October 2018

# Understanding and removing barriers to the adoption of Pervasive Encryption


**Mark Moore**
Software Architect
IBM Competitive Project Office

# Table of Contents

## Executive Summary

The environment in which data security strategies are being determined is decidedly hostile. The number of breaches is up. The breach at a large American retailer shows that being compliant with industry standards, as they were, may not be sufficient. Insider jobs at other companies has resulted in the loss of millions of records and in each case show that data security is much more than a firewall and good locks on the data center doors. The European General Data Protection Regulation (GDPR) is just the latest example of governments protecting citizens by cracking down on security.

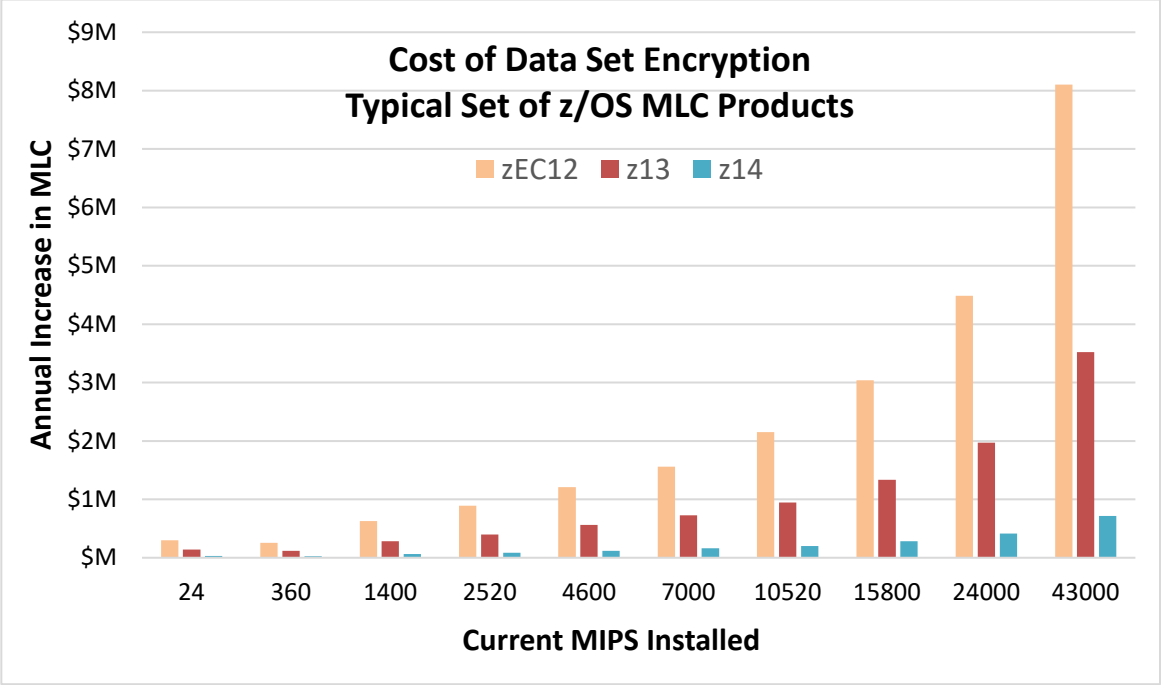
GDPR specifically calls out encryption as a path to data security, helping to ensure that access to data is provided only to those with functional requirements for it. However, encryption is often perceived as complex and computationally expensive. It raises concerns of cost, implementation difficulty, and potential data loss. These concerns can form barriers to implementing encryption or result in an implementation that is less than total.

IBM z14™ and IBM LinuxONE™ are built to help secure enterprise data by encrypting it at rest and in flight. They address concerns of cost by enabling the encryption of data without modification to applications and without impact to SLAs. They ensure data in flight is not only encrypted but encrypted to adequate standards. Each core has symmetric key cryptographic co-proccessing, CPACF, which implements AES cryptography in several modes. Common Criteria EAL5+ certified isolation provided by the type-1 hypervisor, PR/SM™, defends against side-channel attack on workloads. The hardware security module (HSM), Crypto Express6S, is designed to meet FIPS 140-2 level 4. That provides, as part of its comprehensive feature set, the highest level of protection for cryptographic keys identified to date.

As a result, we believe z14 and LinuxONE are uniquely qualified to provide cryptographic security for enterprise data.

