White Paper

Building Modern Hybrid Cloud Infrastructure for the Digitally Determined

Sponsored by: IBM

Ashish Nadkarni Peter Rutten

June 2020

EXECUTIVE SUMMARY

Digitally determined organizations need a modern infrastructure strategy to reliably accelerate their transformation journey, which involves implementing technology-enabled business strategies to expand their competitive differentiation in the market. With such an infrastructure in place, digitally determined firms effectively and efficiently combine (technology) platforms, (business) processes, (data) governance, and (people) talent to gather deep, timely, and actionable insights from data. These insights can be used to optimize business operations, accelerate innovation (develop new and innovative products and services), and transform customer engagement. Industry-leading hybrid cloud–enabling platforms enable businesses to have a common infrastructure foundation for hosting current-gen apps, which are used for revenue-generating operations, and next-gen apps, which are used for future proofing the business itself. Such platforms are versatile, extensible, and secure to support the diverse compute and data management requirements of each set of apps — which spans virtualization, containerization, seamless mobility between on premises and public cloud, and out-of-box support for developer-ready software stacks.

IBM LinuxONE is an example of a powerful, secure, modern, and scalable platform that enables cost-effective consolidation of current- and next-gen apps on a hybrid cloud infrastructure. With LinuxONE, digitally determined organizations can:

- Quickly deploy mission-critical and cloud-native workloads on an open deployment platform enabled by **Red Hat OpenShift** and **IBM Cloud Paks**.
- Ensure the highest levels of privacy and protection of data in flight, at rest, and beyond host boundaries with **Data Privacy Passports** and **improved hardware-assisted security.**
- Obtain the highest levels of service quality with a resilient, scalable, and compliant platform that supports workload isolation using **Secure Execution for Linux** and embedded artificial intelligence (AI) for faster diagnostics and operational recovery.
- Gain deployment flexibility by choosing to deploy a platform built with modular industry-standard frames and onboard acceleration for a compressed datacenter footprint.

In addition, IBM's fully managed IBM Cloud Hyper Protect Services such as IBM Cloud Hyper Protect Virtual **Servers** and **IBM Cloud Hyper Protect DBaaS** (available via IBM catalog) offer LinuxONE-based services in the IBM Cloud.

Note: This document was developed with IBM funding. Although the document may utilize publicly available material from various vendors, including IBM, it does not necessarily reflect the positions of such vendors on the issues

SITUATION OVERVIEW

Digitally determined firms focus on making effective use of technology to transform themselves. In the short term, digital transformation initiatives are all about achieving superior business outcomes — for example, improving customer experience, optimizing business operations, and gaining better control over costs. In the longer term, businesses have a mandate to transform themselves to stay ahead of the game — for example, expanding their competitive differentiation in existing markets, expanding into newer markets, and developing new approaches to customer engagement.

IDC believes that data is to organizations what drinking water is to humans. It is not just the quantity but also the potability that matters. To gain that potability, organizations must be able to combine (technology) platforms, (business) processes, (data) governance, and (people) talent to gather deep, timely, and actionable insights from this data.

Infrastructure for the Digitally Determined

Modern infrastructure — and more specifically a modern, secure, and scalable hybrid cloud infrastructure — is becoming a de facto approach for organizations to reliably accelerate their transformation journey. A modern hybrid cloud infrastructure enables businesses to have a common infrastructure foundation for embracing "IT duality," a situation in which the IT organization must support revenue-generating operations while providing a foundation for enabling future readiness-related business investments:

- Revenue-generating operations are supported by current-gen apps. Current-gen apps are mostly procured off the shelf and require traditional approaches to infrastructure — for example, externally attached storage and virtual machines (VMs).
- Future readiness-related investments are supported by next-gen apps. Next-gen apps are designed to be cloud native, use newer development methodologies, and are often deployed on newer computing technologies such as containers.

In the long run, it is not cost effective for businesses to implement "IT duality" by having dedicated infrastructure for each set of apps. This creates additional overhead in terms of people and processes, and as the firm transitions into the future, it has the added challenge of wasted technology investments that cannot be transferred because of the lack of compatibility between the application and the underlying hardware platforms and systems. In the long run, it is also not wise for businesses to pursue an all-or-nothing cloud strategy. There are merits to on-premises and cloud deployments, and the best approach is to embrace an infrastructure architecture that combines the best of both worlds.

