Pervasive Encryption and High Security with Linux on IBM Z

Data protection and compliance are business imperatives

In the era of ever-present attacks and breaches, security and compliance regulations had become very important. Also new and emerging regulations are coming out all the time, the most important the European Union General Data Protection Regulation (GDPR), New York's Cybersecurity Requirements for Financial Services Companies and Australia's Notifiable Data Breach (NDB) scheme, and the Payment Card Industry Data Security Standard (PCI-DSS).

The rationale behind passing these standards is to help organizations better protect customers' privacy and security by design.

“Despite firms’ newfound confidence in defining what data needs to be segmented and isolated to avoid vulnerabilities, they have made no strides in data encryption. Today, 45% of firms encrypt little to no data, which is nearly identical to the 46% of firms which said the same in 2017. This is an alarmingly large number considering that 77% of firms claim to be focused on protecting data above all else.”[1]

Encryption

Extensive use of encryption is an extremely effective way to help reduce the risks and financial losses of a data breach and help meet regulatory requirements and compliance mandates.

However, when it comes to implementing encryption organizations struggle with questions such as:

- What data should be encrypted?
- Where should encryption occur?

Designed for Pervasive Encryption

The IBM® z15™ (z15) and IBM z14® (z14) are designed for pervasive encryption, delivering a consumable approach to enable extensive encryption of data in-flight and at-rest to substantially simplify encryption and reduce costs associated with protecting data and achieving compliance mandates.

Both, z15 and z14, excels with security features that are built into the hardware, firmware, and operating systems. This includes improvements with the on-core hardware accelerated encryption via CPACF[2], Crypto Express features —certified to FIPS 140-2 Level 4, and IBM Hyper Protect Virtual Servers.

IBM Data Privacy Passports

The new IBM Data Privacy Passports offering is the industry’s first commercial data privacy and security enforcement solution with off-platform access revocation. You can choose who accesses data, and when and at what level to revoke their access. Data Privacy Passports is designed to protect your enterprise and your ecosystem’s data, regardless of data source, at-rest and in-flight with no performance tradeoffs or application changes.

Secure Execution for Linux

Secure Execution for Linux is a Trusted Execution Environment (TEE) on IBM Z designed to deliver better security at greater scale than alternative offerings. It enables workloads to run in full isolation with protection from internal and external threats across a hybrid cloud. It is supported for KVM based virtual machines[3]. As well, Secure Execution for

[1] Source: Forrester Consulting on behalf of IBM, Oct 2019
[2] CPACF = Central Processor Assist for Cryptographic Function
[3] IBM is working with its Linux distribution partners to get the functionality included in the Linux distributions for IBM Z

Linux technology is leveraged by IBM Hyper Protect Virtual Servers on IBM Z.

Linux on IBM Z and the world of Comprehensive Encryption

Encryption support is an integral part of the Linux® operating system, and the concept with Linux on IBM Z is providing differentiation without being different. This is accomplished by integrating the exploitation of the IBM Z encryption hardware features into strategic components of the stack, such that applications can transparently benefit.

This enables organizations to exploit the z15 and z14 cryptographic hardware capabilities with their existing Linux cryptographic infrastructure, kernel, and standard libraries encryption, while improving the usability and performance of encrypting/decrypting the data.

‘Protected key’ encryption-which is unique to IBM Z-provides keys that are processed by the on-core cryptographic acceleration, while being protected by keys hidden in the IBM Z firmware, not accessible to any software. Protected keys are volatile in nature and are derived from secure keys that are encrypted using a master key that is protected by a tamper-responding HSM[4] in the Crypto Express features.

All Linux workloads can benefit from the fast encryption in z15 and z14, since the encryption functions in the Linux kernel, and the libraries, openSSL, openCryptoki, GSKIT and Java™ 8/JCE, are transparently delivering the performance to the applications.

Java applications can benefit from hardware support to accelerate the GCM[5] cryptographic mode for block ciphering, and the on-core true random number generator allows to generate irreproducible unique data, which is the basis to generate high quality keys.

Linux on IBM Z is well equipped for encrypting all data in-flight using protocols like TLS, SSH, or IPSec. Exploiting the outstanding cryptographic performance of the z15 and z14, Linux users can afford to encrypt their network traffic in a transparent manner using OpenSSL, OpenSSH, and IPSec.

The CPACF capabilities are extended with z15, and performance improvements will be available with CPACF and the new Crypto Express7S adapter.

IBM z/VM® 7.2, z/VM 7.1 and z/VM 6.4, and KVM provide support to enable the crypto hardware exploitation by Linux guests in support of encryption of data in-flight and data at-rest. As well, the z/VM versions support encrypted paging—using protected keys, ciphering occurs as data moves between active memory and a paging volume—protecting guest paging data from users and administrators.

Specific IBM Z hardware security

The IBM Z logical partitioning (LPAR) technology is the only commercial platform with an EAL5+ hardware security certification. This certification level means that workloads are isolated when running in separated LPARs.

The IBM Hyper Protect Virtual Servers allows for deploying software appliances into LPARs that can’t be inspected by system administrators.

Summary

Data protection and compliance are no longer a matter of if, and with Linux on IBM Z you can provide comprehensive data protection that your organization and customers demand, and that can slash the associated.

References in this publication to IBM products and services do not imply that IBM intends to make them available in all countries in which IBM operates.

This information is provided “as is” without warranty of any kind, express or implied, and 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 document. Nothing contained in this document 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.

[4] HSM = Hardware Security Module

[5] GCM = Galois Counter Mode