IBM Security

Keeping up with the Hack-Dashians Data Encryption for IMS and DB2 Databases (“GDEz”)

Howie Hirsch
hshirsch@us.ibm.com
CyberSecurity Specialist

June 22, 2017

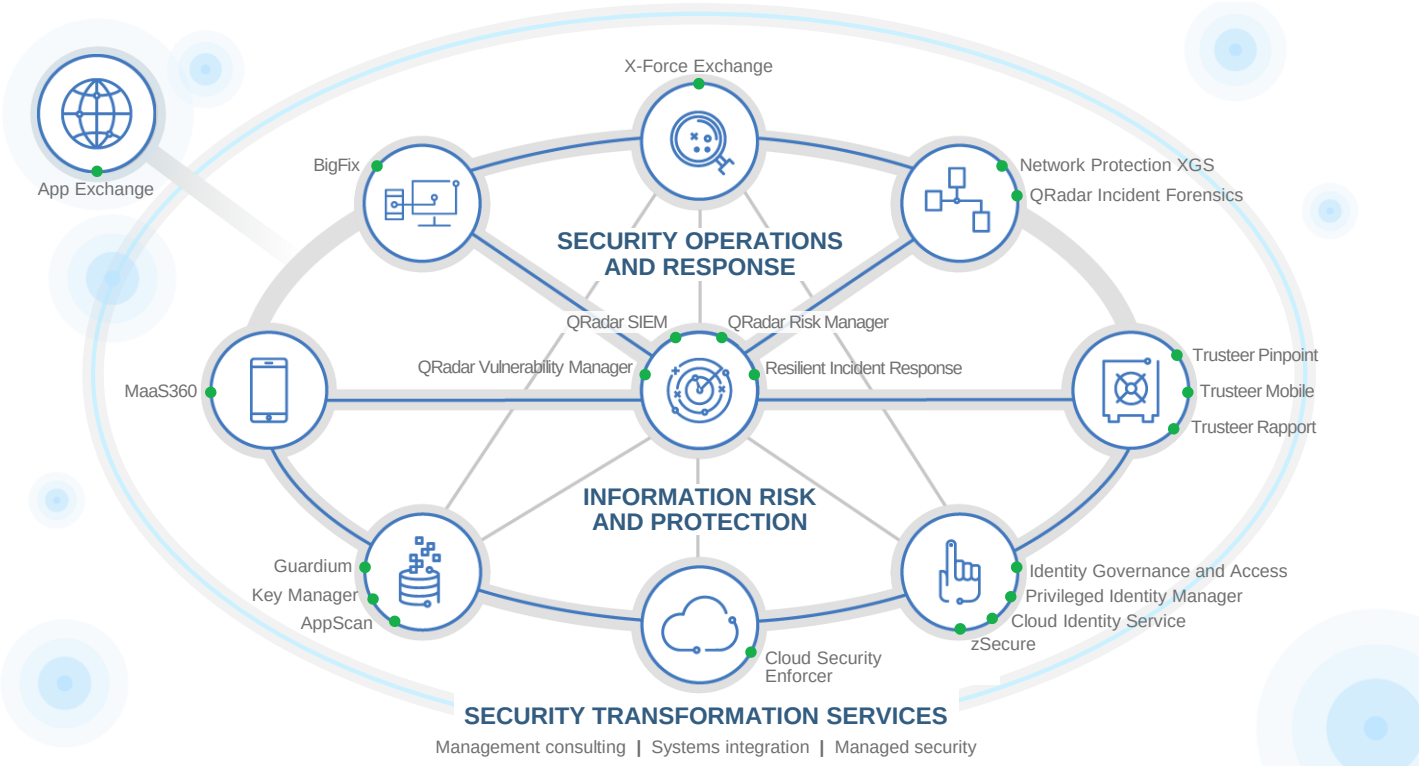
IBM

© 2015 IBM Corporation

© 2015 IBM Corporation

© 2015 IBM Corporation

IBM has the world's broadest and deepest security portfolio



© 2015 IBM Corporation

The increasingly desirable target of the mainframe

80% of all active code runs on the mainframe

80% of enterprise data is housed on the mainframe

Today's technologies have eliminated "mainframe isolation"

Drivers for Data Security

External Threats Sharp rise in external attacks on sensitive data from non-traditional sources	▪ Cyber attack ▪ Organized crime ▪ Corporate espionage ▪ Government-sponsored attacks ▪ Social engineering
Internal Threats Ongoing risk of unintentional and malicious insider behavior put sensitive data at risk	▪ Administrative mistakes ▪ Careless inside behavior ▪ Internal breaches ▪ Disgruntled employees actions ▪ Mix of private / corporate data
Compliance Growing need to address a steadily increasing number of mandates	▪ Governmental regulations (GDPR, SOX) ▪ Industry standards (PCI DSS) ▪ Local mandates

Mainframe customers are more vulnerable to security incidents:

Key concerns

50% concerned with privileged insiders

21% concerned with advanced persistent threats

29% concerned with web-enabled z/OS apps

"As mainframes become a major component in service-oriented architectures, they are increasingly exposed to malware. Web services on the mainframe have significantly impacted security."

Meenu Gupta
President, Mittal Technologies Inc.

The solution…

86% of customers agree that deploying **multiple layers of defense** provides the best mainframe protection

Source: IBM Webinar 2/6/2014, Security Intelligence Solutions for System z and the Enterprise

Defense in Depth of DB2 IMS and VSAM Data

First Layer - Encryption (this forces only access to clear text data must be in the form of an SQL statement) – Encrypt Data in memory

IBM Security Guardium Encryption Tool for DB2 and IMS Databases

Second Layer - Database Activity Monitoring (this ensures each SQL statement is inspected, audited, and subject to security policy control) –

IBM Security Guardium Database Activity Monitoring

Third Layer - Audit access to VSAM linear datasets –

IBM Security Guardium Datasets Activity Monitoring and zSecure Audit

Fourth Layer - Implement business need to know control for critical data (this reduces abuse of privilege access) –

DB2 10 Row masking and Column filtering

Fifth Layer - Test data management and generation –

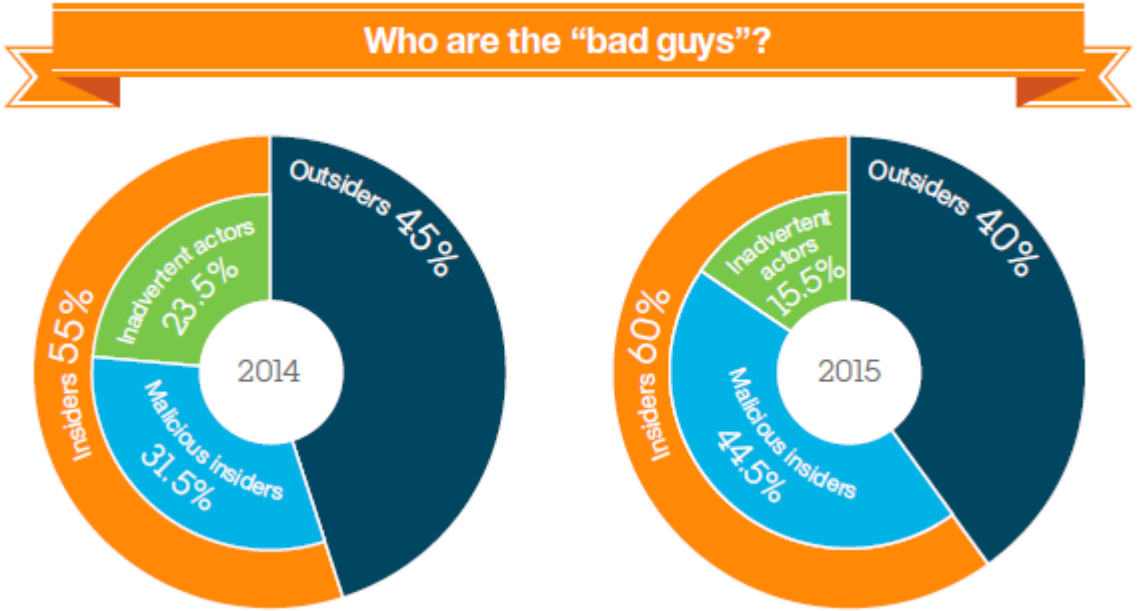
Optim TDM/ Data Privacy

Increasing Insider Threat

Who represents an insider threat?

