Solution Brief

Cross Industry

IBM **LinuxONE**

IBM Hyper Protect Virtual Servers

Protect critical Linux workloads during build, deployment, and management on-premise

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

For cloud-enabled workloads, both on and off premise, security is a top priority. Large-data breaches resulting in costly fines, devaluation of brand reputation, and huge revenue loss are serious concerns.

With so many potential threat vectors to combat, organizations are asking themselves critical security questions:

How can we ensure cloud ready workloads are fully protected throughout the entire lifecycle?

How can we prevent external or internal threats from compromising our sensitive data?

The challenge

Companies face challenges in both remaining **agile to adapt** to changing markets and also maintaining high levels of **security**. Cloud-based technologies are becoming the new normal, but there is still a great deal of vulnerabilities that can be exploited by malicious actors.

Data breaches are detrimental to your customers' privacy and trust, your brand reputation and your potential revenue. Not only can sensitive data be exposed, but companies can incur steep fines for failing to ensure that their workloads are compliant with industry standards.

DevSecOps is the methodology of incorporating security throughout an organization's processes, rather than attempting to bolt on security at the end of a product's development. Although a sizeable investment, businesses will save more in the long run by investing in this methodology, using secure technologies and adhering to customer privacy best practices. But what are the best ways to do this?

Average cost of a data breach

$3.92M[1]

Percentage of breaches caused by malicious or criminal acts.

51%. [1]

Organizations in breach of GDPR can be fined up to 4% of annual global turnover or **€20 Million.**[2]

1. IBM security study - https://www.ibm.com/security/data-breach/
2. https://eugdpr.org/the-regulation

The IBM solution

IBM Hyper Protect Virtual Servers is a software solution that is designed to protect your mission-critical workloads with sensitive data from both internal and external threats. This offering provides developers with security throughout the entire development lifecycle.

- All images are signed and securely built with a trusted CI/CD (Continuous Integration, Continuous Delivery) flow.
- Infrastructure providers will not have access to your sensitive data, but can still manage images through APIs.
- Validate the source used to build images at any time – no backdoor can be introduced during the build process.

This offering aligns with the IBM Cloud Hyper Protect Services portfolio for on-premises deployment to IBM Z® and IBM LinuxONE™ servers.

Build applications with security

Deploy workloads with trust

Manage applications with simplicity

The IBM solution

Trusted CI/CD

All images are signed and securely built with a trusted CI/CD flow. This means that no backdoor or malware can be introduced during the build process, ensuring that the confidentiality of the application is protected. As a result, solution developers can confirm their image's integrity, knowing that the securely built image only contains what's intended.

Restricted Access

Implementing least privilege access is a common security practice – this means no one has the access to resources or data unless they absolutely need it. In this solution, infrastructure providers and cloud admins do not have access to the application data, including memory, application logs, keys, and data in local storage. They can still manage the application through APIs, but no access to the data itself is needed.

Image Provenance

Full transparency of the application image contents and their origin are made available via a Manifest – making it easier for developers to validate what they're shipping and users to know what they're deploying in their environment. Auditors can use the Manifest to compare a components list against actual components that are reviewed or scanned to check for malware or abnormalities before deploying.

.

No cloud / system admin access

Developers can build and validate their own images

Docker images inherit security without any code changes

The solution value

Security

Implementing a DevSecOps methodology is key in saving enterprises money, time, and frustration down the road. A development pipeline that incorporates security throughout, avoids additional costs of trying to add security measures in after the fact. In addition, it reduces the risk of data breach or malicious threat, avoiding diminished client trust and brand reputation.

Simplicity

Deployment of applications is all about empowering developers – this includes providing familiar tools as well as a secure, enterprise wide, fully automated, and continuous, software delivery pipeline. This means adding security without adding complexity to the process. Admins and developers can still execute their job with the same user experience, all without accessing sensitive data or leaving vulnerabilities for external hackers to exploit.

Innovation

Enterprises need to modernize, without compromising on existing security or functionality. By enabling the adoption of containers, microservices and open standard tooling for development, innovation can happen even faster. Modernization of applications allows for agility and quick response to changing markets and changing client needs. Remain competitive while also protecting your business IP and client trust.

Flexibility

Hyper Protect Services provide secure cloud services for both on-prem and off-prem deployment of mission critical workloads. This means build once, and have the flexibility to deploy anywhere, giving the same trusted security, availability, and reliability expected from IBM Z and LinuxONE. Based on individual needs per workload (resources, time, cost, etc.), you can choose to develop cloud native both in the private, public cloud, or a combination of the two.

Learn more

For more information, go to:
https://www.ibm.com/marketplace/hyper-protect-virtual-servers

Financing Available: IBM Global Financing provides numerous payment options to help you acquire the technology you need to grow your business. For more information, visit: ibm.com/financing.

IBM Systems, New Orchard Road Armonk, NY 10504.
Produced in the United States of America, January 2020.

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 performance data and 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. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.