IBM Z and LinuxONE
Introduction
May 2020

IBM Secure Execution for Linux

Frequently Asked Questions

Worldwide

12031512-USEN-01

IBM Secure Execution for Linux

What is Secure Execution?

Secure Execution is an IBM LinuxONE and Linux® on Z exclusive Trusted Execution Environment (TEE) technology that helps protect data in use.

It is a hardware-based security technology that is built into the IBM z15 and LinuxONE III generation systems. It is designed to protect workloads from insider threats and external attacks to help prevent security breaches.

Use Secure Execution to provide scalable isolation for individual workloads to help protect from not only external attacks, but also insider threats. IBM Secure Execution can help protect and isolate workloads on-premises, or IBM LinuxONE and IBM Z® hybrid cloud environments.

What is a Trusted Execution Environment (TEE)?

TEEs enable sensitive workloads to be able to run securely on untrusted or compromised infrastructure.

TEEs protect data in use by enabling hosted workloads to process unencrypted memory securely without exposing it to the host or any other workloads in the same environment. They provide secure computation capability through special-purpose hardware in modern processors. In general, the special-purpose hardware provides a mechanism by which a process can run without its memory or execution state being visible to any other process on the processor, even the operating system or other privileged code. In other words, it creates an “environment for executing code, in which those executing the code can have high levels of trust in that surrounding environment, because it can ignore threats from the rest of the device” (Trustonic 2019).

Computation in a TEE is not performed on data while it remains encrypted. Instead, the execution environment is made secure by the special hardware provided. TEEs provide a higher level of trust in the validity, isolation, and access control over sensitive workloads compared to general purpose software environments.

What is a Zero Trust?

“Zero Trust is the security concept centered on the belief that organizations should not automatically trust anything inside or outside its perimeters and instead must verify anything and everything trying to connect to its systems before granting access” (CSO 2018).

Zero Trust security enables the right user to have the right access to the right data under the right conditions. Hardware enabled protections such as Secure Execution can move clients closer to realizing a Zero Trust ecosystem through workload isolation and hardened access restrictions over their data assets.

Why should we protect data in use?

Protect data in use to help eliminate the window of vulnerability that is inherent to current approaches in protecting data. Current security architectures for protecting data address data in rest and data in transit, few secure data in use. Secure Execution will protect data in use.

Data in use is the more volatile form of data because, typically, to be able to modify data, the data would need to be decrypted. Anytime you have decrypted data out in the open during transit, it is vulnerable. This creates the window of vulnerability that malicious entities can exploit and gain access to sensitive workloads. Confidential computing is meant to ensure that data is protected even when it is being processed. “The basic premise of confidential computing lies within the mechanism of a TEE” (SCmagazine 2020).

The Confidential Computing Consortium was established in 2019 and its participants include many of the top players in the technology industry. The consortium seeks to use technology to address data in use and accelerate the adoption of confidential computing. Secure Execution furthers the confidential computing agenda through the implementation of a hardware-based TEE on the IBM Z and LinuxONE platforms.

Does Secure Execution encrypt data in use?

Secure Execution does not encrypt data in use, but rather protects it.

Computation in a TEE is not performed on data while it is encrypted. Instead, Secure Execution provides a hardware-based technology (TEE) that enables hosted workloads to process unencrypted memory securely without exposing it to the host or any other workloads in the same environment.

Do I have to change my VM or container images?

The applications and the workload code do not require any changes. Steps are necessary to encrypt images in a specific way so that they are capable of running in a Secure Execution environment.

For more information, please read Chapter 5 of the Overview on Knowledge Center.

Does Secure Execution work with containers?

Secure Execution currently works with KVM, but the future intent is to be able to run through container-based environments like Kubernetes.

Does Secure Execution work with OpenShift?

Not currently. OpenShift will be available on the z15 T02 and LinuxONE III models but does not currently support Secure Execution technology.

What are the system requirements?

Hardware Requirements:

- IBM z15™, IBM z15 T02, IBM LinuxONE III or IBM LinuxONE III LT2

IBM Secure Execution for Linux requires support in the KVM host and the KVM guest. The following Linux distributions are currently supported:

Guest:

- RHEL 7.8, RHEL 8.1, Ubuntu 19.10, Ubuntu 20.04, SLES 12 SP5
- IBM is working with its Linux distribution partners to provide support in future distribution releases

Host:

- Ubuntu 20.04
- IBM is working with its Linux distribution partners to provide support in future distribution releases

Why does Secure Execution require Host and Guest support?

Secure Execution requires both guest and host support from a Linux distribution provider for full functionality. This is due to requirements for both the host (hypervisor) and guest (VM workload) to be supported in order for the full solution to be functional. IBM is with working with its Linux distribution partners to ensure support for both host and guest in upcoming distribution releases.

Is Secure Execution for Linux the same as SELinux? (Security Enhanced Linux)

No. SELinux is a set of security functions embedded in the Linux kernel. SELinux implements an access control on the operating system/process level whereas Secure Execution is a hardware based trusted security isolation between Host and Guest and access control.

Can customers run Secure Execution in the cloud?

Yes, utilize Secure Execution to help ensure the confidentiality and integrity of each application and its data when running sensitive workloads on cloud vendor environments.

What are the pricing options?

This feature is a no cost offering. It is included in the hardware of LinuxONE III and z15 system offerings and enabled by ordering the feature code 115.

How do customers order this?

Contact your IBM sales representative for additional information on IBM Secure Execution for Linux.

Where can I find more information?

Evaluate the full IBM security portfolio to create a layered security defense by visiting these websites:

- IBM Z: ibm.com/it-infrastructure/z
- IBM Z Enterprise Security: ibm.com/it-infrastructure/z/capabilities/enterprise-security
- IBM LinuxONE: ibm.com/it-infrastructure/linuxone
- IBM Security Solutions: ibm.com/security/solutions

Sources

https://www.trustonic.com/news/technology/what-is-a-trusted-execution-environment-tee/
https://www.csoonline.com/article/3247848/what-is-zero-trust-a-model-for-more-effective-security.html
https://www.scmagazine.com/home/opinion/executive-insight/confidential-computing-the-confidentiality-of-data-in-business-is-at-peak-recognition/

(C)Copyright IBM Corporation 2020
IBM Corporation
New Orchard Road
Armonk, NY 10504
U.S.A.
05/20

IBM, ibm.com, IBM logo, IBM Z and z15 are trademarks or registered trademarks of the International Business Machines Corporation.

A current list of IBM trademarks is available on the Web at https://www.ibm.com/legal/us/en/copytrade.shtml, and select third party trademarks that might be referenced in this document is available at https://www.ibm.com/legal/us/en/copytrade.shtml#section_4.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

InfiniBand and InfiniBand Trade Association are registered trademarks of the InfiniBand Trade Association.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

OpenStack is a trademark of OpenStack LLC. The OpenStack trademark policy is available on the OpenStack website.

Red Hat®, JBoss®, OpenShift®, Fedora®, Hibernate®, Ansible®, CloudForms®, RHCA®, RHCE®, RHCSA®, Ceph®, and Gluster® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

RStudio®, the RStudio logo and Shiny® are registered trademarks of RStudio, Inc.

TEALEAF is a registered trademark of Tealeaf, an IBM Company.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Worklight is a trademark or registered trademark of Worklight, an IBM Company.

Zowe™, the Zowe™ logo and the Open Mainframe Project™ are trademarks of The Linux Foundation.

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.

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.

12031512-USEN-03