IBM Hyper Protect Virtual Servers v2.1

Protect your Linux workloads processing sensitive data with confidential computing throughout their lifecycle - build, deployment, and management - to fulfill compliance and regulation requirements

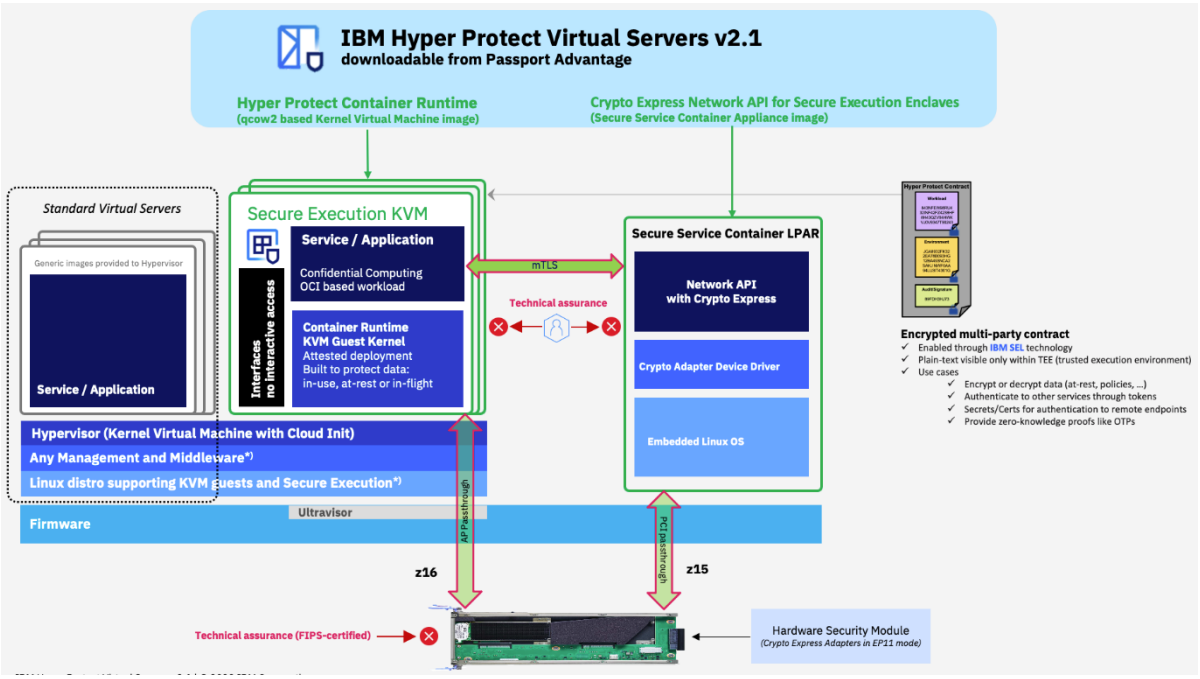
As clients continue their application modernization journey, the trend to run containerized applications in production has significantly increased. However, it is imperative that clients take the appropriate action to safeguard the data inside those containers. The need to protect this sensitive business data and intellectual property continues to grow and does not affect only large or regulated organizations. Protecting against internal and external threats is essential as the cost of resolution and number of data or security-related breaches continues to rise...

IBM Hyper Protect Virtual Servers has addressed the need for data and privacy protection during deployment and production since its first release. The protection against internal and external threats begins during development and continues in production environments. Hyper Protect Virtual Servers continues to evolve and leverage the latest technologies. Key Hyper Protect Virtual Servers concepts include the data-in-use protection and simplified management of deployment while assuring data confidentiality, integrity, and no interactive access to a deployed instance.

Hyper Protect Virtual Servers 2.1 leverages the next generation of workload isolation technology provided by IBM Z® and IBM® LinuxONE through IBM Secure Execution for Linux (SEL), a hardware- based security technology that is designed to provide scalable isolation for individual Linux® workloads on-premises. This further extends the existing Confidential Computing portfolio of IBM as the companion solution to the already available IBM Cloud Hyper Protect Virtual Servers for VPC in the IBM Cloud®, and in combination, enables hybrid cloud environments designed for Zero Trust and total data privacy protection.

