



# 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 fulfil compliance and regulation requirements



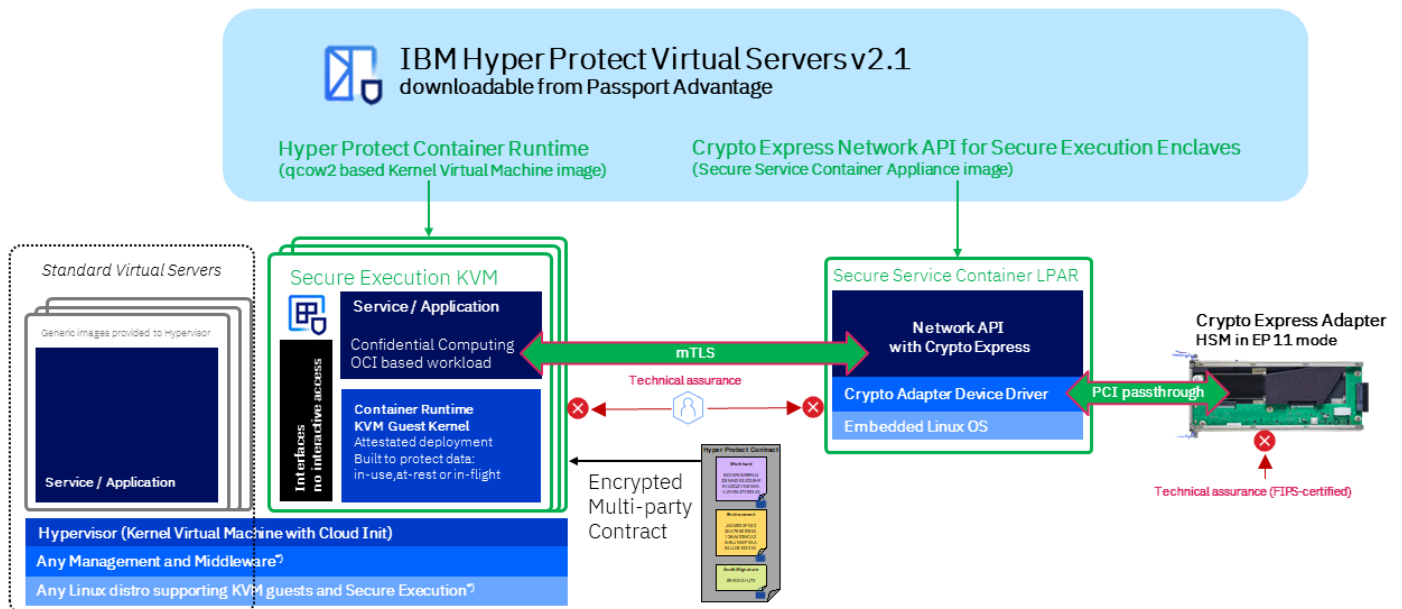
The need to protect sensitive business data and intellectual property is continuing to grow and does not affect only large or regulated organizations. The need for protection against internal and external threats is always present, while the cost of resolution and the number of data or security-related breaches is growing. The trend to run containerized applications in production has significantly increased in past years and is continuing to grow.

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 are 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 zSystems and IBM LinuxONE™ through IBM Secure Execution for Linux, 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 persona 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

Hyper Protect Virtual Servers 2.1 provides clients the following benefits:

### **Flexible deployments in Linux Hypervisor**

Secure Execution for Linux 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. 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. With Secure Execution, you can deploy secured and isolated services within a single IBM Z® or LinuxONE server without needing to run on physically separated logical partitions (LPAR)1 as required by the previous version of IBM Hyper Protect Virtual Servers.

### **Container runtime based and strengthen 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 v2.1 provides the Hyper Protect Container Runtime image to be deployed as a Kernel Virtual Machine (KVM) guest on a given 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 component reduces the complexity and costs associated with a given solution. IBM Hyper Protect Virtual Servers supports in this version customer provided container registry in addition to any public registries like IBM Container Registry, DockerHub or Base Container registry maintained by Linux distributors.

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. As multiple personas and legal entities collaborate, it is essential to separate duty and access. Hyper Protect Virtual Servers is based on a newly introduced encrypted contract concept, which enables each persona to provide its contribution, while being ensured 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 Version2 offers integrated data-at-rest protection with Linux Unified Key Setup (LUKS) encryption passphrase only present within the Trusted Execution Environment and based on a key derivation during deployment, based on seeds provided by the workload and environment persona. It is based on a key derivation calculated in the bootloader during deployment of the IBM Secure Execution for Linux 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 already mentioned multi-party contract these seeds are protected. Dependent of the needs 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 Secure Execution for Linux technology, enables end-to-end asset protection or regulatory compliance regarding data privacy with a FIPS certified HSM2). 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 component of Hyper Protect Virtual Servers within. As the also provided Grep11 server is deployed in the Hyper Protect Container runtime EP11 operations are now performed in the HSM which communication is secured through an mTLS-protected network channel from the Trusted Execution Environment.

## Hardware Requirements

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

## Linux Distribution Requirements

IBM Hyper Protect Virtual Servers requires IBM Secure Execution for Linux in the KVM host. The following Linux distributions support IBM Secure Execution for Linux:

- 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.

Support for the containerized workloads within the Hyper Protect Container Runtime is not provided through IBM and needs to be obtained prior deployment and/or production usage.

## Why IBM Hyper Protect Virtual Server v2.1?

Created to leverage Privacy-enhancing technology and data protection in development and production environments which are build 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 Multi Party Computation (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 or insights are protect even when being calculated 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>

Learn more about Secure Execution:

- Documentation:  
[ibm.com/docs/en/linux-on-systems?topic=virtualization-introducing-secure-execution-linux](https://www.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](https://www.ibm.com/it-infrastructure/z)
- IBM Z Enterprise Security:  
[ibm.com/it-infrastructure/z/capabilities/enterprise-security](https://www.ibm.com/it-infrastructure/z/capabilities/enterprise-security)
- IBM LinuxONE:  
[ibm.com/it-infrastructure/linuxone](https://www.ibm.com/it-infrastructure/linuxone)
- IBM Security Solutions:  
[ibm.com/security/solutions](https://www.ibm.com/security/solutions)

Learn more:

<https://www.ibm.com/products/hyper-protect-virtual-servers>

© Copyright IBM Corporation 2022  
IBM Corporation  
New Orchard Road  
Armonk, NY 10504

IBM, the IBM logo, ibm.com, IBM Cloud, IBM Z, IBM z16, LinuxONE and z15 are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at [www.ibm.com/legal/copytrade.shtml](https://www.ibm.com/legal/copytrade.shtml).

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 world-wide basis.

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.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates. The client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions. THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation.

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