## Cost-Effective Data Security

For mainframe customers, encryption immediately raises the concern of increased monthly license charges (MLC). It is thought that the overhead associated with encrypting and decrypting data sets could significantly increase MIPS and, as a result, costs. However, this is largely a fear of the unknown.

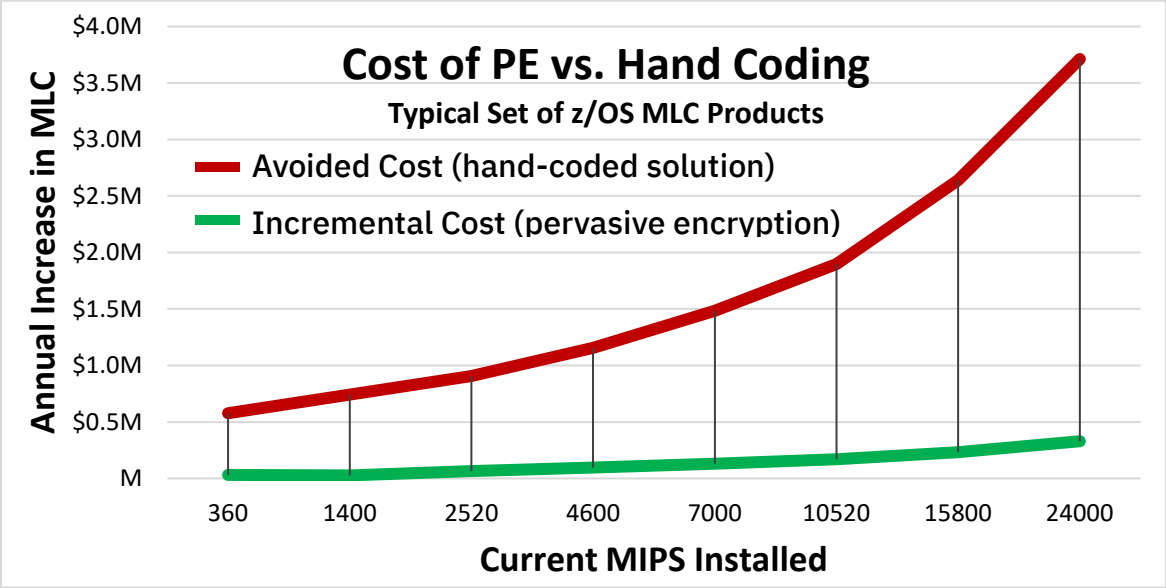



*Source: IBM internal study. Assumptions: MIPS acquisition cost is $1500/MIPS. Amortization over 5 years. Typical IPLA additional cost of 30% over MLC. Other costs are flat. ISV licenses not included*

With z14, the computational cost of data set encryption has been reduced to a negligible level. A survey of customers' performance data shows that on IBM z13®, overhead with data set encryption would have been more than 10%, on z14 that overhead is, on average, just 2.6%.1 The cost of data set encryption for a typical basket of z/OS® MLC products on z14 is 20% of what it was on z13.2

[1] Data provided to IBM from customers during development of IBM Z Batch Network Analyzer support for data set encryption. Values ranged from 1% to 8% on z14 and 3% to 35% on z13.
[2] IBM internal study conducted by IBM IT Economics Team using a composite customer profile built from customer engagement data.

Still, a frugal z14 owner might try to minimize costs further by encrypting minimally. Rather than encrypt entire data sets, one might attempt to modify applications to encrypt only the data required to become compliant with an industry regulation or law. There are challenges to this. First, one must be able to locate the data. 59% of respondents to a 2017 Ponemon study3 said that discovering where sensitive data reside is their most difficult challenge – the result of data proliferation, moving workloads to the cloud, and a growing number of end points. Even if sensitive data is located, it is not static. Data changes, as do regulations, and there is overhead associated with maintaining application changes to account for those changes.




