Pervasive Encryption
In the Digital Enterprise

May 18, 2017

Michael Jordan
IBM Distinguished Engineer
Data protection and compliance are business imperatives

“It’s no longer a matter of if, but when…”

26% 🧟‍♂️
Likelihood of an organization having a data breach in the next 24 months ¹

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

$4M
Average cost of a data breach in 2016 ²

European Union General Data Protection Regulation (GDPR)
Payment Card Industry Data Security Standard (PCI-DSS)
Health Insurance Portability and Accountability Act (HIPAA)

3 Source: Breach Level Index -- [http://breachlevelindex.com/](http://breachlevelindex.com/)
Extensive use of encryption is one of the most impactful ways to help reduce the risks and financial losses of a data breach and help meet complex compliance mandates.

However, 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.
Application changes are costly

- People
- Skills
- Ongoing maintenance
- Application lifecycle

Application outages to implement encryption
Updates for regulatory changes
Key management
New business requirements
The net is that organizations need a better way to protect the data at the core of their enterprise.
Data is the new perimeter

A transparent and consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify & reduce the costs associated with protecting data & achieving compliance mandates.
## Pervasive Encryption with IBM z Systems
*Enabled through tight platform integration*

<table>
<thead>
<tr>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Encryption</td>
<td>Protect network traffic using standards based encryption from end to end, including encryption readiness technology² to ensure that z/OS systems meet approved encryption criteria</td>
</tr>
<tr>
<td>Data Set &amp; File Encryption</td>
<td>Protect Linux file systems and z/OS data sets¹ using policy controlled encryption that is transparent to applications and databases</td>
</tr>
<tr>
<td>Coupling Facility</td>
<td>Protect z/OS Coupling Facility² data end-to-end, using encryption that’s transparent to applications</td>
</tr>
<tr>
<td>Secure Service Container</td>
<td>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</td>
</tr>
</tbody>
</table>
| Integrated Crypto Hardware| Hardware accelerated encryption on every core – CPACF  
PCle Hardware Security Module (HSM) & Cryptographic Coprocessor – Crypto Express5S |

*And we’re just getting started ...*

---

¹ Statement of Direction* in the z/OS Announcement Letter (10/4/2016) - [http://ibm.co/2ldwKoC](http://ibm.co/2ldwKoC)
² IBM z/OS Version 2 Release 3 Preview Announcement Letter (2/21/2017) - [http://ibm.co/2J43ctN](http://ibm.co/2J43ctN)

* All statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.
Data Protection // z/OS Dataset Encryption

Protection of data at-rest

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
- Supports: CICS, DB2, IMS, Logger, DIV, & zFS

In-memory system or application data buffers will not be encrypted
DS8000 Disk Encryption
Encrypting disk drives protect data at rest when disk drives are retired, sent for repair or repurposed

Once the key has been served to storage system any system connecting to storage system can retrieve unencrypted data
Data Protection // Coupling Facility Encryption

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

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!
**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 // 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

**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*
A Paradigm Shift

*From selective encryption to pervasive encryption*

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

The practice of pervasive encryption can also:

- 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
Encryption by Policy

Automatic data protection

Organizations can protect data by encryption policy to:

• Avoid the need for costly application changes
• Protect data automatically, before it’s created
• Encrypt data in bulk, at coarse scale
• Simplify and reduce the cost of compliance

Using encryption that:

• Is transparent to applications
• Is tied to access control
• Uses protected encryption keys managed by the host system
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

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.
Multiple Layers of Encryption

Robust data protection

App Encryption
hyper-sensitive data

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

File or Dataset Level Encryption
Provide broad coverage for sensitive data using encryption tied to access control for in-flight & at-rest data protection

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

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

Database Encryption

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

File or Data Set Level Encryption

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

Full Disk & Tape 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

File or Data Set Level Encryption

- Broadly encrypt data at rest
- Covers VSAM, DB2, IMS, Middleware, Logs, Batch, & ISV solutions

Database Encryption

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

App Encryption

- Hyper-sensitive data
- Tied to access control
- Uses protected encryption keys managed by the host

Full Disk & Tape Encryption

- Encrypt in bulk for low-overhead
- Utilizes IBM z Systems integrated cryptographic hardware

Protection against intrusion, tamper or removal of physical infrastructure

Broad protection & privacy managed by OS... ability to eliminate storage admins from compliance scope
**Multiple layers of encryption for data at rest**

*Robust data protection*

---

**IBM Security Guardium Data Encryption for DB2 and IMS Databases**

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

---

**Database Encryption**

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

---

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

---

Protection against intrusion, tamper or removal of physical infrastructure

---

Data protection & privacy provided and managed by OS... ability to eliminate storage admins from compliance scope

---

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

---

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

---

Clear text data cannot be accessed outside DBMS access methods

---

[Image]
Multiple layers of encryption for data at rest

Robust data protection

Application Encryption

- 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

Database Encryption

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

File or Data Set Level Encryption

- Encryption tied to access control for in-flight & at-rest data protection
- Applications must be responsible for key management

Full Disk & Tape

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

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

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

Building an effective Security Immune System is essential to protecting the data at the core of the enterprise.

Encryption is the solid foundation upon which a robust immune system is established.

Applies to ...
- Traditional Workloads
- Hybrid Cloud
- APIs
“It’s not a matter of if, but when.”

A large financial services organization, running it’s core business applications on IBM z Systems, is incredibly concerned with reputational risk and staying out of the headlines for the wrong reasons. In addition, they are encumbered by a revolving door of internal and external auditors, and inspections and inquires from their clients.

“Our CEO made a mandate that all of what we consider NPI — confidential-type information — must be encrypted.”
Thank You