September 2019

Compression and Pervasive Encryption

z15 Offers the Best of Both Worlds

IBM **IT Economics Consulting & Research**

Securing your data with pervasive encryption on IBM Z

The size and frequency of data breaches are growing at an alarming rate. The average data breach now affects over 25 thousand records and costs almost $4 million[1]. Nearly eight billion data records were breached in 2017 alone and 96% of them were not encrypted[2]. Had that data been encrypted, and the encryption keys secured, the risk of exposure would have been vastly diminished.

With the launch of IBM z14™ in 2017, IBM announced that its hardware included additional encryption features (CPACF) embedded in the processor chip, reducing the increase in CPU utilization to the low single digits; on average, around 2.6%. This number was derived by measuring the MIPS overhead for 23 different clients when encrypting their z/OS® datasets and represents the average of all values measured. The ability to encrypt data, both at rest and in flight, for a very low cost, was great news for customers concerned about data security.

Labeled pervasive encryption, the capability was designed to eliminate many "non-functional" roles as potential sources of data loss. Non-functional roles are those that are not involved in the primary function of workloads running on the system. A storage administrator, for example, is such a role. The storage administrator needs to be able to move a database from one storage device to another but does not need access to the data content inside the database. If the database is encrypted and the administrator has no access to the encryption key, they cannot access the data.

Combining compression with pervasive encryption

A side effect of encrypting the data on z14 is that it renders storage-level compression ineffective, because once you've encrypted data, it is not readily compressed. A zEnterprise® Data Compression (zEDC) card could be used to compress the data before encryption, but that is an added expense.

On IBM z15™, with the Integrated Accelerator for zEnterprise Data Compression, the industry standard compression used by zEDC is now built into the z15 core, very much like encryption is with CPACF. Now customers can have the best of both worlds with compression and encryption (in that order) right on the processor cores. Encryption becomes even less expensive, since after compression, there is much less data to encrypt.

Figure 1 illustrates the MIPS savings experienced when encrypting compressed data versus uncompressed data. In this example, the red line shows the MIPS consumption of the computational overhead of encrypting uncompressed data on a IBM z13®, and the blue line shows the used MIPS for encrypting data that has been compressed using a zEDC card. Data is shown for 3 phases during a day with different workload profiles. Phase 1 (midnight to 7 am) has low almost no data to encrypt, phase 2 (8 am to 3 pm) has somewhat higher encryption activity, whereas phase 3 (4 pm to 11pm) has a high amount of data to encrypt. Since measurements in phase 3 are not taken every hour, only the spikes are relevant.

[1] 2019 Ponemon Cost of a Data Breach Study - https://www.ibm.com/security/data-breach

[2] DarkReading 019 Smashed World's Records for Most Data Breaches, Exposed Information - https://www.darkreading.com/attacks-breaches/2017-smashed-worlds-records-for-most-data-breaches-exposed-information/d/d-id/1330987

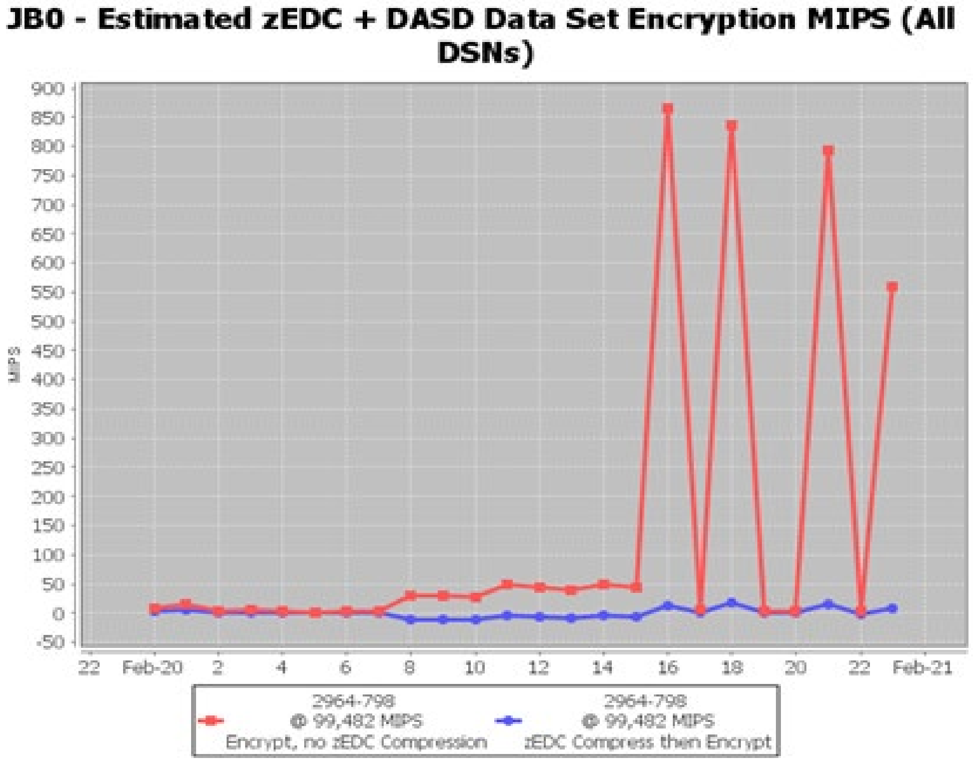


Figure 1: MIPS consumption comparison of encrypting uncompressed data (red line) versus zEDC compressed data (blue line)

Figure 2 gives an example for the financial cost savings, where the MSU cost for encryption of data sets on z14 is measured for uncompressed data and zEDC compressed data, respectively.