- An inadvertent actor
- A malicious employee
- A 3rd party/partner with access to sensitive data

  (And falls into one of the categories above)



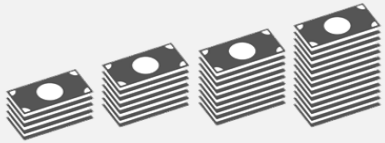
Employees with privileged access to sensitive data carry the greatest risks!

Image Source: IBM X-Force Research 2016 Cyber Security Intelligence Index

Security challenges specific to the mainframe:

Rising costs

Mainframe security administration is typically a manual operation and relies upon old and poorly-documented scripts; highly-skilled mainframe administration resources are limited



Ensuring compliance

Compliance verification is a manual task with alerts coming only AFTER a problem has occurred, *if at all!*

Increasing complexity

The mainframe is an integral component of many large business services, making managing security threats extremely complex creating a higher risk to the business

Lack of visibility

Mainframe processes, procedures, and reports are often siloed from the rest of the organization

Mainframe legacy applications represent a massive exposure of core business information and functions

"Millions of users unknowingly activate CICS every day, and if it were to disappear the world economy would grind to a halt."

Phil Manchester
Personal Computing Magazine

Who run's DB2 on z/OS?

65 of the world's top banks

24 of the top 25 U.S. retailers

10 of the top 10 global insurance providers

Applications by the numbers

1 million active COBOL programs

80% **active** COBOL code

250+ **billions** lines of COBOL code today

2/3 of ALL business transactions for U.S. retail banks
run directly on mainframes

Safeguarding sensitive data requires intelligence and automation

ANALYZE
Automatically discover critical data and uncover risk

ADAPT
Seamlessly handle changes within your IT environment

PROTECT
Complete protection for sensitive data***, including encryption***

A Data Centric Approach

To protect critical data against unauthorized access and enable organizations to comply with government regulations and industry standards.

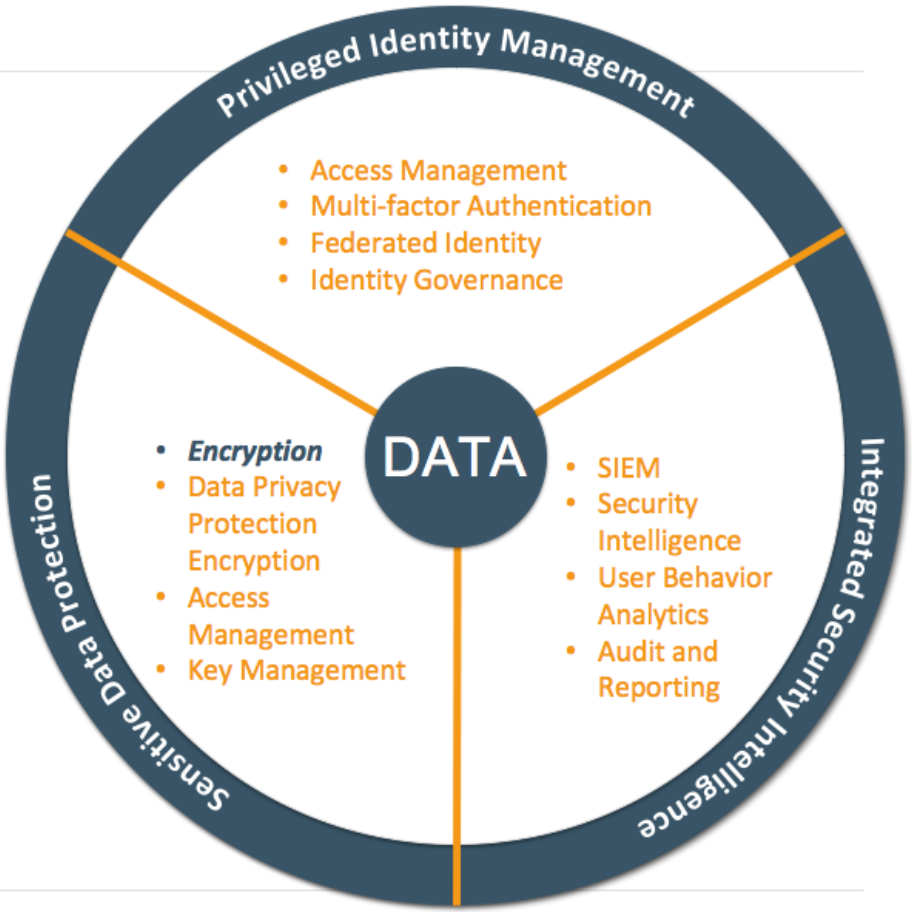
- Prevent data breaches
- Identify data risks
- Ensure data privacy
- Real-time incidence response
- Reduce the cost of compliance
- Streamlined non-intrusive operations