Highlights

- Deploy your containerized workload in a Trusted Execution Environment that protects data in use and encrypts data at rest
- Leverage Linux virtualization designed for enterprise scale and common infrastructure for logging and (container) management
- Restrict and separate access through an encrypted multi-party contract architected for different personas and entities
- Provide workload as Open Container Initiative image which leverages additional data and privacy protection without code changes
- Allow proof of deployment through attestation



* Customer provided and Third-Party charges may apply. Support restrictions by 3rd party and Linux distribution provider may apply
** IBM Secure Execution for Linux (SEL) support for Crypto Express adapters available only for IBM z16® and IBM® LinuxONE 4 or above

Hyper Protect Virtual Servers 2.1 provides clients the following benefits:

Flexible deployments in Linux Hypervisor

IBM Secure Execution for Linux (SEL) enables deployment of isolated workloads protected by Confidential Computing at scale and enables client-defined middleware and hypervisor. With this, Hyper Protect Virtual Servers can be integrated into a virtualized Linux environment and is no longer an isolated logical partition (LPAR) on the system. The protection boundary moves from the LPAR level, which includes the operating system and application, to complete isolation of the application from the operating system in a trusted execution environment (TEE). Client code and data are exclusively controlled by their administrators, no exceptions.

Hyper Protect Virtual Servers 2.1 can be deployed on any Linux distribution with a KVM compliant hypervisor. Commit up to 16 TB of memory for hosting protected applications on an IBM z16® or IBM® LinuxONE Emperor 4 system and beyond. 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) as required by the previous version of IBM Hyper Protect Virtual Servers.

Container runtime based and strengthened malware protection

Any Open Container Initiative (OCI) image gains the benefit of a Confidential Computing solution with an additional level of protection. Hyper Protect Virtual Servers 2.1 will only deploy container versions, which are validated at deployment through explicit digest or are signed.

To achieve this, IBM Hyper Protect Virtual Servers 2.1 provides the Hyper Protect Container Runtime (HPCR) image to be deployed as a Kernel Virtual Machine (KVM) guest on a provided and managed Linux LPAR. It contains a hardened and extended bootloader to start the embedded guest operating system with an integrated Container Runtime to simplify workload deployment and abstraction.

Leverage common infrastructure for Container registry, Logging and Management

The reuse of existing and common infrastructure components reduces the complexity and costs associated with a given solution. IBM Hyper Protect Virtual Servers 2.1 supports customer provided container registry in addition to any public registries like IBM Container Registry, DockerHub or Base Container registry maintained by Linux distributors. There is support for using internally hosted private container registries by leveraging existing PKI infrastructure as root of trust.

To integrate the IBM Hyper Protect Virtual Servers solution into existing logging and auditing environments and enable simplified compliance, it is now possible to provide a remote LogDNA or syslog compliant instance during deployment. This endpoint can differ per-deployment and collects workload-specific logging information reported with encrypted data-in-flight for failure analysis or compliance and audit reasons.

Multiparty contract and attestation of deployment

To apply Zero Trust principles from workload development through deployment, it is essential to separate duty and access as multiple personas, and legal entities collaborate. Hyper Protect Virtual Servers 2.1 is based on a newly introduced encrypted contract concept, which enables each persona to provide its contribution, while ensuring through encryption that none of the other personas can access this data or intellectual property. The deployment can be validated by an auditor persona through an attestation record which is signed and encrypted to ensure only the auditor has this level of insight.

Integrated data-at-rest protection

IBM Hyper Protect Virtual Servers 2.1 offers integrated data- at-rest protection with Linux Unified Key Setup (LUKS) encryption passphrases only present within the Trusted Execution Environment. It is based on a key derivation calculated in the bootloader during deployment of the IBM SEL Kernel Virtual Machine. The key is based on independent seeds provided by the workload and environment persona or legal entities. As a result, neither persona or entities can access the data without cooperation of the other persona or entity.

In combination with the multi-party contract, these seeds are protected. Dependent of the need, these seeds may be either randomized for any build or deployment or protected by a Hardware Security Module.

