White Paper

IBM LinuxONE: A Secure Data-Serving and Hybrid Cloud Infrastructure

Sponsored by: IBM

Peter Rutten Ashish Nadkarni
September 2019

IDC OPINION

A technology-enabled business strategy such as digital transformation (DX) makes it possible for firms to expand their competitive differentiation in the market. Although disruptive, DX requires firms to effectively and efficiently combine (technology) platforms, (business) processes, (data) governance, and (people) talent to gather deep and timely insights from data and actuate these insights to optimize business operations, accelerate innovation (develop new and innovative products and services), and transform customer engagement.

Gaining deep, timely, and actionable insights from large and diverse data sets requires firms to take innovative approaches to technology platforms. A recommended approach is to deploy current- and next-gen applications (apps) on a modern infrastructure platform. Current-gen apps are mostly procured off the shelf, require traditional approaches to infrastructure, and support established revenue-generating business operations. Next-gen apps are developed specifically for future-readiness DX initiatives, are designed to be cloud native, use newer development methodologies, and are often deployed on newer computing technologies such as containers. This means that modern infrastructure solutions capable of hosting current- and next-gen apps must support extreme performance and scalability; be optimized for data consolidation and serving; support pervasive security; be agile and dependable; support both traditional and newer computing, development, and deployment models; and natively support modern open source frameworks.

LinuxONE from IBM is an example of a secure data-serving infrastructure platform that is designed to meet the requirements of current-gen as well as next-gen apps. IBM LinuxONE is ideal for firms that want the following:

- **Extreme security:** Firms that put data privacy and regulatory concerns at the top of their requirements list will find that LinuxONE comes built in with best-in-class security features such as EAL5+ isolation, crypto key protection, and a Secure Service Container (SSC) framework.
- **Uncompromised data-serving capabilities:** LinuxONE is designed for structured and unstructured data consolidation and optimized for running modern relational and nonrelational databases. Firms can gain deep and timely insights from a "single source of truth."
- **Unique balanced system architecture:** The nondegrading performance and scaling capabilities of LinuxONE — thanks to a unique shared memory and vertical scale architecture — make it suitable for workloads such as databases and systems of records and secure transactional apps such as blockchain.

LinuxONE will be a good fit for enterprises as well as hybrid clouds and cloud service provider firms that require a high-performance, extreme-scale, and highly secure data-serving and consolidation infrastructure platform for running current- and next-gen apps and workloads that are crucial for their DX initiatives.

SITUATION OVERVIEW

Firms embark on digital transformation initiatives to expand their competitive differentiation in the market, now and in the future. DX is a technology-enabled business strategy but is often very disruptive because it requires firms to regularly "reinvent themselves while continuing to operate their business as usual" (i.e., search for new sources of revenue and differentiation while maintaining current sources). DX is about not only getting firms' hands on as much data as possible but also being able to effectively and efficiently combine (technology) platforms, (business) processes, (data) governance, and (people) talent to gather deep and timely insights from this data. Furthermore, it is about being able to actuate these insights to optimize business operations, develop new and innovative products and services, and transform customer engagement. For most firms, DX is not a case of if; it is a case of when. It is no longer the purview of large megacorporations; it applies in equal measure to businesses in industries such as financial and insurance services, manufacturing, retail, and healthcare. The lack of a data-centric strategy poses an existential threat to any firm, large or small, with a product or a service.

Infrastructure for Digital Transformation

Gaining deep, timely, and actionable insights from large and diverse data sets requires firms to take innovative approaches to technology platforms, which comprise applications and infrastructure. From the application side:

- Reinventing the firm means developing new and advanced apps (also known as next-gen apps). Next-gen apps are developed specifically for future-readiness DX initiatives, are designed to be cloud native, use newer development methodologies, and are often deployed on newer computing technologies such as containers.
- Maintaining existing revenue streams means maintaining the currency of business apps (also known as current-gen apps). Current-gen apps are mostly procured off the shelf, require traditional approaches to infrastructure, and support established revenue-generating business operations.

