2020
IBM LinuxONE III
Business innovation driven by proven technology
Introduction

The world is changing, and businesses are relying on IT to meet the demands of this new environment. Solutions need to be delivered at a quick pace, with accuracy, while at the same time minimizing risk. What traditionally could have been done tomorrow, now needs to be done today.

As organizations reimagine the role of technology, the expectations of IT are shifting. Pressure for greater enterprise agility, innovation, and to do more with technology as product and value streams converge means organizations need to develop greater confidence in their technology investments.

At the same time, the agility of open source software is turbo charging this transformation. It’s also raising questions about how to enable this behavior while managing risk.

The pendulum is swinging towards privacy and protection of data. Deloitte is already seeing a focus on compliance to meet regulations and mandates from governments and regulatory bodies as organizations look to protect themselves from brand-impacting events and substantial fines.

The IBM® LinuxONE III is the latest iteration of IBM's Linux-only enterprise platform, which first hit the market five years ago. With a competitive total cost of ownership, organizations can address the requirements of today’s environment and achieve rock-solid flexibility with LinuxONE III.

For decades this technology has been enabling more than two-thirds of the Fortune 100 to protect their highly sensitive data on one of the world’s most secure platforms. Now it can support a multi-cloud environment and provide a mechanism for innovation, while securing the core.
Disrupting boundaries

One of the key challenges of innovation is managing the balance between enabling impactful innovation and control and security. This boundary has been dissolved by the IBM LinuxONE platform, which allows you to achieve both at scale.

Open source and innovation

Open source software remains an indispensable resource for enterprise-scale innovation. Forward-thinking companies are rebuilding their technology stacks, which include DevOps and NoOps concepts, autonmics, instrumentation, and cloud-native tooling.

Open source software is not new. It’s been 30 years in the making and its roots go back to the mid-1990s. The most notable creation from open source, the Linux operating system, powers more than 70 percent of the internet.

Linux has been running on the technology underpinning the LinuxONE platform for more than 20 years. IBM has been very active with the development of the LinuxONE platform features and has aligned them to the continuous delivery model being adopted across IBM’s products. This means features are enabled via updates and will likely happen quickly, in line with the open movement principles.

IBM is not alone, as others are also developing for the platform—which shows how this product is being generally adopted.

Combining the best of enterprise technology with open source innovation allows organizations to meet the challenges of innovating securely.

Delivering at scale

While innovating is a core component of business, being able to drive that innovation at scale, after ideation and an incubation period, is one of the top concerns of CIOs. Technology needs to be able to scale appropriately, sometimes with different methods and processes than have been in place before. But the constraints of a solution should not keep innovation from happening. As they’re developed, innovative solutions and ideas that need technology backing should also be able to scale quickly to ensure they are not held back or delayed.

The LinuxONE III enables organizations to deliver at scale. Delivered in an industry-standard 19-inch rack, the LinuxONE III provides configuration flexibility from one to four frames. An uplift of 25 percent more total system capacity than previous models, it comes with up to 190 configurable cores enabling it to scale to support thousands of servers in a single footprint.

Combining the best of both worlds

LinuxONE III combines proven security with open source technologies. This powerful combination scales quickly without jeopardizing security, thus providing organizations with the ability to deliver the rock-solid flexibility required when IT and the business combine.
A new era of Linux security

Today’s environment is one of heightened risk and prolonged uncertainty. Blurring the lines between business-as-usual risk management, crisis management, and resilience can enable agility in the face of an uncertain future. As can built-in functionality that allows applications to be deployed at the highest levels of security and reliability.

Security is complex, can be hard to deploy, and typically needs additional software, servers, and skills. LinuxONE III can give organizations peace of mind that the highest levels of security for their applications is in place, complying with regulations is simplified, and the auditors’ visits can be less stressful.

Complying with regulations is also becoming an increasingly complex, cross-functional effort and many CXOs are looking for opportunities to dramatically improve regulatory productivity. Yet organizations continue to struggle with securing people, getting executive buy-in, and identifying the technologies required to address compliance risks. This exposure can lead to very large financial impacts and huge brand reputation.

In addition, data breaches continue to hit the news. Driven by hackers and criminal insiders, data breaches can impact an organization for years to come and have a direct impact on the organization’s customers.

Using confidential computing and a deeper level of data encryption can help organizations address these issues.

---

**$392 million**

Average cost of a breach of more than 50 million records

**80%**

Share of breaches that included records containing customer personally identifiable information

Source: Cost of a Data Breach Report 2020, IBM Security
Deloitte IBM alliance | IBM LinuxONE III • Business innovation driven by proven technology

Confidential computing

Protecting your virtual servers

Government mandates and compliance regulations are changing and can be expensive to implement and maintain—and audit. But auditor visits are necessary and productive to ensure organizations are meeting these mandates.