A Hybrid Cloud Infrastructure Foundation

Firms benefit from investing in an infrastructure architecture that combines the best of on-premises and public cloud deployments. Known as hybrid cloud infrastructure, it is built using platforms that are versatile, extensible, secure, and crucially support the diverse compute and data management requirements of both current- and next-gen apps. Such platforms have the following key attributes:

- **They are designed to be modular.** Designed with industry-standard datacenter building blocks, the platforms can scale effortlessly on premises, requiring no additional accommodations. They also conserve datacenter footprint by offering hardware offloads.
- **They feature an open, scalable, and flexible deployment operating environment that supports quick deployment of mission-critical and cloud-native workloads on premises.** The platforms feature packaged orchestration frameworks that can effortlessly scale the workload to the public cloud in a secure manner.

- **They offer pervasive security that goes beyond just encryption of data.** The platforms ensure the highest levels of privacy and protection of data in flight, at rest, and beyond host boundaries. They also offer a secure conduit through which data can be transferred to and hosted in a managed service offering.
- **They are highly resilient, scalable, and compliant platforms that offer the highest levels of service quality and support workload isolation in a secure application runtime environment.** The platforms also feature embedded AI for faster diagnostics and operational recovery.

Pervasive Infrastructure Security Is More Than Encryption

Security continues to be a top concern for CXOs when it comes to data and infrastructure. Firms have learned (some the hard way) from well-publicized incidents from the recent past that taking a holistic approach to security means treating internal threats on par with external threats. It means ensuring that anyone who has or can gain unauthorized access to parts of the infrastructure is not able to simply "walk away with a motherload of sensitive data." It is for this reason that the security paradigm for a modern infrastructure must reach beyond just data encryption. It must be pervasive and always on — identifying risks and protecting against internal and external threats. Crucially, it must include a secure runtime environment that cannot be compromised by anyone with administrator access. Infrastructure security at firms should be an intricate system of checks and balances that includes:

- **Multilayer security.** Authorization and authentication schemes intercept, grant, and/or prevent internal and external user-, application-, or network-level access in real time. A trusted computing environment offers to protect and isolate workloads (from both internal and external threats) better than a standard software environment.
- **Trusted execution environment (TEE).** TEE is meant to protect and isolate workloads (from both internal and external threats) better than a standard software environment. It is an environment for executing code, in which those executing the code can have high levels of trust in that surrounding environment because it can ignore threats from the rest of the device.
- **Horizontal isolation.** This limits administrative access to the data that resides inside or can be accessed from within virtual machines, containers, or server instances and their backups and snapshots. Current practices and technology limitations provide VM administrators, when given administrative authority, broad access to potentially very sensitive information.
- **Vertical isolation, access matching, and auditing.** This protects data from not only peer environments but also administrators above those environments, matching "need to know" with "sensitivity index" of data and "actual access" to the platforms that can access this data. Always-on auditing mechanisms detect patterns and can alert administrators to system or data breaches so that the scope of the breach can be contained quickly.
- **Data privacy.** Data is encrypted, followed by a stringent key management scheme that is decoupled from user, app, and network authentication and authorization schemes. It should provide a secure **conduit for moving** data off platform to a managed cloud service.

Vertical Scaling for a Data-Centric Approach to Infrastructure

There is a myth in the IT industry that taking a horizontal scaling approach to next-gen application architecture is a be-all and end-all solution, whether on premises or in a public cloud, to all the performance and scaling challenges facing current-gen applications. While horizontal scaling has its benefits, it also introduces risks to the business, such as:

- **Data consistency and resource utilization.** Many horizontal scaling apps, including those that make use of server-based storage and those that run in the cloud, make use of an eventual data consistency scheme implemented in the form of asynchronous replicas or erasure-coded copies. This means that at any snapshot in time, there can be multiple sources of truth should there be any kind of disruption or failure, such as a security incident. In addition, such applications require the addition of nodes for scaling capacity and performance independent of each other, leading to underutilization of resources and therefore additional operating expenses in the long run.
- **Cluster deficiency.** The use of built-in or third-party clustering software further complicates the data consistency and resource utilization situation — where networked nodes are coupled under an automated active-passive or active-active operating mode. While the software is expected to take corrective action under normal circumstances, it often fails to do so. In addition, human-induced mistakes can often exacerbate the situation when quick actions lead to unforeseen complications.