z Security Immune System - A Data Centric Approach

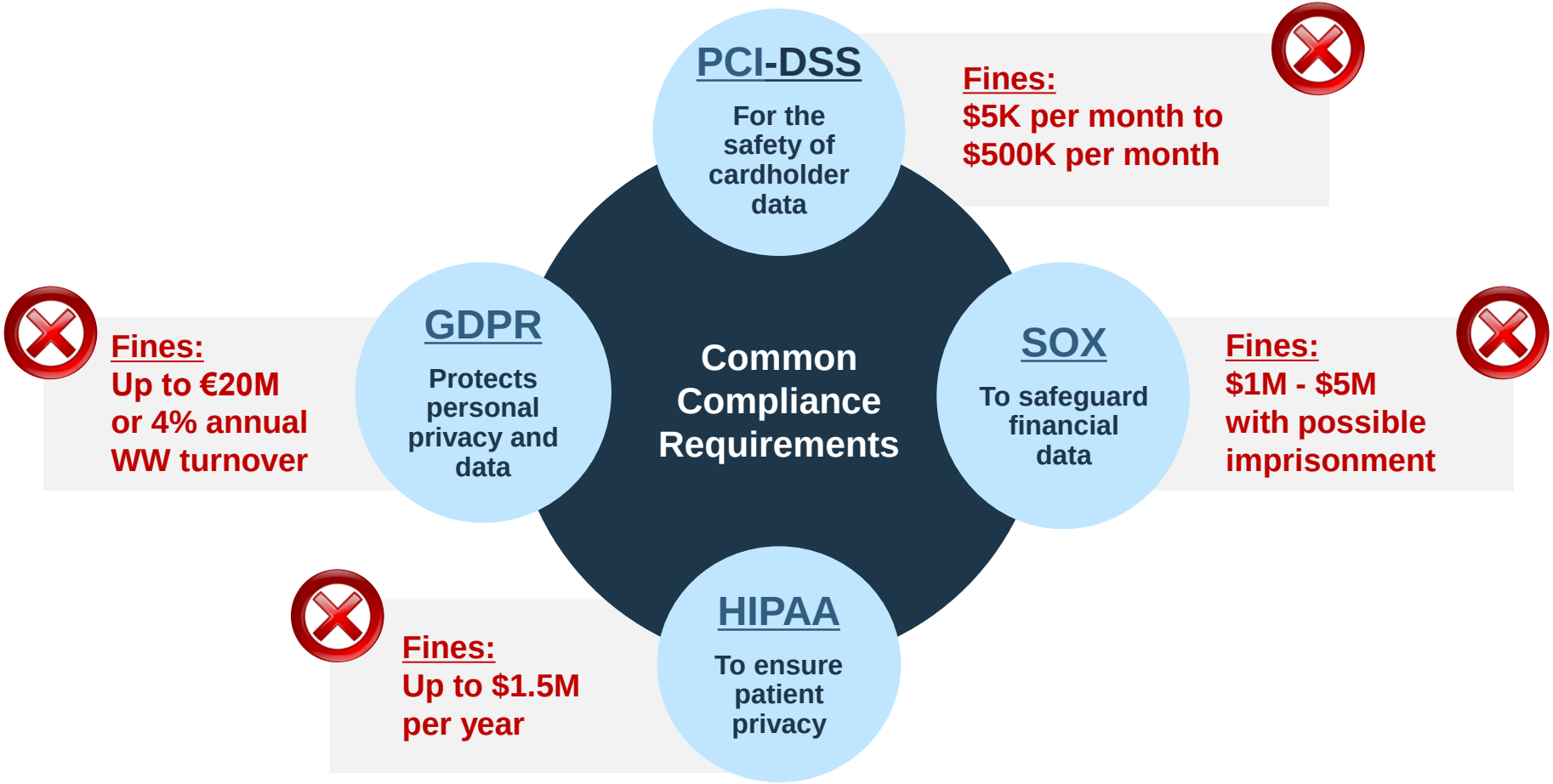
Encryption is the solid foundation on which a robust immune system is built

Providing …

- Granular data access controls for Separation of Duty (SOD)
- Only authorized users may view decrypted "Clear" information
- Data privacy protected on storage media and during transaction execution
- Combine with real time activity monitoring and incidence response to prevent unauthorized accesses to sensitive data
- Optimize for performance and low overhead
- Reduce the cost of meeting compliance



The need for encryption is often spurred by the need to protect data privacy and meet regulatory compliance …



Data encryption defined

- The process of encoding data so that only authorized users can read it by decrypting encrypted data with a key

EXAMPLE

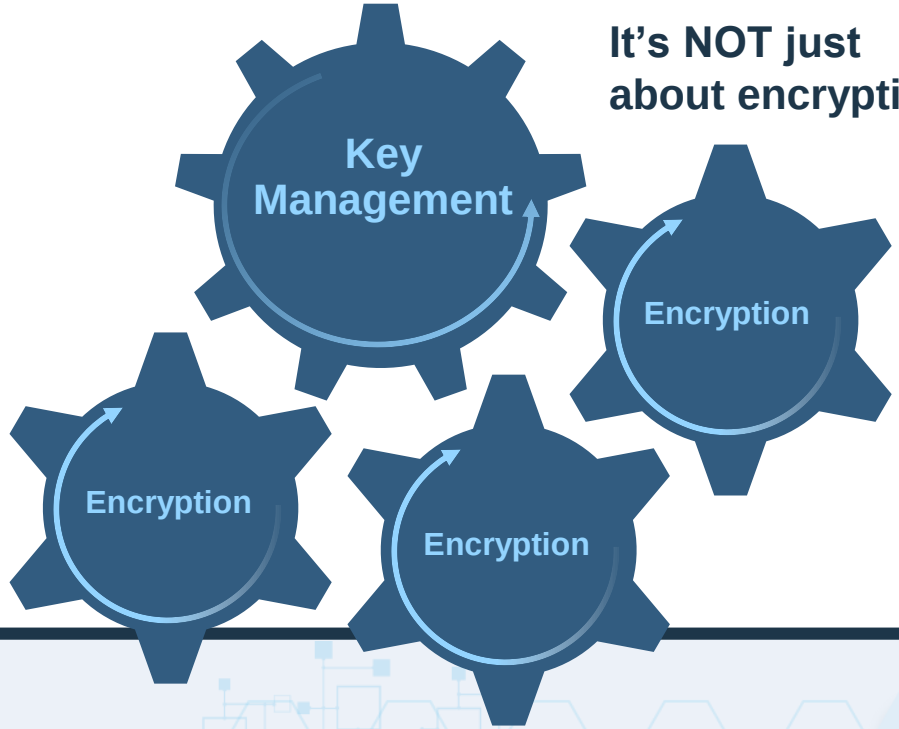
Original Value	Encrypted Value
4536 6382 9896 5200	1@#43$%!xy1K2L4P

Database Encryption
Encrypt tablespace, log and other database files

Unstructured Data Encryption
Encrypt and control access to any type of data used by LUW server

Cloud Encryption
Encrypt and control access to data used by cloud instances

To successfully encrypt, you also need to decrypt – with KEYS!



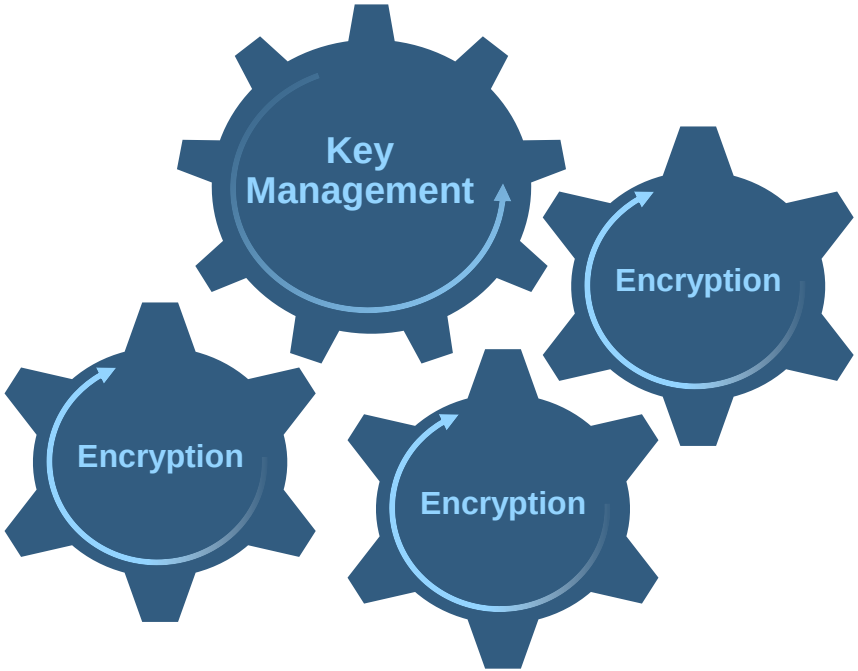
It's NOT just about encryption

It IS about understanding the lineage of encrypted data:

- **What** was encrypted?
- **When** was it encrypted?
- **How** was it encrypted?
- **Where** are the keys?
- **What** policies to allow decrypted clear text ?