Since 2018, cybersecurity incidents caused by insiders increased by 47 percent and the cost of insider threats rose by 31 percent. It is no longer the realm of outsiders trying to get data for criminal purposes. Internal threats exist, be it intentional or opportunistic.

Running mission critical workloads on Linux can now be protected and secured with the most reliable technology. New and built into the LinuxONE III is a Trusted Execution Environment which provides a method to fully isolate and protect a virtual machine.

In this environment, the applications and the servers they reside on are signed with cryptographic keys, preventing unwanted access. In addition, the secure boot feature means that protected servers cannot be started unless they are actually what you intended them to be. These features stop unwanted server configurations from being ghosted and potentially compromising your environment.

Protecting the application and sensitive data from internal and external threats is addressed. Infrastructure providers also cannot access your server. Malicious virtual machines in the same virtualization environment cannot access your data. And operations staff cannot see your application environment, even from another compromised virtual server.

Earlier LinuxONE models made this possible through the use of hardware partitioning (PR/SM). The LinuxONE III, which is also enabled at the KVM level, provides even greater scale in virtual server protection.

On top of this level of security, the cryptographic keys themselves are encrypted with a master key. As a result, no key is kept in the clear or able to be discovered in a system log trace or dump, compromising security.

The master keys are retained in a Hardware Security Module (HSM), which provides tamper proof hardware protection for your most important keys.

Deploy securely as part of your distributed cloud

With a secure container for your mission critical workload, you can now run applications across your distributed cloud, secure in the knowledge they are safe and running in the trusted environment you built.

You’ll find this confidential environment behind services in the cloud under IBM Hyper Protect and Blockchain services in the IBM Cloud. This enables you to securely manage these protected workloads across your distributed cloud. The “build once run anywhere” premise gives you the flexibility to move workloads between your cloud environments, or balance application workloads across a hybrid cloud, knowing it will not be compromised.
Encryption everywhere

It's all in the hardware

The addition of hardware encryption now available in LinuxONE III makes it cost effective and much simpler to protect your critical workloads. Previous options to achieve this level of encryption involved more software or hardware, significant integration efforts, and very specific solutions. The LinuxONE III enables this level of encryption through two features.

The CPACF feature is built into the technology and comes as standard. This provides chip-based acceleration for certain cryptographic algorithms. The speed of this feature allows for protected key encryption, where cryptographic keys can be wrapped in a special key to prevent unwanted disclosure of those keys.

Provided as an IBM Crypto Express Adapter, this add-on feature provides the functions of an HSM, which is tamper proof and can withstand physical and logical attacks, erasing the cryptographic keys if it senses an attack.

IBM Cloud Hyper Protect Crypto Services now takes this to the cloud, enabling you to manage your cloud keys on FIPS140-2 level 4 certified hardware.

Fiber Channel Endpoint Security ensures that data flowing on Fiber Channel Protocol (FCP) links between the LinuxONE III and data storage devices are encrypted and protected.
Your data travels—so give it a passport

Data is critical to your business but keeping it safe can be difficult and expensive to achieve. Enabled by the LinuxONE III, IBM Data Privacy Passports provide audit and encryption to protect data wherever it goes. At the same time, it gives full control over access to the data through a policy-based engine.

Through the use of a Passport Controller, you can not only protect data but also make the right data available at the right time to the right person. The protected data is encrypted to prevent unauthorized access.

Enforced data protection allows you to secure your data, while overcoming any operational constraints this typically imposes. For instance, you can mask certain parts of the data and make it available to only those who act in a role that is allowed to see that data. If you are not permitted to see that data, the data is masked from you, but operationally you can still perform your role.

The granularity of control means you no longer need to go through elaborate processes for creating test data, as you can test with real data which has automatically been made safe. With 90 percent of organizations admitting to experiencing disclosure of sensitive data in their test environments within the past year, this is a critically important feature.

It means you can keep your auditor happy, as encrypting all data is now possible. It also means you can stop access to data that may have left your systems by simply deleting the object encryption key—protecting data that could be taken by rogue parties.

The LinuxONE III platform makes this possible through the use of hardware-based encryption capabilities, performing the cryptographic operations at a speed that now makes this data protection capability a must have in today’s environment.

