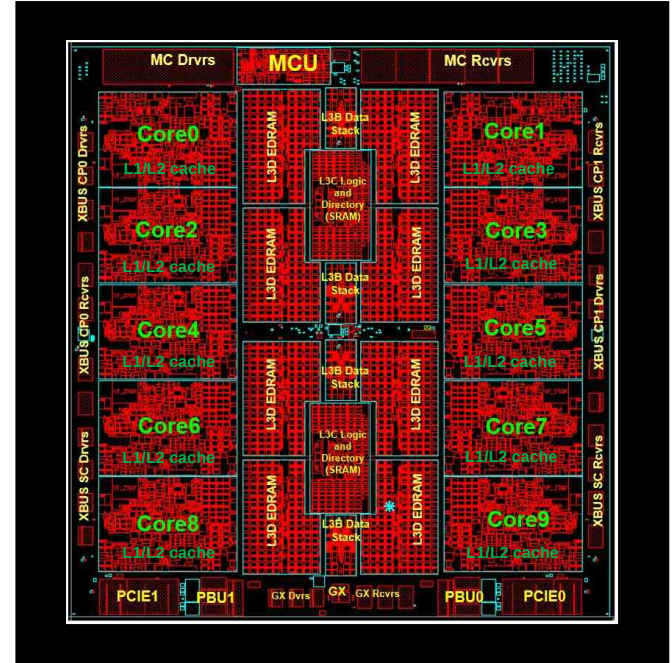
14nm SOI Technology
- 17 layers of metal
- 6.1 Billion Transistors

Chip Area
- 26.5 x 27.8 mm

IBM Secure Container*

Even Root Users and Sys Admins can not access or see data and software

Malware can not self install into the container

All Data is encrypted. Keys are protected in memory

*Invented, owned and majorly developed in the IBM Böblingen development lab

IBM Secure Service Container Appliance

Secure Service Container

Management UI / REST API	Solution / Application
	Application Interfaces
	Management Backend
	Base Operating System

New IBM Db2 Analytics Accelerator

Analytics acceleration on z14 Model ZR1 with the high quality of service of IBM Z. No need for an external server.

Uses IBM Secure Container Technology

Invented and developed in the IBM Böblingen Development Lab

What else is new in z14 Model ZR1 and IBM LinuxOne Rockhopper II?

Largest z14 Model ZR1 is expected to provide up to 13% more total z/OS and up to 60% more total Linux on Z capacity than the largest z13s

2x memory (8TB)
(compared to their predecessors)

IBM z14 Model ZR1
>850 Million fully encrypted transactions per day

Processor Units:
4, 12, 24 or 30 on max 6 CPs

IBM LinuxOne Rockhopper II
Docker-ceritified infrastructure tested with up to 330000 Docker containers

IBM z14 Model ZR1 & IBM LinuxONE Rockhopper II

Co-created with clients

Key innovations and technologies developed in

the Böblingen Development lab

Platforms provide trusted digital experiences in a

scalable, public, private, or hybrid cloud

infrastructure

Low cost enterprise entry models in a industry

standard form factor, an all-in-one solution that

New IBM z14 & Rockhopper II: A deeper look at security

10. April 2018 @ IBM Z Presse Event

Rita Pleus
Rita.Pleus@de.ibm.com
IBM Mainframe Product Manager Hardware + Operating Systems
zChampion, WW Lead Security

IBM **Z**

you^{IBM}

Trademarks

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

Warum Datenschutz (und Verschlüsselung) ?

Regulations

European Union General
Data Protection Regulation
(GDPR) ab 25.Mai 2018

IT-Sicherheitsgesetz
(ITSiG)
seit 25.Juli 2015

Payment Card Industry Data
Security Standard (PCI-DSS)

PSD2-Richtlinie
seit 13.01.2018

Cyberkriminalität

„Cyber-Kriminalität, Cyber-Spionage gegenüber
Staat und Wirtschaft und provozierte Ausfälle
Kritischer Infrastrukturen
sind eine ernstzunehmende Bedrohung unserer
Gesellschaft
im 21. Jahrhundert."
(Quelle BSI : Die Lage der IT-Sicherheit in
Deutschland 2017)

Business

- Sicherheit als Differenzierungsmerkmal von
  Unternehmen
  - Freiwillig zum Zweck der Kundenwerbung/-
    vertrauen
  - Notwendig zur Erfüllung gesetzlicher Auflagen

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

Focus on eliminating barriers to encryption:

- Decouple encryption from data classification

- Prevent from extensive application changes

- Enable encryption of database indexes and/or key fields

- Reduce cost associated with processor overhead

In order to help organizations protect all of their digital assets

Pervasive encryption is the new standard

IBM **Z**

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 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[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.

IBM Z

System z : Multiple Layers of Encryption
Robust data protection

Complexity & Security Control (vertical axis)

Coverage (horizontal axis)

App Encryption
hyper

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*

Enabled through RACF and/or SMS and Z14 CPACF Performance

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

IBM **Z**

Data Protection // z/OS Dataset Encryption
Protection of data at-rest

Legend:

*** - encrypted data

abc - unencrypted data

z/OS

z/OS

z/OS

CF

Network

DB2,IMS, zFS, etc... abc

CPACF

IBM DB2

I am IMS IBM

Storage System

SAN

***

***

LinuxONE/Linux on z

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

IBM Z

IBM Hyper Protect Services

How do IBM Hyper Protect Services keep your data safe?

