End-to-End Encryption and High Security with Linux on IBM z14

Data protection and compliance are business imperatives

There is no doubt in the market, security and compliance to the industry and government regulations had become very important. On the other hand, new and emerging regulations are coming out all the time, such as the European Union General Data Protection Regulation (GDPR) and the Payment Card Industry Data Security Standard (PCI-DSS).

"*It's no longer a matter of if, …*". That's a conclusion when looking at data breach statistics. "*Breaches are no longer a binary proposition where an organization either has or hasn't been breached. Instead they are wildly variable — having varying degrees of fallout — from breaches compromising entire global networks of highly sensitive data to others having little to no impact whatsoever.*"[1]

These are the two main drivers, why data protection and compliance are business imperatives today.

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?
- Who is responsible for encryption?

IBM z14 – Designed for Pervasive Encryption

All workloads have one aspect in common: the need for a platform with deeply integrated security. All IBM® z14™ (z14) models are designed for pervasive encryption, delivering a transparent and consumable approach that enables extensive encryption of data in-flight and data at-rest, to substantially simplify and reduce the costs associated with protecting data and achieving compliance mandates.

The z14 excels with security features that are built into the hardware, firmware, and operat-ing systems. This includes cryptographic performance improvements with the on-core hardware accelerated encryption with every core via CPACF[2], the Crypto Express6S feature—certified to FIPS 140-2 Level 4, and the IBM Secure Service Container.

Linux enters the world of Comprehensive Encryption

z14 provides the enabling technologies for comprehensive data encryption with Linux.

The concept with Linux on IBM Z® is providing differentiation without being different. This is accomplished by integrating exploitation of the Z encryption hardware into strategic compo-nents of the stack, such that applications can transparently benefit.

Encryption support is an integral part of the Linux operating system. The encryption with Linux on Z enables organizations to exploit the z14 cryptographic hardware in their existing Linux crypto infrastructure, kernel, and standard libraries helping to improve the usability and performance of encrypting / decrypting data in-flight and at-rest.

Important for the comprehensive encryption with z14 was the integration of 'protected keys' into the Linux kernel and infrastructure.

[1] Source: Breach Level Index, http://breachlevelindex.com

[2] CPACF = Central Processor Assist for Cryptographic Function

The ‘protected key’ capability is unique to IBM Z. It provides keys that allow for the on-core cryptographic acceleration, while being protected by keys hidden in the Z firmware that is 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[3] in the Crypto Express6S feature. The master key is never exposed to hypervisors, operating systems and applications, and if the key would get exposed to a hacker, it’s worthless, because it can’t be used to decrypt the data.

All Linux workloads can benefit from the faster encryption in z14, since the encryption func-tions 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 Galois Counter Mode (GCM) cryptographic mode for block ciphering.

The recent Linux kernels support end-to-end encryption of block devices, such as disk partitions and logical volumes, by leveraging the CPACF protected key technology.

Network encryption through TLS and IPsec use CPACF & SIMD[4] to leverage the IBM Z encryption hardware performance.

Organizations can protect their data during the complete journey from Linux on IBM Z through the cryptographic hardware, the SAN infra-structure into the storage server cache, and finally on the storage devices.

Organizations don’t have to change their encryption approach, they simply can get consumable data protection for their data.

In addition, IBM Z servers can qualitatively improve the way data is protected. The new on-core true random number generator allows to generate irreproducible unique data, which is the basis to generate high quality keys.

z/VM® V7.1 and V6.4 provide the support to enable the z14 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 with access to volumes and administrators.

More IBM Z hardware security

The IBM Z logical partitioning (LPAR) techno-logy 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 Secure Service Container allows for deploying software appliances into LPARs which cannot be inspected by system admin, and with IBM Secure Service Container for IBM Cloud Private, encryption and data protection capabilities are provided for hybrid and private cloud containerized workloads on IBM Z.

Summary

Data protection and compliance are no longer a matter of if, and with Linux on z14 you are able to provide comprehensive data protection that your organization and customers demand, and that can slash the associated.

By placing the security controls on the data itself, the solution creates an envelope of protection around the data on z14.

ZSF03206-USEN-05

[3] HSM = Hardware Security Module

[4] SIMD = Single Instruction Multiple Data provides for vector processing