<u>If you lose your keys, you've also lost your most valuable assets!</u>

Encryption and key management imperatives to succeed



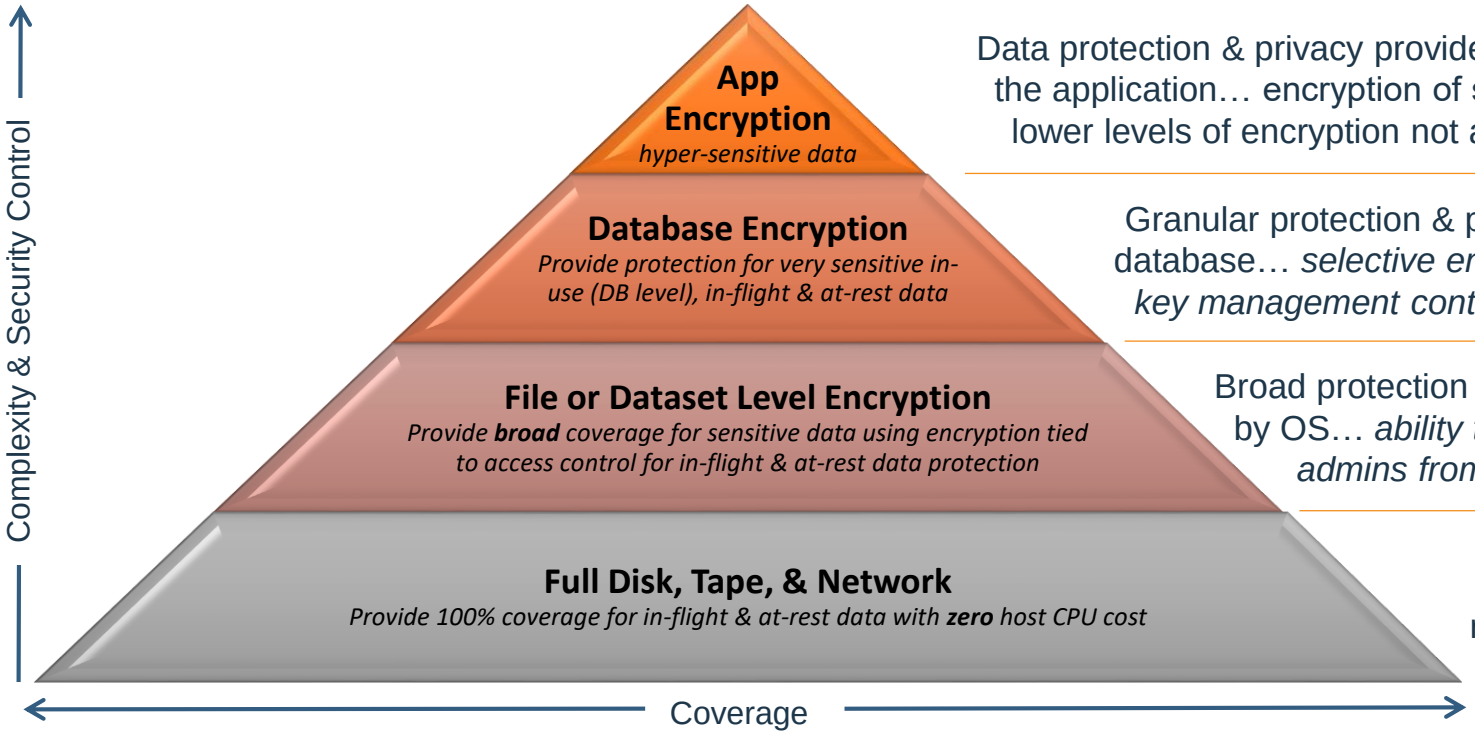
Encryption

- Keep data private and under control
- Protect data in files and folders
- Protect data in media or volumes
- Protect data on-premise, in-cloud and hybrid combinations

Key Management

- Follow industry standards
- Integrate with self-encrypting storage, applications, and databases
- Use key labels for data access policies
- Provide a clear audit trail
- Separate key and data management
- Enable cryptographic erasure

Multiple Layers of Encryption for 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

Data Protection

z/OS Data Set Encryption – first step towards pervasive encryption

- Statement of Direction in the Announcement letter IBM United States Software Announcement 216-392, dated October 4, 2016

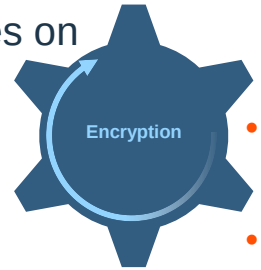
IBM plans to deliver application transparent, policy-controlled dataset encryption in IBM z/OS. IBM DB2® for z/OS and IBM Information Management System (IMS™) intend to exploit z/OS dataset encryption.

https://www.ibm.com/common/ssi/rep_ca/2/897/ENUS216-392/ENUS216-392.PDF

Why Do I Need Database Encryption – A Comparison

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[1]

- Broadly encrypt data at rest
- Covers VSAM, DB2, IMS, Middleware, logs, & ISV solutions[2]
- 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