There are merits to taking a vertical scaling approach for platforms that run systems of record and insight. Such platforms make it easier to:

- Manage a single source of truth in terms of data consistency and security, even when dealing with databases and applications inherently designed with an eventual data consistency.
- Provide superior response times by adding more "cores," which enables on-demand performance without the need for any external provisioning activities, making it easier to enable a singular security paradigm across the entire system.
- Make better use of the infrastructure through the ability to share resources across all VMs.

IBM LinuxONE — HYBRID CLOUD INFRASTRUCTURE FOR THE MODERN ENTERPRISE

In 2015, IBM introduced its LinuxONE platform specifically for buyers seeking a fully engineered enterprise-grade solution with a unique balanced multitenant platform architecture and industry-leading pervasive security that is optimized for data-serving and mission-critical workloads and applications. Since then, IBM has continued to add more features to make the platform more versatile and extensible. With the introduction of LinuxONE III, the platform has truly evolved into an enterprise hybrid cloud infrastructure platform that is best suited for:

- Firms that choose to run revenue-generating business applications on premises because of data privacy and regulatory requirements or because of the inability of the public cloud service provider (SP) to meet stringent availability, performance, and scalability objectives required by their business.
- Managed SPs and cloud SPs that need a secure multitenant platform for hosting applications and want to differentiate themselves from the large public cloud SPs by providing superior quality of service. Such providers offer secure hybrid cloud solutions.
- Enterprises that are building hybrid clouds and developing cloud-native applications to run across those hybrid clouds. They benefit from LinuxONE because the platform provides vertical and horizontal scalability for the containers thanks to the scale-up ability of the processors, the platform's security, and the ability to run cloud-native applications on the same platform where the data resides and reduce latency between the data and the applications.

LinuxONE Architecture

IBM has engineered LinuxONE as a highly scalable data-serving and transaction-processing platform that is vastly different from a standard x86-based server running Linux. In addition, LinuxONE combines the best of both worlds – the qualities of IBM's premier enterprise platform with the openness of Linux and open source software.

The nondegrading performance and scaling capabilities of LinuxONE (even when at near 100% utilization) simplify the solution and reduce the extra costs that many IT architects assume to be necessary to factor in degrading performance above 50% utilization. Further, IBM has designed LinuxONE to be custom ordered to the firm's specifications, and LinuxONE comes fully tested to resist hazards such as earthquakes, fires, and floods.

Design Based on Proven IBM Enterprise Platform Technologies

LinuxONE is a tried and tested mission-critical hardware platform with a unique shared memory and vertical scaling architecture. Dedicated Power cores in I/O channels and SAPs for I/O orchestration enable the platform to handle heavy I/O without compromising on latency. This makes LinuxONE vastly better for running stateful workloads such as databases and systems of record.

Built with Hardware-Assisted Data Compression

A new feature on LinuxONE is hardware-based data compression on the processor chip. Previous versions of the platform had a compression card, or users could perform data compression with software. With the latest LinuxONE, they can execute much faster data compression on the chip.

IBM has repackaged the functionality of the IBM LinuxONE I/O card (called IBM zEnterprise Data Compression [zEDC] Express) into the Integrated Accelerator for zEnterprise Data Compression. This is an architected instruction that is publicly available, thereby opening it up for software exploitation. Furthermore, the instruction is nonprivileged, meaning that one does not need to be authorized or in kernel mode in order to use it. As a result, any user space application can take advantage of this accelerator without the need for special privileges. This is especially important on LinuxONE because it means that there is no need for kernel support. The acceleration is fully deployed in the user space. Furthermore, the new instruction is available to all guests with no virtualization requirement because it is part of the instruction architecture.

The accelerator is fully DEFLATE compliant, a very common compression format that is used throughout industry and in many protocols. This is important for open source software being able to take advantage of it. The expected benefits are a significant reduction in time to compress and decompress data and lower CPU use to perform that operation. What's more, high-speed compression greatly optimizes data flows through a system.