Enforced data scenario

Customer name masked from the Finance Department
Customer balance masked from the Customer Relations Department
Key management

Employing data protection mechanisms as previously described is only part of the picture. Regulations like GDPR, PCI-DSS, and HIPAA, to name a few, require specific key management processes to be created and well documented. In fact, how you manage your keys should be one of the first steps in defining a security protection policy.

The LinuxONE III platform comes with a number of key management solutions. These built-in tools enable you to provide the process and management steps required to meet the defined compliance requirements.

- IBM’s Security Key Lifecycle Manager (IKSLM), which can run on the LinuxONE III platform, provides a mechanism to manage operational cryptographic keys. This feature will take advantage of hardware acceleration.

- Trusted Key Entry (TKE) Workstation is an optional feature in the form of a stand-alone key management capability. It’s typically kept in a secure room where keys can be managed from a single point of control and provides a way to manage Master Keys in the Crypto Express Adapter for LinuxONE.
Cost optimization

Optimizing compute cost has always been at the forefront of technology considerations with many CIOs describing a significant gap between business leadership’s expectations of IT and corresponding financial support. Thus, cost management remains high on the agenda, and allowing for innovation while balancing this cost restraint can be an issue. LinuxONE III provides the means to reduce cost while enabling innovation.

Multi-faceted cost reduction

The IBM LinuxONE III provides mechanisms to realize high levels of cost savings. In an environment where software is licensed per processor, this enables you to potentially save on software licensing. So simply consolidating for licensing savings can make the business case alone.

A typical x86 server runs at between 10 and 20 percent utilization. This effectively means you could be paying for 80 to 90 percent that you don’t use. Due to the high average sustained CPU utilization of the platform, combined with the workload management capabilities and features, cost savings can be realized. For example, one organization achieved a 15:1 reduction in processor requirements resulting in significant cost savings.

It can be hard to get a like-for-like comparison of costs for footprint reduction or server sprawl, especially when the distributed environment cost may be spread across many cost centers. However, doing the legwork to understand the real picture may deliver savings. IBM has a LinuxONE cost calculator to help understand this at a high level.

It’s not unusual to see a data center full of servers as more are deployed. These consume space, facilities, and power. Through server consolidation, LinuxONE III can reduce these requirements. For example, one organization transitioned its environment and consolidated to LinuxONE, increasing transaction volumes four-fold and decreasing cost of ownership by 44 percent.

Moving to a hybrid cloud architecture model has the potential to reduce cloud data center facilities consumption. Consolidating servers can remove the need to build another data center or rent space in a co-lo, thus avoiding a costly expense.

“Not only have we been able to demonstrate cost savings, we have also helped clients achieve dramatic improvements in system performance.” - Bob Miller, Deloitte Consulting LLP
Achieving cybersecurity goals, cost effectively

The security provided by on-chip or specialized crypto adapters makes it more efficient to protect workloads and applications. Having data managed and masked across your enterprise is by no means a small task, especially if it encompasses multiple servers and technologies. LinuxONE III makes it simpler and more cost effective to achieve cybersecurity goals.

Having a consolidated architecture makes it simpler to manage. Common tools, easy-to-use technology, and a standardized approach means it can cost less to manage.

LinuxONE III makes the technology available to businesses of all sizes. It’s not only the big industrials that have access to solutions that can meet compliance or brand protection needs. For example, LinuxONE is being used to provide confidential computing environments to payment startups, effectively disrupting the payments industry. Another organization is using a secure IBM Blockchain environment as a competitive advantage to speed the process of tracking carbon-negative luxury goods.
Conclusion

LinuxONE III is a platform that fits into the requirements of the modern world. It meets the challenges of security and compliance that are top of the agenda for many organizations today. These features combine to provide a confidential compute environment.

At the same time, it brings together a flexible environment where innovation through open source can be combined with security. The result is a safe environment where businesses can move quickly to meet the challenges of the market.

The enhanced features of the LinuxONE III platform combined with an optimized cost model can help reduce costs. These savings can appear through server consolidation, data center facilities and space management, and reductions in software licensing, so it’s important to consider all elements of the technology environment when building a business case.

LinuxONE III is also bringing its features to a wider audience than previously imagined. Service providers can now use LinuxONE to differentiate their offerings and using the LinuxONE in a cloud model—private, hybrid, or public—makes these features available on a pay-as-you go structure.

It also provides an ideal platform for existing IBM Z customers looking to reduce costs by moving applications via a form of application refactoring, rewrite, or simple replacement. LinuxONE III provides the means of moving these applications to a new platform, while maintaining the highest levels of security and reliability.

LinuxONE III fundamentally changes what is possible and brings proven technology together with new functions and features that meet the immediate requirements of business today.
References