Firms benefit from investing in a modern and shared approach to data management and infrastructure that is specific to the nature of their application portfolio and the nature and objectives of their DX initiatives. This infrastructure must support:

- Extreme performance, flexibility, and scalability
- Data consolidation and sharing between apps
- Stringent service-level objectives
- Pervasive security that goes beyond just encryption of data
- Multiple computing models such as bare metal, virtualization, and containers
- Newer development and deployment models such as DevOps
- Open source cloud frameworks such as OpenStack and automation tools such as Puppet and Chef
- Containers and container orchestration
- Hybrid cloud

Security of Infrastructure Includes Encryption and More

Multiple IDC surveys indicate that security is a top concern for CXOs when it comes to data and infrastructure. The security paradigm for a modern infrastructure goes beyond just data encryption. It is pervasive and always on — identifying risks and protecting against internal and external threats. 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." Infrastructure security at firms should be an intricate system of checks and balances that includes:

- **Multilayer security —** authorization and authentication schemes that intercept, grant, and/or prevent internal and external user-, application-, or network-level access in real time
- **Horizontal isolation —** limiting administrative access to the data that resides inside or can be accessed from within virtual machines (VMs), 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 —** protecting data from not only peer environments but also administrators above those environments
- **Access matching —** matching "need to know" with "sensitivity index" of data and "actual access" to the systems that can access this data
- **Always-on auditing mechanisms —** detect patterns and can alert administrators to system or data breaches so the scope of the breach can be contained quickly
- **Data encryption —** data encryption, followed by a stringent key management scheme that is decoupled from user, app, and network authentication and authorization schemes
- **Data protection —** when data moves off-platform

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 systems that host critical systems of record and certain application components of a high-performing data-serving platform. Such systems 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 systems through the ability to share resources across all virtual machines

IBM LINUXONE

IBM introduced its LinuxONE brand of Linux-only technology specifically for buyers seeking a fully engineered enterprise-grade platform solution with a unique balanced multitenant system architecture and industry-leading pervasive security that is optimized for data-serving and mission-critical workloads and applications. Accordingly, LinuxONE is best suited for:

- Firms that choose to run business applications on-premises because of data privacy and regulatory requirements or because of the inability of the public cloud service provider to meet stringent availability, performance, and scalability objectives
- Managed service providers (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
- 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 system where the data resides and reduce latency between the data and the applications

In addition, IBM is showcasing the capabilities of LinuxONE as an enterprise-grade platform for running blockchain on-premises and in the cloud. For example, LinuxONE systems running in the IBM Cloud demonstrate LinuxONE's conformance 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.

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. For one, LinuxONE supports up to 8,000 Linux servers in a single footprint. In addition, LinuxONE combines the best of both worlds — the enterprise qualities of the IBM Z platform with the openness of Linux and open source software.

Designed Based on IBM Enterprise Platform Technologies

LinuxONE is a tried and tested mission-critical hardware platform (based on IBM Z), with a unique shared memory and vertical scaling architecture. Dedicated Power and RAS cores in I/O channels and SAPs for I/O orchestration enable the platform to handle heavy I/O without compromising on latency and service millions of transactions per second without breaking a sweat. This makes LinuxONE vastly better for running stateful workloads such as databases and systems of record.

Data Compression on the Chip

A new feature on LinuxONE that has been available on IBM Z 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 z14's I/O card (called zEnterprise Data Compression [zEDC] Express) into the integrated accelerator for zEnterprise Data Compression. This is an architected instruction that's publicly available, thereby opening it up for software exploitation. Furthermore, the instruction is non-privileged, meaning that one doesn't 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's 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.

Open Source Linux-Based Software Stack

LinuxONE's hardened Linux-based software stack can run most 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, Docker), automation and orchestration software (e.g., Kubernetes, OpenStack, Puppet, Node.js, Juju, and Chef), and compute-intensive workloads such as blockchain.

The nondegrading performance and scaling capabilities of LinuxONE (even when at 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. In addition, Ubuntu on LinuxONE Systems makes it easy to build, model, deploy, and manage enterprise-grade scale-out clusters and scalable cloud architectures. Finally, 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.

Hybrid Cloud Development

With the broad move toward containers, Kubernetes, and microservices, IBM and Red Hat announced planned support for OpenShift, RedHat's containerization and Kubernetes software across platforms and clouds, on LinuxONE in August 2019. LinuxONE already supported containers and Kubernetes, but with OpenShift, this will enable portability of applications across hybrid cloud, especially for Java and Python. Users can containerize applications and then move those containerized applications onto a different architecture, through multi-architecture support. For example, a container built on an x86 platform could then be deployed on a LinuxONE. Users can also factorize applications into microservices and then containerize them or vice versa.