Runs Most Enterprise-Adopted Open Source Linux-Based Software

LinuxONE supports several Linux-based open source software stacks – they run on hardened versions of commercial Linux distributions (e.g., Red Hat Enterprise Linux, SUSE Linux Enterprise, and Ubuntu Linux LTS). This makes it easy for enterprises to build, model, deploy, and manage enterprise applications with a scalable hybrid architecture. In recent times, IBM has added support for open source software packages such as databases and data management (e.g., MariaDB, PostgreSQL, MongoDB, and Apache Spark), virtualization and container platforms (e.g., KVM, Linux containers, and OpenShift), automation and orchestration software (e.g., Kubernetes, OpenStack, Puppet, Node.js, Juju, and Chef), and compute-intensive workloads such as blockchain.

Hybrid Cloud Powered by Red Hat OpenShift and IBM Cloud Paks

Since its launch, LinuxONE has evolved into a very capable enterprise-grade open hybrid cloud platform powered by two key software stacks: Red Hat OpenShift and IBM Cloud Paks, with IBM Cloud Infrastructure Center managing the underlying virtual infrastructure.

Red Hat OpenShift for LinuxONE

With the broad move toward containerized applications, enterprises need a robust orchestration and availability platform that uses open source tooling. IBM and Red Hat announced support for OpenShift — Red Hat's container and Kubernetes-based PaaS — on LinuxONE in August 2019. Currently, OpenShift is the de facto hybrid cloud deployment and orchestration stack on LinuxONE, enabling portability of applications across public and on-premises private cloud. With OpenShift on LinuxONE users can:

- Develop and deploy cloud-native applications while taking advantage of the platform's security features and exploit the scalability of the platform when containerizing large applications.
- Leverage single-point management across various on-premises and cloud platforms, achieve agility across their cloud ecosystem, use open technology and tooling, and support mobility of workloads, services, and data across the hybrid cloud ecosystem.
- Move containerized applications onto a different computing platform as needed — for example, a container built for an x86 platform could then be rebuilt and deployed on LinuxONE. Users can also factorize applications into microservices and then containerize them or vice versa.

IBM LinuxONE offers on-demand compute with horizontal and vertical scalability that can nondisruptively grow databases without requiring any partitioning or sharding while maintaining response times and throughput. Running Red Hat OpenShift on IBM LinuxONE also enables cloud-native applications to easily integrate with existing data on the platforms, enabling latency to be reduced by avoiding network delays.

IBM Cloud Paks

Beyond containers and Kubernetes, enterprises still have a need to orchestrate their production topology and to provide management, security, and governance for their applications. They need to do this while improving efficiency and resiliency, reducing costs, and maximizing ROI. IBM Cloud Paks are enterprise-ready, containerized software solutions that give clients an open, faster, and more secure way to move core business applications to any cloud. Each IBM Cloud Pak includes containerized IBM middleware and common software services for development and management, on top of a common integration layer, and is designed to reduce development time significantly. IBM Cloud Paks run on top of Red Hat OpenShift and are optimized for productivity and performance on Red Hat OpenShift on IBM LinuxONE.

IBM Cloud Infrastructure Center

In support of Red Hat OpenShift and IBM Cloud Paks, the IBM Cloud Infrastructure Center provides simplified infrastructure-as-a-service (IaaS) management across compute, network, and storage resources. It provides a consistent, industry-standard user experience to define, instantiate, and manage the life cycle of virtual infrastructure used by OpenShift and the Cloud Paks as well as the deployment of images and policies to maximize resource utilization.

LinuxONE Security

LinuxONE is one of the few platforms in the market in which security is built in and "already on" — clients can benefit from all security features when it is procured. Having security at the hardware level can take one level of risk out of the mix. The features discussed in the sections that follow make LinuxONE unique in many respects.

EAL5 + Isolation at the LPAR Level

This secure multitenancy feature provides isolation between peer environments and greatly benefits enterprises as well as service providers. In addition, the Crypto Express adapter in LinuxONE is designed to be FIPS 140-2 Level 4 certified (the highest possible certification level), meaning that if a tamperproof enclosure for encryption keys is compromised, the system automatically writes zeros over the data to protect the keys.

