IBM Secure Execution for Linux

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

What is IBM Secure Execution for Linux?

Insider threats are incredibly difficult to detect. They are individuals with legitimate access to the company's network who use their access, whether maliciously or unintentionally, in a way that causes harm to the organization. It's important to look at insider threats in addition to external threats, since many organizations focus on securing the perimeter but are often blind to the threats that walk through their front door every day.

IBM Secure Execution for Linux® is a hardware-based security technology that is built into the IBM z15™ and LinuxONE III generation systems. It is designed to give enterprises confidence that their data will be less vulnerable to exploitation by insider threats or external parties than with traditional software-based approaches.

The evolution of confidential computing

Current approaches to security address data at rest and data in transit. Few secure data when it is in use, creating a window of vulnerability 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 Trusted Execution Environment (TEE).

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. Enable sensitive workloads to run securely on untrusted or malicious infrastructure and move closer to realizing a Zero Trust environment.

Access restrictions for administrators

Today's software access controls are policy-based which can be exploited by anyone with administrator credentials. Secure Execution provides hardware-based access restrictions between a KVM hypervisor host and guests in virtual environments to provide protections and safeguards against insider threats such as malicious administrators.[1]

Enhance security by isolating workloads

Secure Execution helps provide isolation between individual multi-tenant workloads running on a shared LPAR. Protecting highly sensitive data from other hosted workloads can help give enterprises confidence that their assets will not be exposed to other malicious applications that gain access to the same virtual environment.

Designed for enterprise scale

Commit up to 16TB of memory on a single LPAR for hosting protected applications. Deploy within a single IBM Z® or LinuxONE server without needing to run on physically separated LPARs.[1] IBM Secure Execution can help protect and isolate workloads running on-premises, or on IBM LinuxONE and IBM Z hybrid cloud environments.[1]

System & Linux distribution requirements

Hardware: IBM z15, IBM z15 T02,
IBM LinuxONE III or IBM LinuxONE III LT2

Host: Ubuntu 20.04

Guest: RHEL 7.8 & 8.1, Ubuntu 19.10 & 20.04 and SLES 12 SP5

[1] Disclaimer for all—Workload isolation uses enhanced hardware and firmware protection provided by the IBM z15 and LinuxONE III model family.