Compression	Encryption (MSU) 7 days	Encryption (MSU) Year	Average cost/MSU (€)	MSU Cost (€)
No	213	11,106	1	11,106
Yes - zEDC	76	3,962	1	3,962

Figure 2: MSU cost comparing encryption for uncompressed and zEDC compressed z/OS data sets in Euros

The cost and benefits of Pervasive Encryption

The two major cost components of encryption are infrastructure (hardware, software) and labor, namely the effort to implement and administer encryption features.

We have shown how compressing the data before encrypting it can reduce the infrastructure cost on z14. This should be even more pronounced on z15 with Integrated Accelerator for zEnterprise Data Compression. Combining Integrated Accelerator for zEDC compression with BSAM/QSAM file encryption on z15 showed an improvement in elapsed time by up to 72% while reducing CPU by up to 7% compared to not using compression and encryption[3]. zEDC compression on z14 has an average compression ratio of around 6 to 1 or 7 to 1[4], and early measurements on z15 show a compression ratio of around 8.5 to 1 on SMF data.

Potentially, there are four labor constituencies that could benefit from pervasive encryption, namely security administrators, systems administrators and operations, application programmers, and users. Our analysis focuses on the two middle groups.

Pervasive encryption, which requires no application changes, can result in a 3-5% savings in administrative and application development labor costs based on an IBM internal study where it was compared to hand coding a selective encryption solution, which requires a thorough understanding of every data element and which must be considered sensitive and therefore encrypted, and then generates significant DevOps effort for code, test and support, with the resulting in administrative overhead[5].

Figure 3 shows the incremental cost vs. the estimated benefit for enabling pervasive encryption for z/OS data sets for different sizes of installed MIPS. The incremental cost is calculated using a typical market basket of software products[6] and a 2.6% increase in MIPS when pervasive encryption is enabled. The estimated benefit is based on labor savings when selective encryption is hand coded.

The cost-benefit analysis shows a major return on investment (ROI) of Pervasive Encryption for all customer sizes, driven by a reduction of the operational cost.

[3] Measurements were conducted on both z14 and z15 using 2 CPs and executed using a batch job workload accessing BSAM and QSAM sequential files. This workload consists of 18 I/O intensive utility jobs copying large amounts of data. Measurements completed in a controlled environment. Results may vary by customer based on individual workload, configuration and software levels.

[4] https://www.intellimagic.com/resources/blog/good-zedc-card/

[5] Pervasive encryption on z/OS can result in approximate savings of 3-5% in administrative and programming labor costs, based on an IT Economics analysis. Pervasive Encryption relieves programmers and system administrators from having to selectively implement encryption for their data and programs. Cost benefits ranging from 3- 5% are estimated based on a labor model of headcount derived from IT Economics assessments for client environments. Results may vary by customer.

[6] Market basket products include z/OS, Db2, CICS, COBOL, Db2 QMF and WAS MQ.