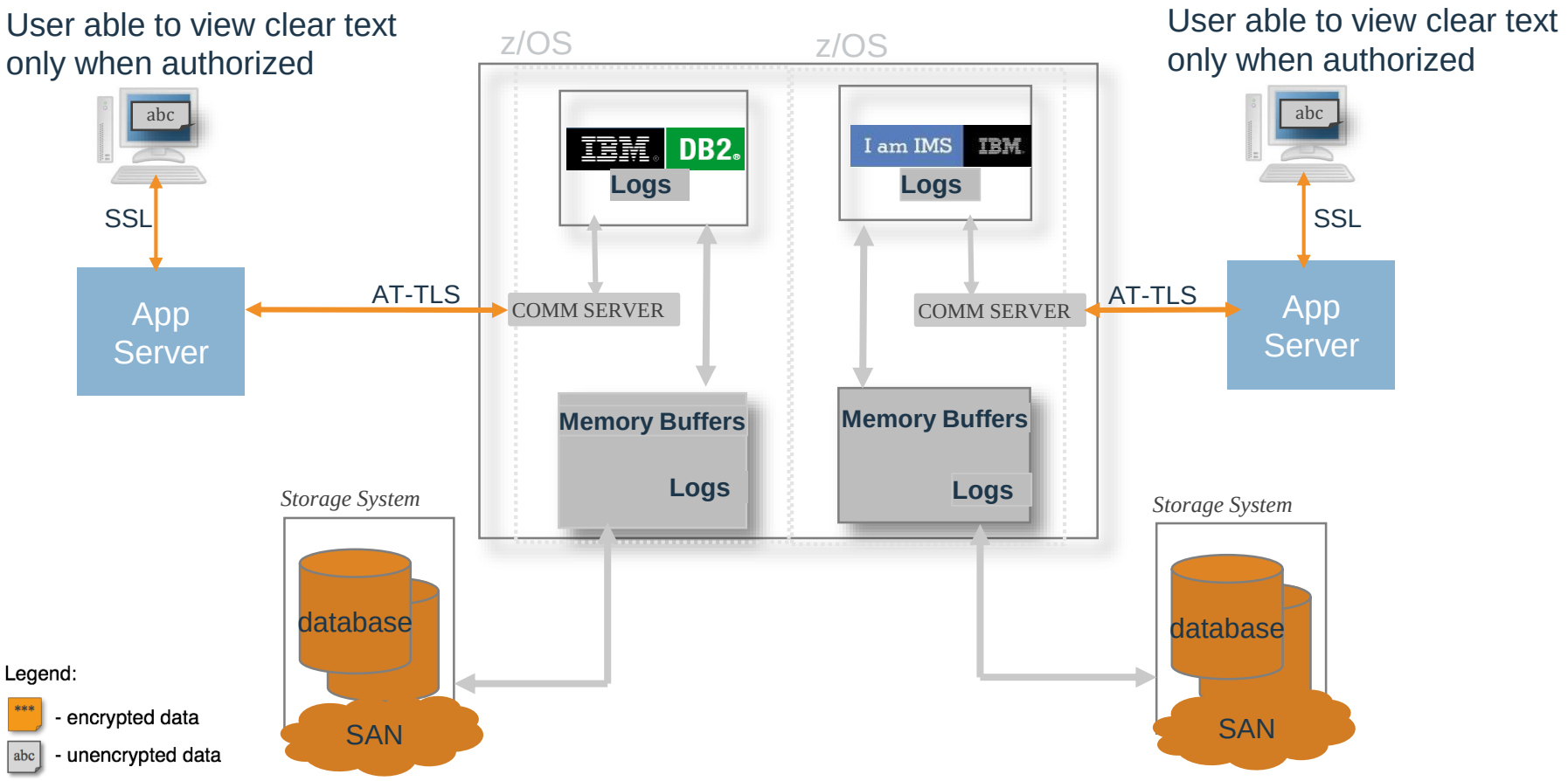
z/OS Database Encryption

- Helps to meet personal data privacy regulations (PCI-DSS,HIPAA, GDPR, etc)
- Honors DBMS access controls
  - Only decrypts authorized results
- Protects against clear text data exposures including:
  - Databases memory buffers and files
  - Log records
  - All dump types
- SOD on data access, key creation, controls, management
- Select which table(s) to encrypt
- Support all DB2 and IMS versions
- Prevents exposures on
  - Unauthorized viewing of encrypted sensitive data
  - Non-DBMS data access

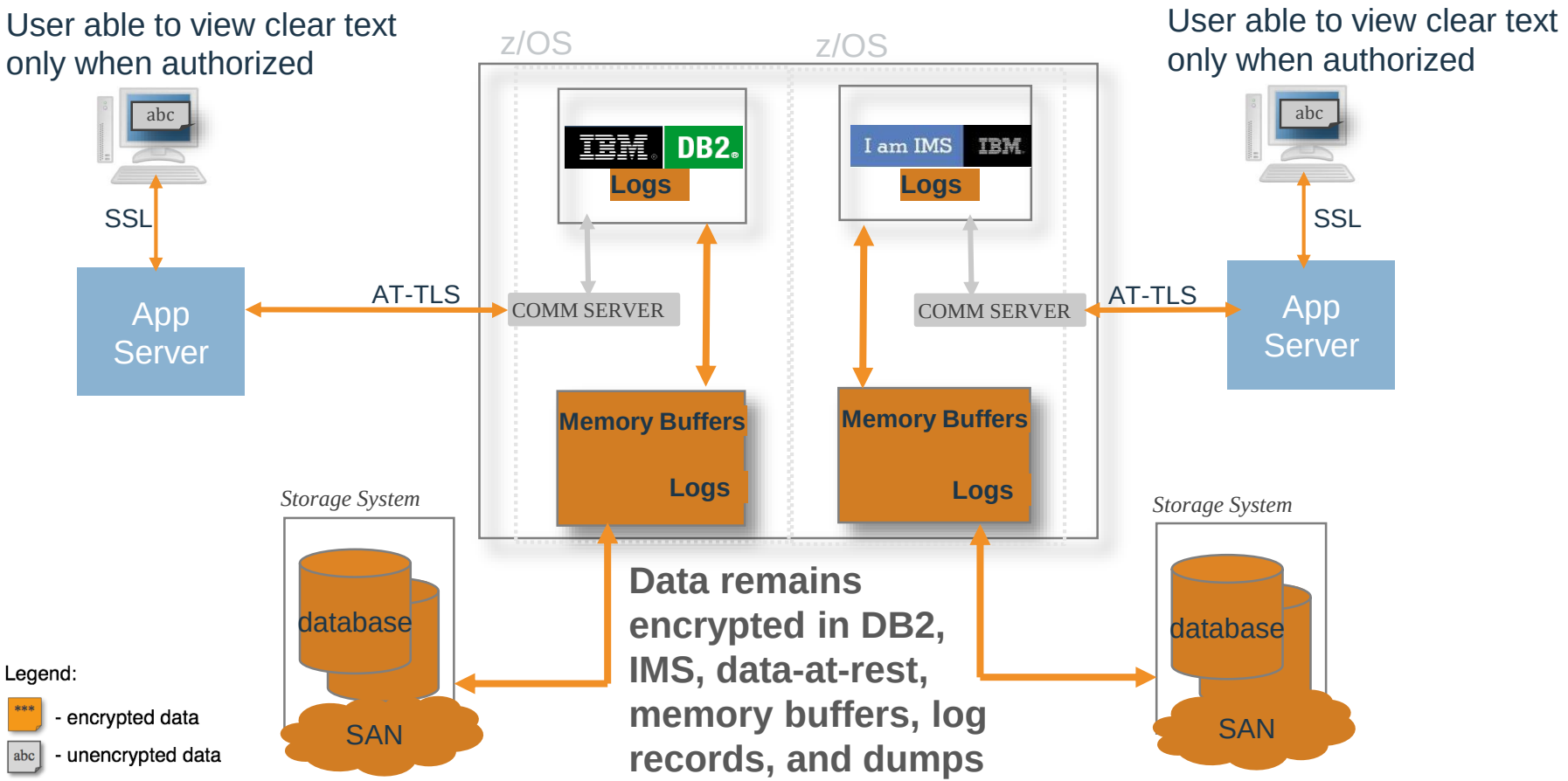
1 Statement of Direction* in the z/OS Announcement Letter (10/4/2016) - http://ibm.co/2ldwKo
* All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

2 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.