Data-at-rest encryption
Encrypt all your code and data stored in the IBM Cloud protected by the Z/LinuxONE hardware and firmware. No insiders have access to the data.

Data-in-transit protection
Protect all data between Hyper Protect services with certificates stored in protected storage and memory thanks to the Z/LinuxONE Secure Service Containers technology.

Data-in-memory protection
Keep data safe while in memory with Secure Service Container on Z/LinuxONE.

Features services

IBM Cloud Hyper Protect Crypto Services
Infuse the highest level of security with data encryption and key management capabilities into your apps.

→ Learn more

IBM Cloud Hyper Protect Containers
Deploy Kubernetes workloads on a highly secure platform built for confidential computing.

→ Learn more

IBM Cloud Hyper Protect DBaaS
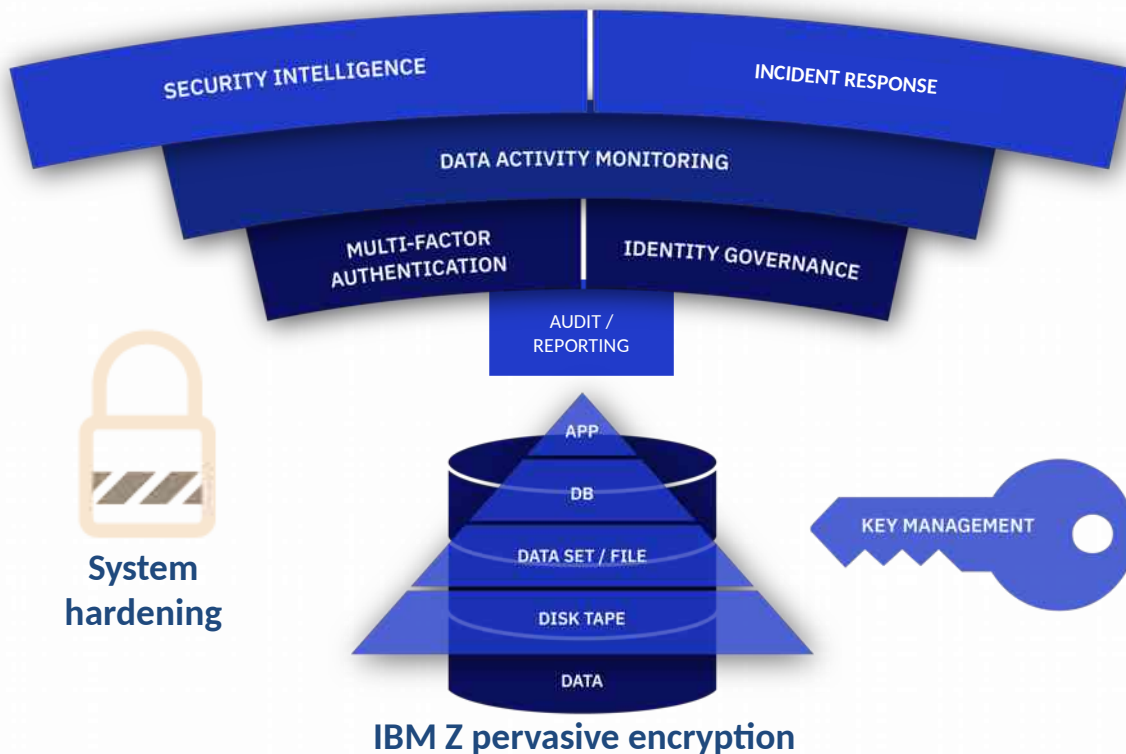Retain your data in a fully encrypted client database without the need for specialized skills.

→ Learn more

https://www.ibm.com/cloud/hyper-protect-services

IBM Z

Protecting data at the core of the enterprise
Encryption is the solid foundation of a layered cybersecurity strategy

System hardening

IBM Z pervasive encryption

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

IBM **Z**

More information

IBM z Systems Security
    http://www.ibm.com/systems/z/solutions/enterprise-security.html

Redbooks
    http://www.redbooks.ibm.com/
    SG24-8410-00 Getting Started with z/OS Data Set Encryption

Crypto Competency Center
    http://www.ibm.com/security/cccc/

Announcement Info
    www.ibm.com/systems/zsolutions

Demo Pervasive Encryption
    https://www.youtube.com/watch?v=EP488nLdGts

Questions about this content?

Master the Mainframe contest 2017, winner – Europe region

1st Place Europe Region:
Sebastian Wind, University of Leipzig, Germany

>> among the top three worldwide !

Sebastian Wind, MtM 2017 video: `https://youtu.be/PEWRV0HMoZY`

>> around 12000 MtM participants ww, from 122 countries.

▪ **MtM - Europe winner celebration at 2018 IBM Systems TU, London, 14th May 2018**

2018
IBM Systems
Technical University
IBM Z • IBM Storage for Z

14. May 2018, London