IBM Hyper Protect Virtual Servers

The IBM Secure Service Container is a framework for securely deploying software appliances on LinuxONE. Secure Service Container appliances are deployed on LinuxONE LPARs that are configured in "SSC mode." The Secure Service Container technology is now available in the cloud as IBM Cloud Hyper Protect Virtual Servers and on premises as IBM Hyper Protect Virtual Servers.

IBM Hyper Protect Virtual Servers provide:

- **Industry-leading peer isolation:** The Secure Service Container technology leverages LinuxONE EAL5+-certified LPAR isolation for near "air gap" separation of appliance environments on a single footprint, obfuscating workloads from the underlying infrastructure.
- **Vertical isolation and protection of data from privileged users:** Direct (SSH) operating system access via a shell or command-line interface is disabled by design for appliances configured in "SSC mode" LPARs. Appliance management and communication are permitted only through well-defined RESTful APIs and web interfaces, prohibiting access by users with elevated system authority; only users authorized for the Secure Service Container LPAR and the appliance running within are granted access to it, thus protecting the appliance's data and execution environment from the insider threat, whether inadvertent or malicious.
- **Confidentiality of data and code — in flight and at rest:** Direct memory access to an IBM Hyper Protect Virtual Server appliance is disabled, and various layers of encryption and signatures are implemented to ensure that no bit of data leaves the appliance memory without being encrypted.
- **Validation of appliance code to reduce the risk of tampering or malware:** IBM Hyper Protect Virtual Server appliances are secured from creation in a trusted firmware boot sequence before software deployment and made tamper resistant through signature verification.

Secure Service Container framework enhances IBM-offered solutions such as the IBM Blockchain Platform, both on premises and in the IBM Cloud, with the encryption and data privacy needed for business networks to host mission-critical, enterprise-grade blockchain data and chain code. Secure Service Container framework is well suited to users for deploying container-based applications on premises in Secure Service Container instances on LinuxONE. This enables applications to leverage the capabilities of the Secure Service Container technology while dynamically scaling up in a single LinuxONE footprint and integrating with users' enterprisewide, cross-platform containers and DevOps strategy. With the latest LinuxONE release, IBM has also added:

- Secure boot-protecting platforms from root-level attacks and viruses that target vulnerabilities during the boot process
- Fibre Channel endpoint security, providing end-to-end data-in-flight protection of Fibre Channel links within and across datacenters to eliminate unauthorized access

Confidential Computing — Introducing Secure Execution for Linux

Confidential computing, an industry movement around using technology to protect data in use, was born out of the need to take a preemptive approach to tackling cyberthreats, which appear to be increasing each day. Compliance with stricter regulations is a fundamental priority for leading enterprises around the world. Such regulations call for maintaining the confidentiality and integrity of applications and their data.

Secure Execution furthers the confidential computing agenda through the implementation of a hardware-based TEE on LinuxONE platform. Key capabilities of Secure Execution for Linux are:

- **Limited access for host administrators.** In traditional x86-based computing environments, the host can access the memory and data of guest applications. Barring some kind of a hardware isolation in place, this situation increases the potential for malicious software to be proliferated throughout the entire software stack. Secure Execution provides isolation between a KVM hypervisor host and guests in virtual environments to help safeguard against insider threats such as malicious administrators while allowing administrators to manage and deploy workloads as black boxes and continue normal job functions. 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 virtual machines and individual containers and help prevent system compromise.
- **Scalable isolation between workloads.** Secure Execution also helps administrators provide isolation between individual multitenant workloads running on a shared LPAR. Protecting highly sensitive data from other hosted workloads can provide businesses the confidence that all their assets are not inadvertently exposed in the event of one or more compromised applications in the same virtual environment. Secure Execution is designed to help enterprises that want to implement the highest levels of confidentiality and data integrity for workloads subject to regulatory requirements.

IBM Secure Execution for Linux provides scalable isolation for individual workloads to help protect from insider and outside attacks. IBM Secure Execution helps protect and isolate workloads running in LinuxONE hybrid cloud environments.