*Source: IBM internal study*

On the other hand, encrypting entire data sets is sure to catch all sensitive data and does not require maintenance as data and regulations change. Additionally, because the overhead of data set encryption on z14 is low, encrypting data sets pervasively is more economical than attempting to encrypt minimally. As the graph above shows, the more MIPS one has deployed, the more economical it becomes.4

[3] Global Encryption Trends Study, April 2017, Ponemon Institute

[4] Study replicates a typical IBM customer workload usage in the marketplace. The results were obtained under laboratory conditions, and not in an actual customer environment. IBM's internal workload studies are not benchmark applications, nor are they based on any benchmark standard. As such, customer applications, differences in the stack deployed, and other systems variations or testing conditions may produce different results and may vary based on actual configuration, applications, specific queries and other variables in a production environment

## Complying with Regulation and Minimizing Audit

Though it is European legislation, GDPR is affecting organizations far beyond Europe's borders. The fines for violations can scale up to the greater of €20M or 4% of worldwide revenue. GDPR specifically mentions pseudonymizing data as one of several ways to protect data. Encryption is specifically noted as a method of pseudonymizing data.

In addition to securing data in the event of a breach, encryption can eliminate entire classes of users from consideration in an audit. Using the case of a storage administrator as an example, if such an administrator needs access to a database to relocate it to a new storage device, that access normally includes the ability to see what's inside a database. However, if the administrator has access to the database, but the database itself is encrypted, the administrator can still perform their task, but cannot see the data. An auditor can verify that a database is encrypted, that the administrator has no access to the key for the database, and end that should be the end of the line of investigation there.

Using this technique, encryption can be applied at a variety of levels in combination with access control to implement very fine-grained data access rules:

Disk and Tape encryption, supported in the storage device itself, enables offline media to be removed without fear of data loss due to content theft or misuse. No special action is required to repair, repurpose, or retire media. However, once media is mounted and unlocked, its data is visible to all with access to the machine.

File and Data Set encryption goes a step further, enabling storage administrators to handle these objects. Anyone with functional access to the application, or a DBA with direct access, can see the data.

Database encryption enables row and column level encryption to protect data from a DBA and from application users that don't have access to that data. For example, most of a client's data may be available to all users, but a tax identification number may be available only to a subset of users.

Application-level encryption may be required in extreme cases to provide access in only particular cases … perhaps with more than one user required to unlock data.

Encryption of data sets on z/OS can be done as a matter of policy. This means that not only can existing data sets be encrypted, but data sets not yet in existence can be automatically encrypted at the time they are created. Using RACF® to control the access to data sets and, separately, access to the keys required to read the data sets, enables the implementation of sophisticated data security policies that not only keeps data safe, but reduces audit time and expense.

Although Linux does not have anything strictly analogous to a z/OS data set, Linux® on IBM Z® and LinuxONE do enjoy the hardware support for cryptography in things like the Linux kernel module, dm-crypt for full-disk encryption. Secure keys, discussed further in the next section, can be used to with

cryptsetup to encrypt and decrypt disks. Many other Linux features are similarly enhanced to leverage IBM Z and LinuxONE cryptography support.

## Notes on Implementing Pervasive Encryption

The z/OS facility for managing the operational keys for data set encryption is Integrated Cryptographic Services Facility (ICSF). It is recommended that these keys be "secure keys". Secure keys are operational keys that are encrypted using a key present in the Crypto Express card, the master key. A bad actor with a copy of a data set and its secure key cannot read the data because they do not have the master key. The FIPS 140-2 level 4 design and construction of the Crypto Express card is designed to ensure that the master key cannot be extracted.

When a data set is opened, the secure key is passed to the Crypto Express where it is decrypted and passed through firmware to a CPACF where it is reencrypted with a transient key available only to the Z firmware while the partition using the key is running. That newly encrypted key is passed back to ICSF where it is cached. Whenever the operational key is needed, it is unwrapped by the CPACF. The unwrapped "clear key" is never exposed to any partition – there is never an opportunity for malware possibly installed in the partition to capture it.

When an existing data set is encrypted, its data will have to be read in its initial, unencrypted state and written as encrypted. Benchmarking performed by IBM shows that data can be encrypted at 9.25 GB/s per z14 core.5 To calculate a z14's capacity based on installed MIPS, that works out to approximately 198 MIPS per GB/s. With those numbers in mind, a rough calculation can be done to determine the time and resources required to encrypt data sets. If there is not sufficient time to perform the encryption without affecting the 4-hour rolling average, additional hardware can be added temporarily.

Encrypted data cannot be compressed. If compression implemented in storage devices is being used, it will stop working. Data must be compressed on the host. IBM provides zEnterprise® Data Compression (zEDC) for this. When used, data is compressed before being encrypted. The work of compression is offloaded to an add-on card. As a bonus, after compression there is less data to encrypt, reducing encryption time.