With Disk Level Encryption
Data encrypted only on while data-at-rest

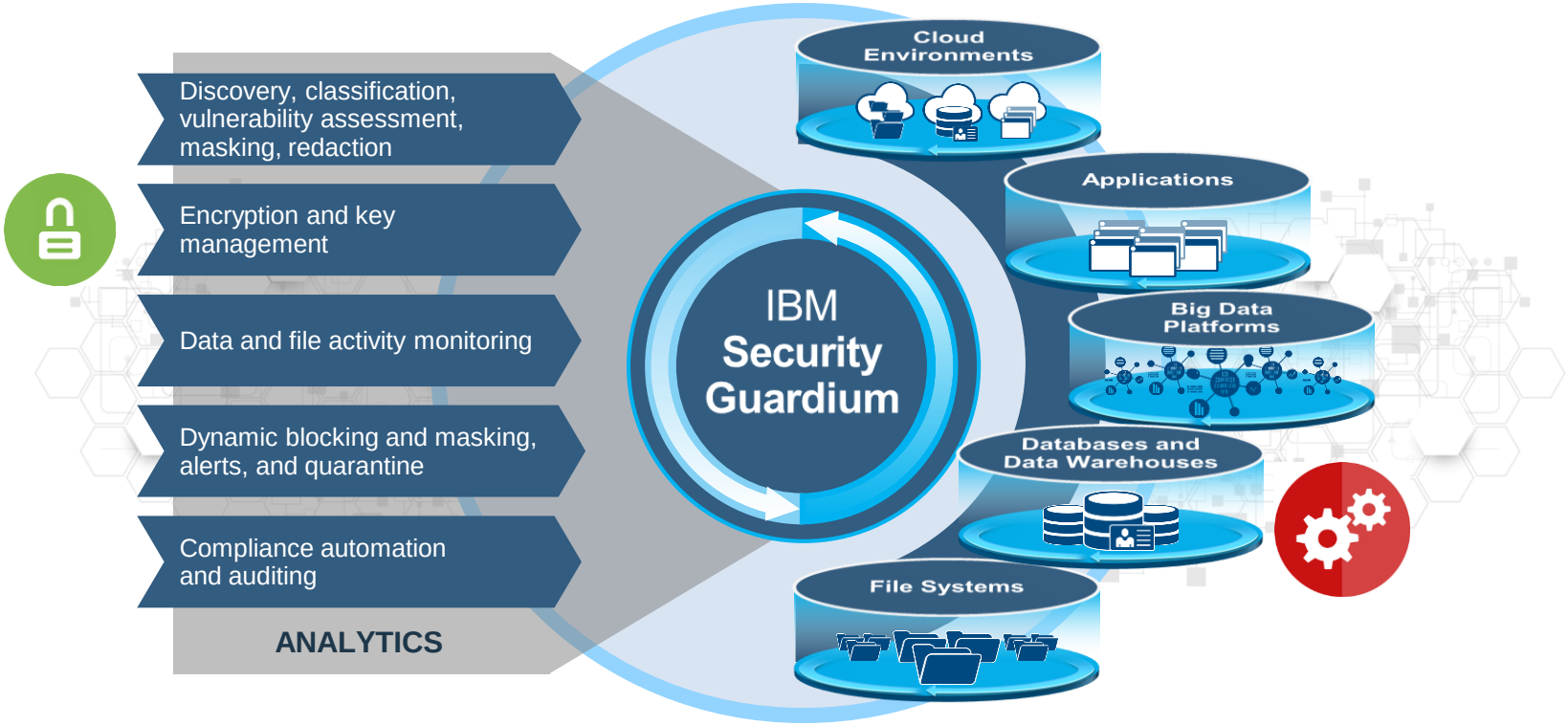


With Guardium Data Encryption for DB2 and IMS Databases Data Can Remain Encrypted Throughout



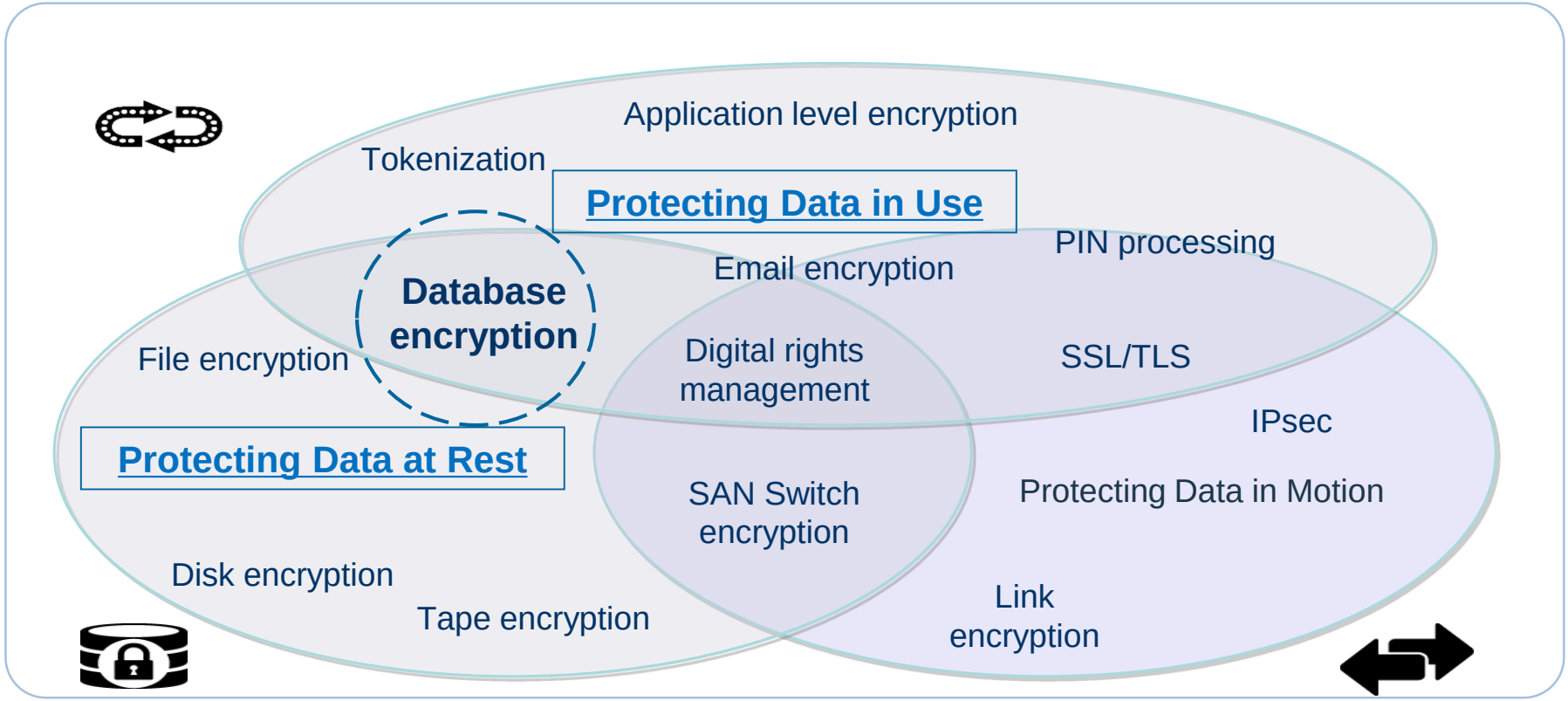
IBM Guardium Encryption is integral to data security

Know your sensitive data and intelligently safeguard it – wherever it resides



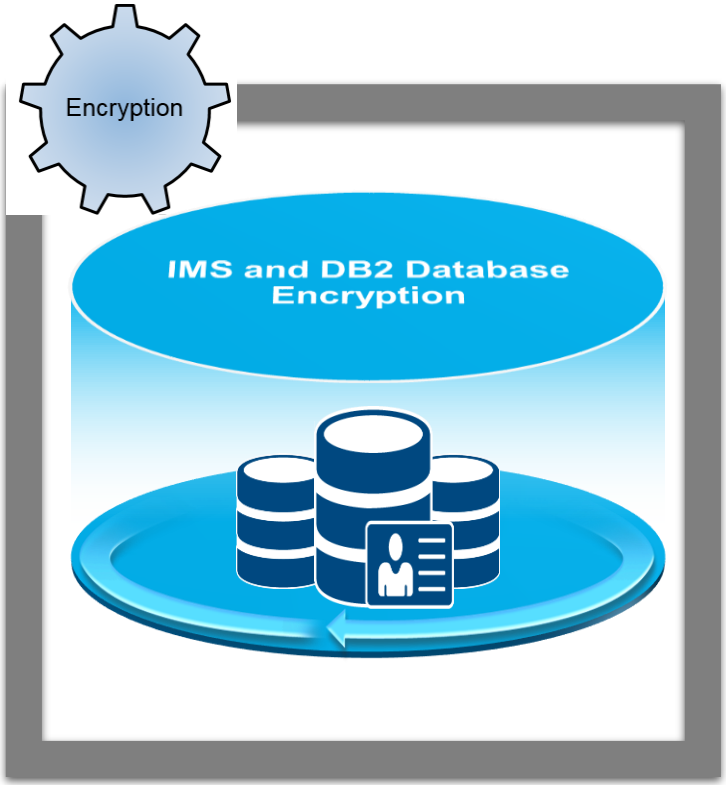
ANALYZE. PROTECT. ADAPT

IBM Security **Guardium Data Encryption for IMS and DB2** protects enterprise data on z/OS