Data Privacy Passports

With the latest LinuxONE release, IBM also announced IBM Data Privacy Passports, which extends the protection of data beyond the domain of its original platform. For example, when a user is extracting data from a LinuxONE server and then using that data on a distributed system, Data Privacy Passports allows for the data protection to be extended to that distributed system. The data goes out encrypted as part of a trusted data object and can then be accessed there according to the centralized data access policy. If data access is revoked, a user will no longer be able to access it on the distributed system through the Data Privacy Passports infrastructure.

Data Privacy Passports uses what IBM refers to as a Passport Controller, which is deployed in a Secure Service Container and can ingest data from any Java Database Connectivity (JDBC) source. It protects data that is accessible through JDBC on LinuxONE, Linux on Z, IBM z/OS, Power Systems, or x86. Data Privacy Passports complements pervasive encryption in that it provides privacy for data on and off the platform through a data-centric approach, while pervasive encryption protects database or application data at the data source.

In this protection scenario, data that originates on the systems of record is protected and then moves through the enterprise while continuing to be protected through the organization's centralized data access policy. How this works is that the data is packaged into a trusted data object that contains metadata and encrypted data. This trusted data object then needs to be processed through the Data Privacy Passports infrastructure in order to be accessed in its clear state. In other words, the data has been protected as a trusted data object, and it is in this state that the encrypted data is moving around and can travel across systems.

Flexible Computing with LinuxONE III LT2

The IBM LinuxONE III LT2 refresh offers unprecedented levels of computing flexibility. It uses the same IBM z15 chip technology present in LinuxONE III LT1. LinuxONE III LT2 is designed to be modular and scalable.

- **Frame.** A single 19in. rack frame supports up to two CPC drawers and redundant PDU power and air cooling for enhanced high availability. Secure Execution for Linux improves tenant density for fortified, container-level granularity.
- **Compute.** LinuxONE III LT2 supports a maximum of 65 cores. A client could have more than twice the number of Linux cores than the LinuxONE Rockhopper II. It supports up to four I/O drawers that can support up to 40 crypto processors. The LinuxONE III LT2 supports accelerators for cryptography (Central Processor Assist for Cryptographic Functions [CPACF]) and compression (Integrated Accelerator for zEDC).
- **Memory and data.** Built with a Redundant Array of Independent Memory (RAIM) design, it supports up to 16TB of system memory (minimum 64GB). This enables LinuxONE III LT2 to support new workloads, data-in-memory applications, and larger local buffer pools. It can efficiently process huge amounts of information for faster business insights.
- **IBM Adapter for NVMe.** This allows SSD connection to I/O subsystem, while higher bandwidth and I/O rates can be achieved with FCP Express32S adapters. The use of a compression accelerator reduces the cost of storing, transporting, and processing data.

IBM Cloud Hyper Protect Services Offered via IBM Cloud Catalog

IBM Cloud Hyper Protect Services enable enterprises to ensure the security of cloud data, digital assets, and workloads. They provide built-in protection for data at rest and in flight – thus helping developers seamlessly build secure cloud applications using a portfolio of cloud services powered by IBM LinuxONE. The LinuxONE platform ensures that client data at rest and in flight is always protected. It gives enterprises complete authority over sensitive data and associated workloads – protecting even from cloud administrator access. LinuxONE also allows customers to build mission-critical applications that require quick time to market and dependable rapid expansion.

IBM Hyper Protect Database as a Service

In recent times, there has been a surge in the adoption of open source–based relational and nonrelational databases in the enterprise, much of it because of acceleration in the development of next-gen apps. IBM is positioning LinuxONE to firms that want to deploy an "as a service" environment for structured and unstructured data management. The security, scale, and performance of LinuxONE make it an ideal platform for deploying database as a service (DBaaS).

Hosted Off-Premises Cloud

Hyper Protect Database as a Service is a self-service model in which the data is hosted on LinuxONE for extreme scale and security features. This is currently being offered as IBM Cloud Hyper Protect DBaaS, built and deployed on LinuxONE in the IBM Cloud as a public cloud service.