The IBM Z Batch Network Analyser (zBNA) is a PC-based tool that can analyze metrics from a data set at work to determine the performance impact of encrypting that data set. It can also compute the potential performance improvement that would result from a hardware upgrade. Finally, zBNA also identifies good candidates for compression with zEDC.

In larger environments, a Trusted Key Entry workstation (TKE) helps to manage multiple Crypto Express cards and domains. Enterprise Key Management Foundation (EKMF) can provide enterprise-wide operational key and certificate management across a variety of platforms.

[5]Tested using OpenSSL speed test, AES-256, XTS mode under laboratory conditions.

For network traffic, z/OS Encryption Readiness Technology (zERT) provides a single source of information to determine which traffic is cryptographically protected and which is not. For the traffic that is cryptographically protected, the attributes of that protection can be determined.

## Expanding the Reach of Pervasive Encryption

IBM Z is not an island. It exists alongside other platforms and as a component of a variety of strategies. Cloud looms large as one of those strategies, but security is seen as barrier to moving to cloud.

z/OS assets may be delivered to the cloud in the form of RESTful APIs. Application Discovery and Delivery Intelligence (ADDI) can visualize the potential of applications and identify candidate services. z/OS Connect can deliver those RESTful services, mapping back to existing mainframe services and data.

IBM Cloud Private (ICP) can help here, as well. Based upon the popular container technologies, Docker and Kubernetes, ICP enables the confident migration of workloads beyond the data center walls.  Easy to scale and highly reliable (IBM Z and LinuxONE can deliver a mean time between failure measured in decades6), ICP provides cost advantages as well. IBM Z Linux running a sample ICP workload provide 7.2 times the throughput at 22% lower cost on compared commodity x86 servers in an internal study. 7

IBM Secure Service Container for IBM Cloud Private is an IBM Z and LinuxONE-based appliance that provides Common Criteria EAL 5+ certified isolation for virtual machines – similar to certification levels for commercial air gapped machines – and as much as 16 TB of physical memory. Data at rest and in flight is encrypted. Boot components are signed and verified. Its Linux operating system is hardened and locked-down, providing no access to a command-line prompt. Administration is through only tightly-defined interfaces. This compares very favorably with Skylake's approach to protected execution which provides only a 128 MB encrypted "enclave" in an environment that is not otherwise isolated, and so far more exposed to side-channel attack.8

[6]Kathy Guarini, Vice President IBM LinuxONE Offerings, https://www.mainline.com/linuxone/
[7]Costs included hardware (production and HA), software (hypervisor, OS, ICP, and MongoDB), plus applicable maintenance costs, and labor, power, and space. Costs calculated over a 3-year term. Tested on 64 Skylake cores (Intel® Xeon® Gold 6140 @ 2.3GHz) across 4 servers vs 6 LinuxONE Emperor II or z14 IFLs on a single server.
[8] SSC and SGX are different technologies and secure applications and portions of applications in different ways.  As such, a straight-line comparison is difficult. The claim and its substantiation are made in the context of common enterprise application development and how each technology would secure the operation of the business logic and data. https://arxiv.org/abs/1702.08719 and Intel® Software Guard Extensions SDK for Linux* OS Developer Reference, 2016. More about PR/SM isolation here: https://tinyurl.com/y9mo9wte

## Superior Data Security, Competitively Priced, with a Variety of Approaches

Securing customer and enterprise data is an imperative. Data loss can result in significant financial loss and, perhaps worse, loss of reputation. However, the amount of data collected is growing by the minute, the definition of sensitive data is changing all the time, and data is proliferating quickly. Attempting to tightly scope what data is to be encrypted can be both expensive and error-prone.

The pervasive encryption approach of z14 and LinuxONE ensures that sensitive data is encrypted because all data is encrypted, at rest and in flight. Tools are provided to measure the impact of Pervasive Encryption before it is implemented. Encryption may be implemented at a variety of levels to provide fine-grained control, reducing risk and eliminating people from audit consideration since they will no longer be able to access data unless it is necessary.

Leaving data on the z14, where it is protected, it is possible to open applications to the cloud through RESTful services provided by z/OS Connect. Additionally, entire workloads maybe hosted in-house or in the cloud in highly secure containers.  Data currently hosted on commodity Linux servers can be protected by migrating those workloads to IBM Z or LinuxONE.

IBM Z and LinuxONE are qualified to cryptographically secure enterprise data.


IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
10/18



86019886-USEN-00