IBM Secure Execution for Linux

Designed to isolate workloads at granularity and scale and help protect them from internal and external threats

Highlights

- Create a Trusted Execution Environment that helps to protect data in use
- Help fortify and protect workloads designed for enterprise scale
- Restrict access to hosted data without impeding admin job functions
- Provide scalable isolation between individual workloads
- Allow proof of integrity through remote attestation

Cyber-attacks on enterprises are increasing and data regulators are imposing major fines on enterprises that don't properly secure customer data. Data breaches are a serious threat and keeping confidential information secure is a fundamental priority for leading enterprises around the world.

The exploitation of sensitive data by internal and external threats can result in large financial penalties, regulatory scrutiny, and company discharges. An approach with hardware-based access controls and workload isolation can help give enterprises confidence that their data will be less vulnerable to exploitation by insider threats or external parties than with traditional software-based approaches.

IBM Secure Execution for Linux® is a hardware-based security technology that is built into the IBM z16™ and IBM LinuxONE Emperor 4™ generation systems. It is designed to provide scalable isolation for individual workloads to help protect them from not only external attacks, but also insider threats. Secure Execution can help protect and isolate workloads on-premises, or on IBM Z® and IBM LinuxONE™ hybrid cloud environments.[1]

Current approaches to security address data at ‘rest’ and data in ‘transit’. When data is in ‘use’, a window of vulnerability exists that insiders or criminals can exploit.

Confidential computing is the industry movement around using technology to address this vulnerability. Secure Execution is designed to further this agenda by protecting data in use through the implementation of a hardware-based Trusted Execution Environment (TEE). Hardware enabled protections, providing workload isolation and hardened access restrictions over their data, can move clients closer to realizing a Zero Trust environment.

Help support data confidentiality and integrity

As more companies move their on-premises workloads to public cloud, the need for a secure hosting solution becomes necessary to help support the confidentiality and integrity of each application and its data. Secure Execution gives you the ability to leverage hardware-based security 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. Enterprises can now protect data and code in use in their hosted workloads by exploiting protection mechanisms offered by Secure Execution.

Secure Execution is designed to eliminate the window of opportunity for hosts and guests infected with malicious code to exploit security lapses and gain full privileges to your hosted core business systems. Workload owners can use Secure Execution to help protect sensitive data from corruption and help support data confidentiality and integrity.

Designed for enterprise scale

Commit up to 16 TB of memory for hosting protected applications on an IBM z16 or IBM LinuxONE Emperor 4 system. With Secure Execution, you can deploy secured and isolated services within a single IBM Z or IBM LinuxONE server without needing to run on physically separated logical partitions (LPAR) [1]. Secure Execution can help protect enterprise ready multi-tenant workloads on-premises, or in cloud and hybrid environments.

Limits access for host administrators

In traditional x86 ring architectures, the host can access the memory and data of guest applications freely, leading to the potential for malicious software to be proliferated throughout the entire system. Isolation between host and guest environments is necessary to help prevent system compromise. Another pain point is that today's software access controls are policy-based which can be exploited by anyone with administrator credentials.

Secure Execution provides isolation between a KVM hypervisor host and guests in virtual environments to provide protections and safeguards against insider threats such as malicious or negligent administrators.[1] This level of vertical isolation is designed to remove the ability for these administrators to have total visibility into the sensitive workloads being hosted on VMs and individual containers. Secure Execution provides hardened access restrictions to protect intellectual property and proprietary secrets while allowing administrators to manage and deploy workloads as black boxes and continue normal job functions.

Enhance security by isolating your workloads

Secure Execution also helps enterprises provide isolation between individual multi-tenant workloads running on a shared LPAR. Protecting highly sensitive data from other hosted workloads can help provide enterprises confidence that their assets will not be exposed to other malicious applications that gain access to the same virtual environment. Secure Execution is designed to help enterprises who want to be able to support confidentiality and data integrity for selected workloads and simplify efforts to meet regulatory challenges.

Provide proof of integrity with remote attestation[2]

With IBM z16 and IBM LinuxONE Emperor 4 it is possible for a user of a workload running in a secure execution guest to verify the integrity of a running image with the help of firmware-based attestation. This new capability allows for improved auditing and facilitates the integration of IBM Secure Execution enclaves into modern confidential computing frameworks.

Root of trust protected by IBM and owned by owner of the server

Even though IBM manufactures IBM z16 and IBM LinuxONE Emperor 4 systems, once an IBM system with secure execution support is sold and installed, not even IBM can access the secrets on which the security of secure execution is based.

Hardware Requirements

- IBM z16, or IBM LinuxONE Emperor 4
- IBM z15™ T01, IBM z15 T02, IBM LinuxONE III LT1, or IBM LinuxONE III LT2

Linux Distribution Requirements

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

Guest:

- Red Hat® Enterprise Linux (RHEL) 9.0 with service, RHEL 8.4 with service, RHEL 7.9 with service
- SUSE Linux Enterprise Server (SLES) 15 SP3 with service, SLES 12 SP5 with service
- Ubuntu Server 22.04 LTS with service, Ubuntu Server 20.04 LTS with service

Host:

- RHEL 9.0 with service, RHEL 8.4 with service
- SLES 15 SP3 with service
- Canonical Ubuntu 22.04 LTS with service, Ubuntu Server 20.04 LTS with service

IBM is working with its Linux distribution partners to provide support in future distribution releases.

Why IBM Secure Execution for Linux?

Created to help maintain the confidentiality and integrity of hosted client data. Secure Execution is designed to deliver:

- Scalable isolation for multi-tenant hosting

  Achieve scalable isolation for multi-tenant hosting on a single system with protection from third parties and isolation between workloads. Protect against administrative access to your hosted workloads, as well.

- Support for enterprise DevSecOps solutions

  Achieve best practices in secure engineering and development. Secure execution is designed to protect the pipeline of code development from start to finish.

  Protect intellectual property and proprietary secrets by protecting active memory and securing application images for distribution and deployment.

- Simplified approach to industry and regulatory challenges

  Designed to simplify efforts to meet regulatory challenges by verifying secure build for hosted workloads. Empower personnel responsible for security configuration with a more straightforward knowledge of security parameters.

- Enterprise ready

  Scale up to 1500 KVM guests running a web page serving workload on an IBM z16 and IBM LinuxONE Emperor 4 using IBM Secure Execution.

Why IBM?

The IBM z16 and IBM LinuxONE Emperor 4 platforms offer an industry-leading level of data privacy, security and resiliency across on premises, public and hybrid cloud environments.

Leveraged by business of all sizes, from large enterprises to next-gen startups, IBM Z and IBM LinuxONE represent a sound investment for your security solutions.

For more information

Contact your IBM sales representative for additional information on IBM Secure Execution for Linux or call us, email us, or book a consultation by clicking “Let’s talk” on the IBM Z website.

Learn more about Secure Execution:

- Documentation: ibm.com/docs/en/linux-on-systems?topic=virtualization-introducing-secure-execution-linux

Evaluate the full IBM security portfolio to create a layered security defense:

- 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

[1] Disclaimer for all—Workload isolation uses enhanced hardware and firmware protection provided by the IBM Z and LinuxONE platforms.
[2] Requires Linux Support in the Guest