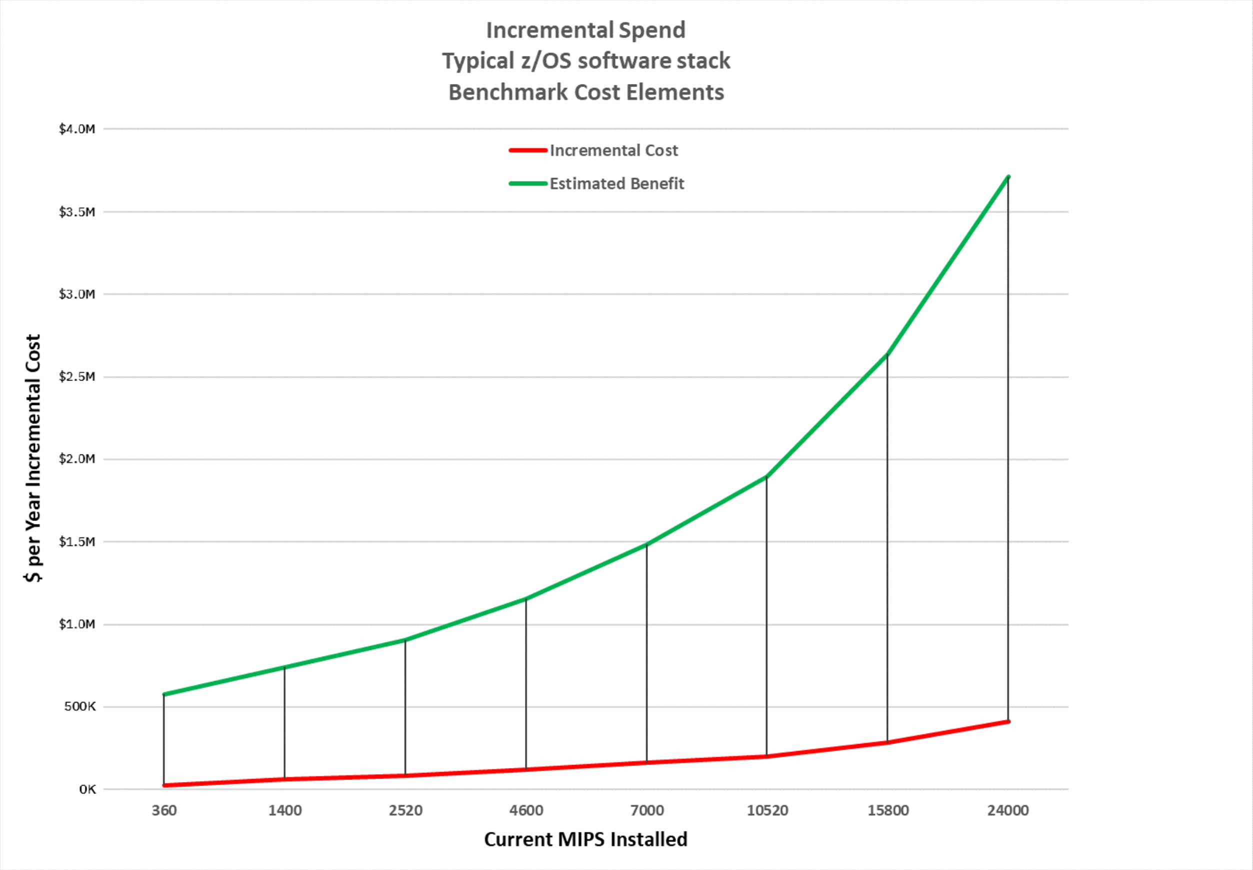


Figure 3: Estimated benefits vs. incremental cost for using pervasive encryption for different sizes of installed MIPS

Designed to protect your data at virtually no cost

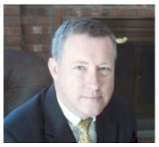
When combined on z15, on-chip compression reduces the volume of data to be encrypted and on-chip encryption reduces the overhead of encrypting what's left, effectively reducing the cost of encrypting your data to practically nothing, while overcoming the barrier of ineffective storage-level compression of already encrypted data. Combine that with the labor savings associated with pervasive encryption, and you really have the best of both worlds.

If your organization is interested in knowing more about the Integrated Accelerator for zEnterprise Data Compression or Pervasive Encryption, contact IT.Economics@us.ibm.com.

About the authors

Ingo Aller is an IBM IT Economics Consultant working with clients mainly in EMEA to identify optimized IT solutions. Ingo has 22 years of IBM experience in the areas of microprocessor development, technical sales, and IT Economics consulting. He is an author or coauthor of numerous technical papers in different technical fields, and holds two patents. As part of his responsibilities he worked for two years in the USA, and for three years in Bangalore, India, where he established a microprocessor design team.

Luc Colleville is an IT Economics practitioner, specialized in examining economic differences between solutions in client environments and focused on identifying areas for efficiencies, cost reductions and increased business value. Prior to this position, Luc has held a number of technical and management positions in presales, marketing and development/test, working mainly on customer cases.



Roger Rogers is an IBM Executive IT Economics Consultant for the IBM IT Economics team and works with clients worldwide to optimize their IT operations. He has more than 35 years of experience in product development, management, and strategy. During his tenure at IBM, Roger has received two IBM Outstanding Technical Achievement awards and has been recognized in IBM's Top 500 IBM Employees list. He is also a frequent speaker at IBM conferences.

Alex Feinberg is an IBM and Open Group Master Certified IT Specialist and the Marketing and Communications Manager for IBM IT Economics Consulting and Research team. With over 30 years of software experience, Alex has led the design and development of many complex applications and can frequently be found presenting at workshops and conferences. His current area of focus is competitive analysis of the IBM Z and LinuxONE platforms, especially in the areas of security and hybrid multi-cloud.

(C) Copyright IBM Corporation 2019
IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
09/19

All statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided “as is” without warranty of any kind, express or implied. In addition, this information is based on IBM’s current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

No other publication, distribution or use is permitted without the prior written consent of IBM. Customers who want a "deep drill down" on CPO Competitive Case Studies should be directed to the IBM Competitive Project Office under NDA. An NDA is required to explain CPO’s methodologies, processes and competitive comparison. You can contact IBM Competitive Project Office by sending an email to IT.Economics@us.ibm.com

References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in these materials may change at any time at IBM’s sole discretion based on market opportunities or other factors and are not intended to be a commitment to future product or feature availability in any way.

31027331-USEN-00