IBM Cloud Hyper Protect Virtual Servers

Hyper Protect Virtual Servers is an IBM Cloud service that provides highly secure virtual servers that can run Linux applications and containerized workloads. It offers a flexible and scalable framework that enterprises can use to quickly and easily provision and manage the created virtual servers. It enables enterprises to protect their critical Linux workloads during build, deployment, and management for LinuxONE servers running on premises. With this service, enterprises can enable their IT staff to:

- **Deploy workloads with trust.** Application administrators can validate the provenance of their applications via a workload manifest before they are deployed into production.
- **Manage applications with simplicity.** IT administrators can manage their firm's infrastructure without visibility into sensitive code or data.
- **Encrypt and sign critical solution components.** Data owners can enable ensure data governance by giving images access to the industry-leading FIPS 140-2 Level 4 Hardware Security Module for signature and encryption.

Innovative LinuxONE Use Cases — Blockchain

LinuxONE is a highly engineered solution that is exceptionally good at data-serving and stateful applications, which benefit from a vertical scaling environment with shared memory and shared processing over an internal high-speed fabric versus running on a horizontally scaling cluster of general-purpose Linux servers or virtual machines. The use cases discussed in the sections that follow showcase the true power of LinuxONE. IDC sees blockchain emerging in highly regulated industries (such as financial technologies) where uncompromised transactional security is of paramount importance. Accordingly, these industries need a transaction-oriented (i.e., highly scalable) computing infrastructure platform that is designed around stringent and pervasive security schemes that are necessary for end-to-end blockchain deployments.

LinuxONE is well suited for running blockchain on premises and in the cloud. For example, LinuxONE platforms running in the IBM Cloud demonstrate the conformance of this platform as an uncompromisingly secure and powerful data-serving cloud platform for blockchain. LinuxONE can also be used to deploy and scale blockchain applications on premises when mandated by data residency or business requirements.

The IBM Blockchain Platform is available as an IBM-managed blockchain as a service on the IBM Cloud, on other cloud environments, and on premises. The IBM Blockchain Platform is an enterprise-ready blockchain service based on the latest version of Hyperledger Fabric, a Hyperledger project hosted by the Linux Foundation, which IBM actively contributes to. The service enables developers to quickly build and host security-rich production blockchain networks on the IBM Cloud. This service is available to be LinuxONE based both on premises and in the IBM Cloud and could be considered one of the best in the industry in terms of security, performance, and data isolation specifications.

Building on blockchain and LinuxONE, the IBM Hyper Protect Digital Assets Platform then provides clients with a robust environment for digital asset management. Encryption keys previously were stored online in "hot wallets" to facilitate access but with a greater exposure to malicious actors or stored offline in a "cold wallet." The IBM Hyper Protect Digital Assets Platform provides exchanges and custodians with a place in which hot wallets, in conjunction with a properly secured exchange or custody application, can be deployed with increased protection while decreasing the time it takes to access those assets.

Cognition Foundry Helps Start-Ups Leverage Enterprise Technologies for Innovation

Guiding start-ups and small companies with architectural design insights and application development while providing access to the extreme computing resources made available in LinuxONE, Cognition Foundry aims to level the playing field for disruptive entrepreneurs. Cognition Foundry's team of developers helps start-ups by developing and testing their applications, ensuring they get the maximum benefit of a highly engineered, open IT infrastructure. Leveraging its large network, Cognition Foundry links rising stars to the enterprise architecture, design, and business skills needed to win in competitive markets while controlling IT costs. The ability of LinuxONE to run open source software is a huge benefit for Cognition Foundry given how pervasive open source software is in the start-up space.

The ability to scale vertically on the platform enables massive expansion without adding infrastructure, which is a tremendous help for Cognition Foundry, a service provider focused on optimal asset management. Recently, the company provided a hybrid cloud platform to its customers, enabling them to move containerized applications back and forth between their on-premises LinuxONE environment and LinuxONE in the IBM public cloud. Cognition Foundry's clients include organizations such as Plastic Bank and Newlight Technologies.

Newlight Technologies Turns Greenhouse Gases into a Resource with Blockchain-Backed Technology

Climate change is one of the greatest challenges facing mankind today. Scientists are predicting dire consequences as a direct result of global warming unless we act now. Newlight Technologies has developed a pathway that it believes can be part of the solution.