IBM Security **Guardium Data Encryption for DB2 and IMS Databases** protects enterprise data privacy on z/OS

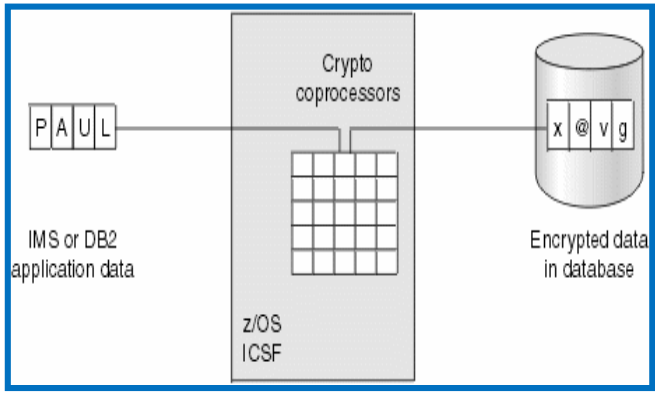
- Transparent to applications
- Provides Separation of Duty (SOD) - only authorized users may view the decrypted “clear” sensitive data
- Uses available System z or System z FIPS 140-2 compliant cryptographic hardware
- Conforms to the existing z/OS and OS/390® security model
- Protects Data-In-Use in memory buffers
- “Clear text” data cannot be accessed outside DBMS access methods

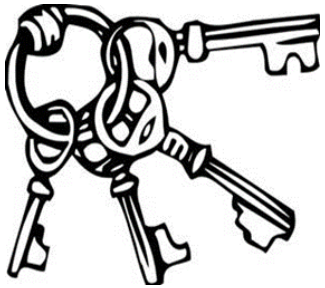


Guardium Data Encryption for DB2 and IMS Databases

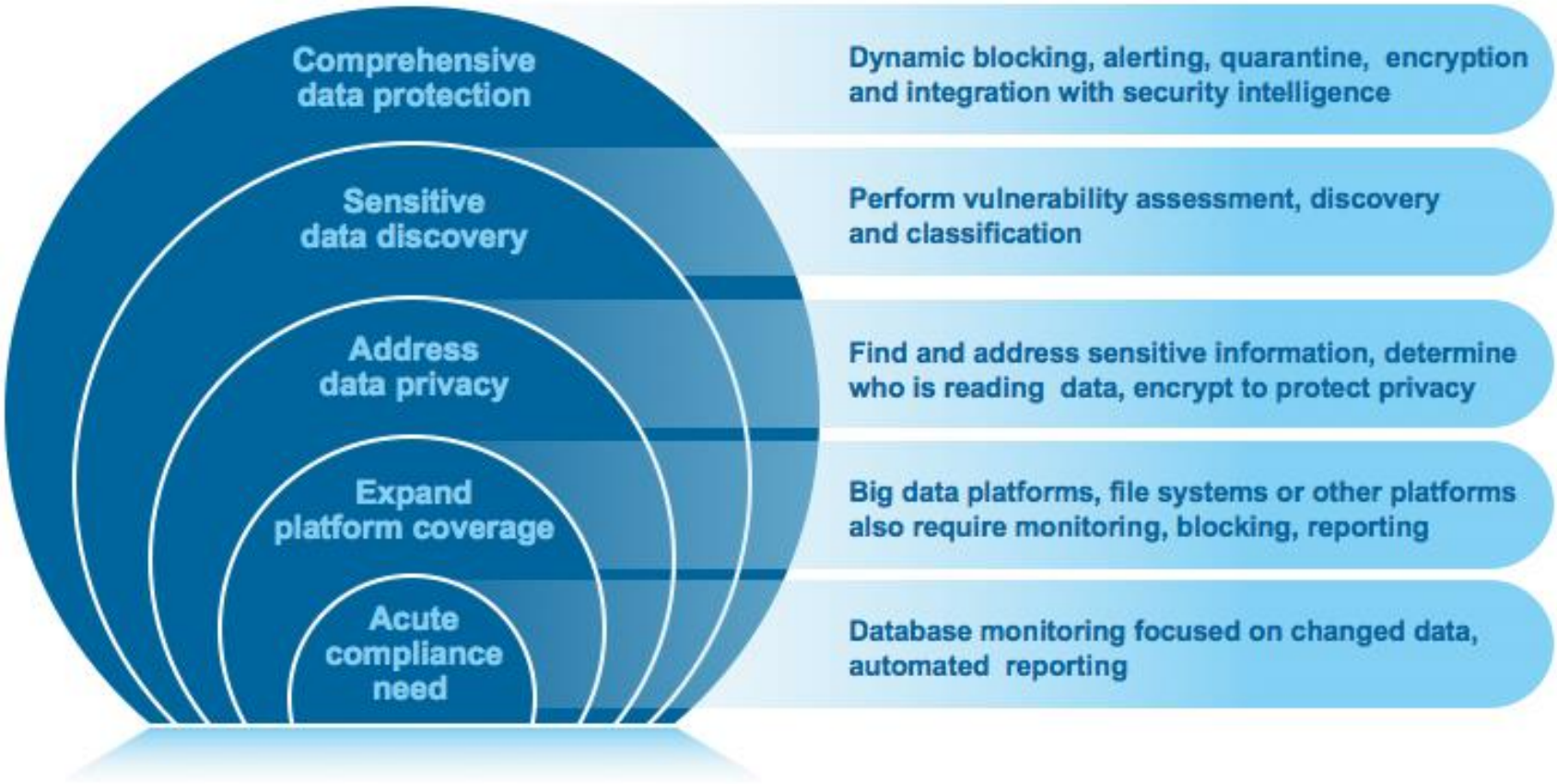
optimized for efficiency and performance

- Straightforward implementation using RACF key labels
- Controls access to sensitive data with RACF and DB2 fine grain access control
- Encrypts sensitive data at the DB2 table and column levels and IMS segment level for:
  - Performance
  - Low overhead
- Encrypts database transaction logs, image copy datasets, DASD volume backups
- Uses z/OS Integrated Cryptographic Service Facility (ICSF) services to protect sensitive data





Guardium supports the whole data protection journey



IBM Security

THANK YOU

FOLLOW US ON:

- ibm.com/security
- securityintelligence.com
- xforce.ibmcloud.com
- @ibmsecurity
- youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. Any statement of direction represents IBM's current intent, is subject to change or withdrawal, and represent only goals and objectives. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

IBM

Backup – Technical Details

Regulations Requiring Data Encryption

Regulation/Driver	Who is Effected?	Requirements
PCI DSS (Visa, MC, Discover, AMEX)	Major retailers and processors world wide	Encryption of credit card data with associated secure key management processes
HIPAA Security Standard (OCR)	Organizations that handle patient health information	Confidentiality, integrity and availability of patient health information
Data Breach Disclosure in over 50 Countries (Example: EU, South Korea, Turkey)	Publically held organizations or government agencies	Notifications and investigations of security breaches
Local Government Data Protection Acts (Local governments around the world)	Publically held organizations or government agencies	Encryption of sensitive data
Executive Mandates	Private and public organizations	Encryption employee and customer data
IP/Trade Secret Protection	Private and public organizations	Encryption and control access to intellectual property

Other data obfuscation terms you should know

Original Value
4536 6382 9896 5200

Masking

The ability to desensitize personal information and make it unreadable from original form while preserving format and referential integrity

- it is a one way algorithm – ie. No unmasking data
- SDM – Static Data Masking
- DDM – Dynamic Data Masking

Masked Value
4212 5454 6565 7780

Redaction

- The process of obscuring part of a text for security purposes.
- The ability to replace real data with substitute characters like (*)