The benefits of hybrid cloud on LinuxONE with OpenShift are that LinuxONE users can develop and deploy cloud-native applications while taking advantage of the platform's security features, 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.

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 they acquire the system. Having security at the firmware 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 Level-4 FIPS 140-2 certified, meaning that if a tamper-proof enclosure for encryption keys is compromised, the system automatically writes zeros over the data to protect the keys.

IBM Secure Service Container

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 provides:

- **Industry-leading peer isolation:** The Secure Service Container technology leverages LinuxONE's 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 a Secure Service Container 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:** Secure Service Container appliances are secured from creation in a trusted firmware boot sequence before software deployment and made tamper resistant through signature verification.

In its initial stage, the Secure Service Container framework has enabled 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.

In a future stage, the Secure Service Container framework is intended to be made available to users for deploying container-based applications on-premises in Secure Service Container instances on LinuxONE. This will enable users' applications to leverage the capabilities of the Secure Service Container technology while dynamically scaling up to millions of containers in a single LinuxONE footprint and integrating them with users' enterprisewide, cross-platform containers and DevOps strategy.

With the latest LinuxONE release, IBM has also added:

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

Data Privacy Passports

With the latest LinuxONE release, IBM also announced 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 Data Privacy Passport Controller, which is deployed in a Secure Service Container and can ingest data from any JDBC (Java Database Connectivity) source. It protects data that is accessible through JDBC on LinuxONE, Linux on Z, 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.

Innovative LinuxONE Use Cases

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.

Database as a Service on LinuxONE

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. LinuxONE's security, scale, and performance make LinuxONE an ideal platform for deploying database as a service (DBaaS). Clients can look at DBaaS in various forms:

- **Complete control over the DBaaS environment:** This is a do-it-yourself type of model. IBM offers a reference architecture that helps clients set up DBaaS in an on-premises OpenStack environment leveraging Trove. Clients can leverage this reference architecture to quickly get DBaaS up and running with DB2, PostgreSQL, and MongoDB. Clients can also choose to create their own path to DBaaS leveraging other open source and technology options available on the LinuxONE platform.
- **Preconfigured on-premises private cloud:** This would be a more prescriptive solution approach than the former because it would essentially provide much faster deployment and leverage the IBM LinuxONE Secure Service Container framework. IBM is exploring the possibility of delivering this on LinuxONE.
- **Hosted off-premises cloud:** This is essentially a self-service model in which the data is hosted on LinuxONE for extreme scale and security features. This is currently being offered as Hyper Protect database as a service, built and deployed on LinuxONE in the IBM Cloud as a public cloud service.

Blockchain on LinuxONE

Blockchain is 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.

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. It offers a proven audit environment for compliance and forensics.

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 describes its approach as "democratizing access to enterprise IT," allowing smaller users, from the outset, to use the same technologies as those used by governments and Fortune 500 companies.

Cognition Foundry's team of developers helps start-ups develop and test their code, 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. As a service provider focused on optimal asset management, it helps the company tremendously. Recently, the company has provided a hybrid cloud platform to its customers, enabling the customers 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, which works with communities in developing countries to recycle plastic bottles in exchange for useful benefits.

CHALLENGES AND OPPORTUNITIES FOR IBM

With LinuxONE, IBM can lay claim to having built a formidable system designed for workloads and applications of the future, blockchain and open source databases being two key technologies. With LinuxONE, IBM is seeking to repeat its long-term success with IBM Z. IBM is now seeking to expand the value and appeal of LinuxONE to a broad spectrum of clients, industries, geographies, and workloads – all with a common set of benefits, such as:

- Multitenant scalability that provides the ability to support diverse production and analytics workloads on the same machine sharing the same data
- Lower energy consumption and licensing costs with better performance and optimal security to enable consolidation of workloads on a smaller infrastructure footprint
- Trusted always-on data-serving platform availability on which firms can "bet their business," take full advantage of data, and provide more services to their customers

IBM could usefully 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 not only an enabling platform for one or two workloads but also a full package with industry-leading security, scalability, and performance capabilities. And it must move the discussion from LinuxONE being a platform for all workloads to LinuxONE being an unrivaled platform for single-source-of-truth data serving with the highest levels of security.

CONCLUSION

The choice of platform matters regardless of whether it is deployed on-premises or in the cloud. And 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. Finally, security must be pervasive (i.e., the entire system is fully protected) and with hardware partitions that are isolated from one another.

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