Newlight aims to help tackle climate change by reducing greenhouse gas levels through a carbon capture process. It has developed a technology that uses greenhouse gases to produce high-performance biomaterials. In partnership with IBM Business Partner Cognition Foundry, Newlight harnessed blockchain technology to ensure that every step in its process and its overall environmental impact can be independently tracked, audited, and communicated to consumers. Newlight uses an IBM Blockchain solution running on LinuxONE to create an indelible record of each step in the transformation of greenhouse gas to high-performance AirCarbon biomaterials.

CHALLENGES AND OPPORTUNITIES FOR IBM

IBM has continued to invest in LinuxONE. What was introduced as a formidable platform designed for workloads and applications of the future is now a complete, secure, and scalable hybrid cloud solution. With LinuxONE, IBM is seeking to repeat its long-term success with IBM Z, which itself has evolved nicely. IBM efforts to expand the value and appeal of LinuxONE to a broad spectrum of clients, industries, geographies, and workloads have paid off:

- A secure cloud-native hybrid cloud solution that enables enterprises to quickly and securely deploy mission-critical and cloud-native workloads on an open deployment platform enabled by **Red Hat OpenShift** and **IBM Cloud Paks** (In addition, IBM can provide high levels of privacy and protection of data in flight, at rest, and beyond host boundaries with Data Privacy Passports and improved hardware-assisted security.)
- A flexible but resilient hybrid cloud solution that delivers enterprise-grade service quality with resiliency and scalability (It supports workload isolation using **Secure Execution for Linux** and embedded AI for faster diagnostics and operational recovery. Enterprises gain deployment flexibility by choosing to deploy hybrid cloud infrastructure using modular industry-standard frames and onboard acceleration for a compressed datacenter footprint.)
- A platform backed by a suite of fully managed cloud-based **IBM Cloud Hyper Protect Services** such as **IBM Cloud Hyper Protect Virtual Servers** and **IBM Cloud Hyper Protect DBaaS** that further enhance the capabilities of an on-premises LinuxONE deployment

IDC believes that with these enhancements, IBM has the opportunity to make a compelling case for LinuxONE for enterprises seeking a common, secure, and scalable hybrid cloud environment for their digital transformation initiatives.

IBM must continue to shift the conversation away from a direct comparison of LinuxONE with a cluster of general-purpose x86-based servers. It must also talk about LinuxONE as a complete hybrid cloud solution with industry-leading software stacks, security, scalability, and performance features all integrated for a true out-of-box experience. It must move the discussion on data resiliency to LinuxONE being an unrivaled platform for single-source-of-truth data serving with the highest levels of resiliency and service quality.

CONCLUSION

Hybrid cloud is a strategy and not a product. When deploying a solution that seeks to deliver key objectives of this strategy, enterprises must pay attention to the platform choices they are making. In addition, the platform must offer secure multitenancy where the credentials are protected, peer environments are highly isolated from one another, encryption is built in at the firmware level, and encryption keys are protected by hardware. It must offer vertical security where data such as sensitive customer records and confidential information is protected from internal and external threats. Security must be pervasive (i.e., the entire system is fully protected) and with hardware partitions that are isolated from one another. Finally, the platform must be developer friendly — it must use industry-standard software stacks that make it easier for developers to develop and deploy applications.

IBM LinuxONE combines the advantages of both commercial (IBM Z) and open source (Linux) systems with security capabilities unmatched by any other offering and scalability for systems-of-record workloads. It is a platform worthy of investment.

About IDC

International Data Corporation (IDC) is the premier global provider of market intelligence, advisory services, and events for the information technology, telecommunications and consumer technology markets. IDC helps IT professionals, business executives, and the investment community make fact-based decisions on technology purchases and business strategy. More than 1,100 IDC analysts provide global, regional, and local expertise on technology and industry opportunities and trends in over 110 countries worldwide. For 50 years, IDC has provided strategic insights to help our clients achieve their key business objectives. IDC is a subsidiary of IDG, the world's leading technology media, research, and events company.

Global Headquarters

5 Speen Street
Framingham, MA 01701
USA
508.872.8200
Twitter: @IDC
idc-community.com
www.idc.com

Copyright Notice

External Publication of IDC Information and Data — Any IDC information that is to be used in advertising, press releases, or promotional materials requires prior written approval from the appropriate IDC Vice President or Country Manager. A draft of the proposed document should accompany any such request. IDC reserves the right to deny approval of external usage for any reason.