Redacted Value
4536 6382 **** ****

Tokenization

- The process of substituting a “token” which can be mapped to the original value
  - Token is a non- personal data equivalent which has no extrinsic value
  - Requires a secured tokenization system to map between the tokens and the original values

Token Value
ABCD GDIC JIJG VXYZ

Encryption

- The process of encoding data in such a way that only authorized individuals can read it by decrypting the encoded data with a key
  - Format Preserving Encryption (FPE) is a special form of encryption

Encrypted Value
1@#43$%!xy1K2L4P

IBM and Business Partner Confidential

Key Types Side-by-Side

Clear Key

- Key material may be exposed in the storage of processor
- Key material may exist in the application address space
- Can be viewed in storage (via dump or on-line monitor)
- If correctly interpreted can expose data
- Sometimes acceptable for short-lived keys with other constraints
- Used in software-based cryptography
- APIs available via Integrated Cryptographic Support Facility (ICSF)
- Encrypt/decrypt operations performed by CPACF

Secure Key

- Key material is never exposed beyond the bounds of a secure tamper resistant card
- Key is encrypted under the Master key and stored in the CKDS
- Crypto Express 2, 3, 4, 5
- APIs available via Integrated Cryptographic Support Facility (ICSF)
- Can be used from Java on z/OS platform
- Encrypt/decrypt operations performed on the Crypto Express card

Protected Key

- Key material may be exposed in the storage of processor
  - Only if using clear key material as the source
- Can be viewed in dump of storage
- Crypto Express 2, 3, 4, 5
  - Not required if using clear key material as a source
- APIs available via Integrated Cryptographic Support Facility (ICSF)
- Encrypt/decrypt operations performed by CPACF

Which Encryption to Use

DB2 Native Encryption

Advantages

- No startup cost

Disadvantage

- Application changes needed
- TDES only
- Could increase MLC
- Only at column level, increase database size
- No SOD, key/password hints stored in DB2 catalog
- Password is open in more places in the clear
- Little adoption since v8

Disk Encryption

Advantages

- No application changes
- Zero z/OS overhead
- Encrypts ALL data
- No crypto express card
- Easy deployment

Disadvantage

- Anyone can see clear text inside the DBMS
- Does not prevent authorized users from seeing clear data outside of DBMS
- One key uses ISKLM to generates,
- Requires disks that supports encryption

GDEz

Advantages

- No application changes
- Strong SOD
- Optional increased security with crypto express card for tamper proof protection
- Encrypts buffer pools, logs, dumps
- Selective table & segment encryption
- Prevents authorized users from seeing data outside of the DBMS
- AES, TDES
- Multiple keys with associated data

Disadvantages

- Disruptive deployment
- Encrypts DB2/z & IMS only
- Index not encrypted
- For charge offering

© 2015 IBM Corporation

Guardium Data Encryption for DB2 for z/OS & IMS Databases
Program information for ordering

Program name	License PID	Charge metric	Value Unit exhibit
InfoSphere Guardium Data Encryption For DB2 & IMS Databases v1.2	5655-P03	Value Unit	VUE007

Program name number	S&S PID	Charge metric
InfoSphere Guardium Data Encryption For DB2 & IMS Databases v1.2 S&S	5655-P04	Value Unit

Value Unit exhibit VUE007

	MSUs minimum	MSUs maximum	Value Units/MSU
Base	1	3	1
Tier A	4	45	0.45
Tier B	46	175	0.36
Tier C	176	315	0.27
Tier D	316	+	0.2

© 2015 IBM Corporation

Highlighted Use Cases and Scenarios – GDE & GDEz vs GDEz

Use Case	GDE	GDEz
Customer wants to protect files and folders in an on-prem only storage environment	✓	✓▲
Customer desires wants to protect **files and folders** in a cloud based environment of over 250 servers	✓	
Can support thousands of agents (25,000+) In the cloud from a single on-prem Policy server	↗	
Customer desires to protect **volumes** (mounts/containers) in the cloud but keep control of encryption keys and policy management on-prem		
Customer desires to manage their policies with a FIPS-140-2 Level 2 hardware appliance	✓	✓▲
Customer desires to protect **files and volumes** stored **concurrently across multiple clouds** while keeping their policy management and keys under local control		
Customer desires to move their encrypted files and folders (and VMs) to new clouds, without having to decrypt or re-encrypt them		✓▲
Customer wishes to protect files and folders stored in a z-environment		✓▲
Customer wishes to store their encryption keys in a KMIP certified, FIPS-compliant key manager (SKLM)		
Customer desires to leverage “Armored Z” technology for encrypting files or folders while keeping encryption keys under separate control using their existing SKLM infrastructure		
Customer wants to leverage REST API interfaces	✓	
Customer wants to limit Admin and Root user access to clear data in the cloud		
Customer wants to protect files and folders with a FIPS 140-2 certified solution	✓	✓▲
Customer desires a high-performance data protection solution with no impact to operations	✓	✓▲
Customer wants a simple, single pane of glass, management console for data protection and policies	↗	
Customer desires cryptographic separation between Policy defined access controls		✓▲
Customer wants to create role-based definitions for access control	✓	RACF
Customer needs to audit all access logs via SIEM	✓	DP

Legend:
✓ Yes, ◆ Technically possible (but not advocated), ↗ Future Enhancement
▲ IMS and DB2 Managed Files only **DP** Guardium Data Protection

IBM Confidential
© 2015 IBM Corporation

Comparison of Supported DB2 Encryption Methods

Function	EDITPROC	FIELDPROC	UDF
Row based encryption	✓		
Column based encryption		✓	✓
Application impact during implementation (Drop/CREATE) [1]	✓	✓ maybe	
SQL based implementation			✓
“Clear Key”	✓ AES, TDES/DES		
“Protected Key”	✓ AES, TDES/DES	✓ AES	✓ AES
“Secure Key”	✓ AES, TDES/DES		

Data Encryption Comparison

Properties	Self Encrypting Devices	DB2 Built-in	EDITPROC	UDF	FIELDPROC
Satisfies PCI	Maybe for data at rest requirement	App Dependent	Yes , For data at rest and in flight to/from application.	Yes , For data at rest and in flight to/from application.	Yes . For data at rest and in flight to/from application.
Complexity	No Application Changes.	Complex Application Changes	No Application Changes	Only impacts Applications that need Encryption	No Application Changes
Implementation	Mount encryptible volume on appropriately configured drive.	ALTER and RELOAD	DROP and RELOAD	SQL UPDATE	DROP and reload unless ALTER ADD column
Clear Passwords	No	Yes	No	No	No
Access Control	No application security provided	App Managed	Table Level	RACF secured UDF	Column Level
Device Hardware	Yes.	No	No	No	No
Key Control	IBM Security Key Lifecycle Manager	Stored in the DB2 Catalog	ICSF or IBM Security Key Lifecycle Manager	ICSF or IBM Security Key Lifecycle Manager	ICSF or IBM Security Key Lifecycle Manager
Application Maintainability	Transparent	Transparent	Transparent	Requires SQL to invoke On-Demand Processing	Transparent
Performance	Best	App Dependent	Acceptable	Overhead for encrypted column	Acceptable
Index Encryption	Yes	Yes	No	Yes	Yes, but SQL Predicate Processing is Negated
Data Protection	Only protect on media	Clear Key	Unload Data in clear	Always Protected	Unloaded Data is clear
Data Type Independence	Yes	Yes	Most data types	Yes	Only CHAR/VARCHAR < 255 bytes Columns

IBM Confidential