Access a Crypto Express adapter in Enterprise PKCS#11 (EP11) mode

The usage of a Hardware Security Module (HSM) to protect keys is common for many use cases. As a Crypto Express adapter is accessed from within the isolated workload, protected by Confidential Computing provided through the IBM SEL technology, it enables end-to-end asset protection or regulatory compliance regarding data privacy with a FIPS 140-2 Level 4 certified HSM. To enable such solutions, directly attach a Crypto Express adapter to a dedicated Secure Service Container LPAR and deploy the Crypto Express Network API for Secure Execution Enclaves provided as a component of Hyper Protect Virtual Servers within the LPAR. As the GREP11 server is also deployed in the Hyper Protect Container runtime (HPCR), EP11 operations are now performed in the HSM which secures communication through an mTLS-protected network channel from the Trusted Execution Environment.

However, with IBM z16 or IBM® LinuxONE 4 servers and beyond, Hyper Protect Virtual Servers can directly invoke crypto operations on Crypto Express 8S adapters configured in EP11 mode, including NIST approved quantum safe algorithms. The provided GREP11 server, deployed in a KVM guest running HPCR, can be leveraged by application workloads to directly invoke EP11 crypto operations. This does not require the provided Crypto Express Network API for Secure Execution Enclaves component to be deployed.

Hardware Requirements

- IBM z16, IBM® LinuxONE Emperor 4, IBM z15®, IBM® LinuxONE III LT1, or IBM® LinuxONE III LT2
- Feature Code 0115 for IBM Secure Execution for Linux (SEL)
- Crypto Express 8S adapter must be configured in EP11 mode for Secure Execution guests to directly invoke EP11 operations: -
  - EP11 firmware 5.8.30 or higher
  - IBM z16 / IBM® LinuxONE firmware bundles S30 and S31b

Linux Distribution Requirements

IBM Hyper Protect Virtual Servers requires IBM SEL in the KVM host*. Following Linux distributions support IBM SEL:
– RHEL 9.0 with service, RHEL 8.4 with service
– SLES 15 SP3 with service
– Canonical Ubuntu 24.04, 22.04, 20.04 LTS with service

Crypto Express 8S adapters for guests running in secure-execution mode are supported by distributions*:
– Canonical Ubuntu 24.04 LTS with service
– RHEL 9.4 with service and RHEL 8.10 with service
– SLES 15 SP6 with service

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

*Support for the containerized workloads within the Hyper Protect Container Runtime is not provided through IBM and needs to be obtained prior to deployment and/or production usage. Appropriate subscription to Linux distribution must be obtained from respective Linux distribution vendor for availing support.

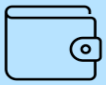
Why IBM Hyper Protect Virtual Server v2.1?

Created to leverage Privacy-enhancing technology and data protection in development and production environments which are built upon Zero-Trust. Hyper Protect Virtual Servers is designed to maintain the confidentiality and integrity of hosted client data, digital assets or intellectual property

Secure Containerized Workloads

Whether you are building a cloud native application, or on an application modernization journey, you can now do both with peace of mind by leveraging IBM's Secure Execution technology.

Containerizing applications within a Confidential Computing environment ensures that your applications are protected, even the IBM admin doesn't have access, and workloads are isolated by a secure boundary to prevent privilege user escalation.



Digital Assets

IBM Digital Asset Infrastructure provides the building blocks to create end-to-end solutions for storing and transferring large quantities of digital assets in highly secure wallets.

Customers can utilize Secure Build to further enhance their security posture. This technology validates code before it is deployed to a container, ensuring that only verified code is allowed to run, ultimately reducing malware threats, and misconfigurations

Secure AI and Multi Party Collaboration (MPC)

As various entities collaborate towards a common goal the need for the individual data privacy as well as intellectual property protection remains. While MPC leverages cryptography, a key aspect of this model is the protection from each other.

With Confidential Computing it is possible to enable distributed MPC, where participants are ensured their data, AI models or insights are protected even when being processed outside their direct control

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 Hyper Protect Virtual Servers:

Documentation:
https://www.ibm.com/docs/en/hpvs/2.1.x

Companion solution offered in IBM Cloud VPC:
https://cloud.ibm.com/docs/vpc?topic=vpc-about-se

IBM Hyper Protect Services
https://www.ibm.com/products/hyper-protect

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

Confidential computing with IBM
ibm.com/confidential-computing

Learn more:
https://www.ibm.com/products/hyper-protect-virtual-servers

IBM Corporation
New Orchard Road
Armonk, NY 10504

1 Disclaimer for all—Workload isolation uses enhanced hardware and firmware protection provided by the IBM Z and IBM® LinuxONE platforms.