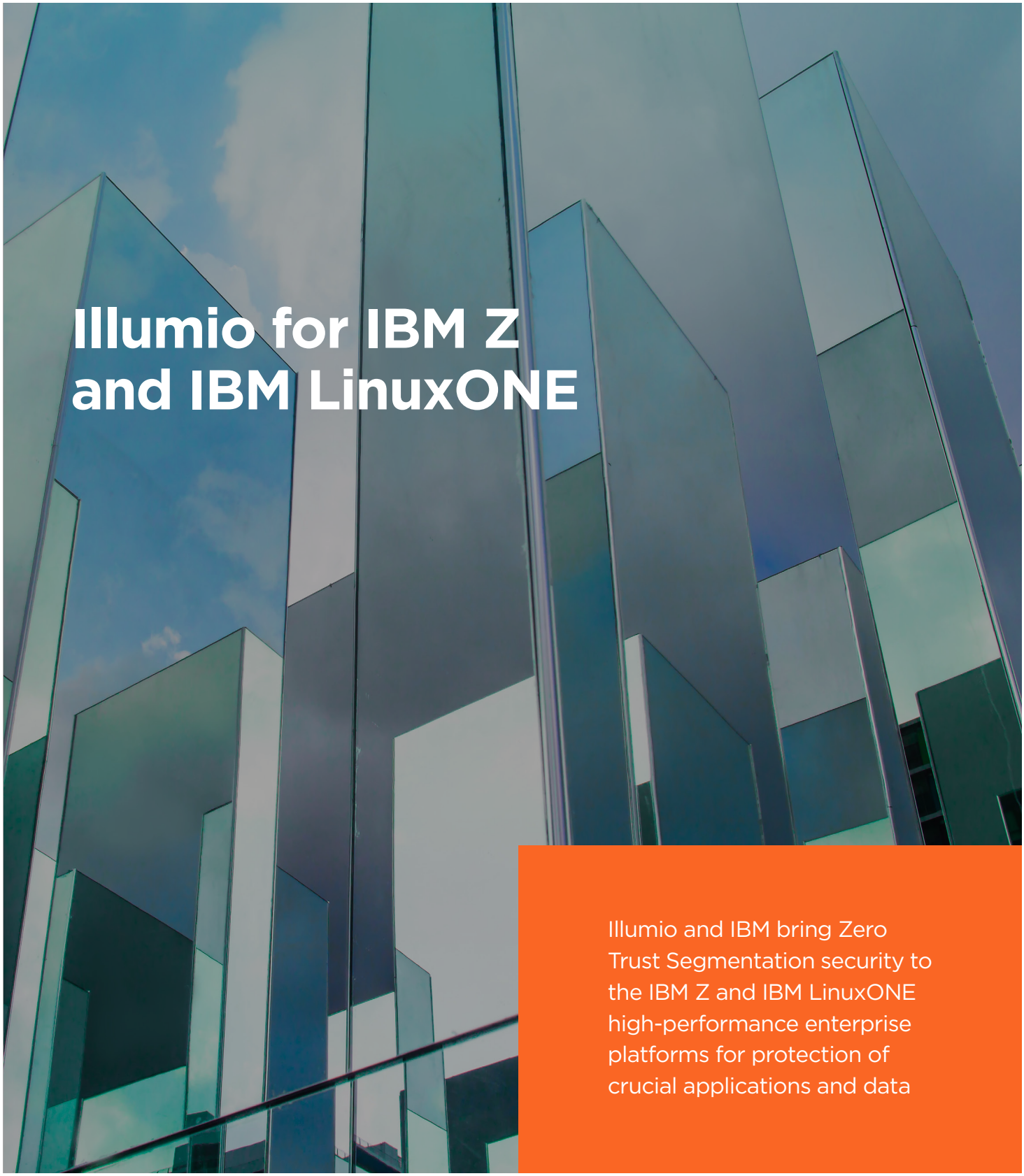
illumio

SOLUTION GUIDE



Illumio for IBM Z and IBM LinuxONE

Illumio and IBM bring Zero Trust Segmentation security to the IBM Z and IBM LinuxONE high-performance enterprise platforms for protection of crucial applications and data

illumio

SOLUTION GUIDE

The Critical Role of IBM Z and IBM LinuxONE

In the cloud era, reliable and secure servers such as IBM Z and IBM LinuxONE are more important than ever. That's because IBM Z powers many of the most critical digital systems for businesses and governments around the world.

Yet IBM Z and IBM LinuxONE servers must defend against new security threats as organizations build out their hybrid cloud environments to drive digital transformation. Attackers and malware can move laterally to access those servers from the cloud and PCs, as well as other hardware and services points.

The ability to keep these security threats from spreading is essential to protecting critical applications and data residing on IBM Z and IBM LinuxONE platforms.

But these new types of risks require new approaches to cybersecurity and additional layers of protection to ensure organizations remain safe.

Zero Trust Security for IBM Z and IBM LinuxONE

A new partnership between Illumio and IBM brings Zero Trust security to IBM Z and IBM LinuxONE — helping enterprises modernize and secure mission-critical workloads with robust application security capabilities.

IBM Z is known as the enterprise platform for mission-critical applications. It brings advanced levels of data privacy, security and resiliency to your hybrid cloud. And IBM LinuxONE combines the advantages of open source (Linux) with IBM Z's industry-leading innovations.

Now, by strengthening IBM Z and IBM LinuxONE security with Illumio Zero Trust Segmentation capabilities, organizations gain a ground-breaking approach to safeguarding their organizations.

Together, Illumio and IBM's security technologies address cyberthreats at both the hardware and software layers of the stack — offering organizations the defenses they need to ensure their mission-critical workloads and sensitive data are safe from cyberattacks.

Making Hybrid Cloud Environments Secure for Digital Transformation

With Illumio Core now available on IBM Z and IBM LinuxONE, organizations can address the need for hybrid cloud security controls in three important ways

See Risks

Get real-time visibility into application traffic, security policy, communication patterns and risk exposure across hybrid environments. Gain an instant understanding of your communication pathways down to the workload level. Easily integrate Illumio telemetry with SIEM and SOAR tools for security analysis and incident response.

Isolate Attacks

Assess and prioritize risks, automatically build and recommend rules, and apply Zero Trust policies for IBM Z and IBM LinuxONE. Quickly block common paths for ransomware. Easily ring-fence critical applications, separate development and production environments, insulate IT systems from OT/IoT devices, and segment core services.

Secure Data

Orchestrate and enforce security policies across IBM Z and IBM LinuxONE systems to mitigate exposure, lower operational costs and accelerate your path to Zero Trust security — all with no impact on computing performance. Quickly block ransomware and easily expand to segment additional applications, data center services and cloud platforms.

Illumio and IBM: Unified IT Infrastructure and Software Security for High-Performance Enterprise Platforms

When it comes to providing Zero Trust Segmentation for IBM Z and IBM LinuxONE enterprise platforms, Illumio is the pioneer and market leader with its intelligent visibility, radical simple policy creation engine, and automated segmentation and enforcement.

Illumio's product suite — purpose-built for Zero Trust security — makes it simple for organizations to segment traffic down to the workload level. Security teams can easily see communication flows and restrict or block sensitive or high-risk pathways.

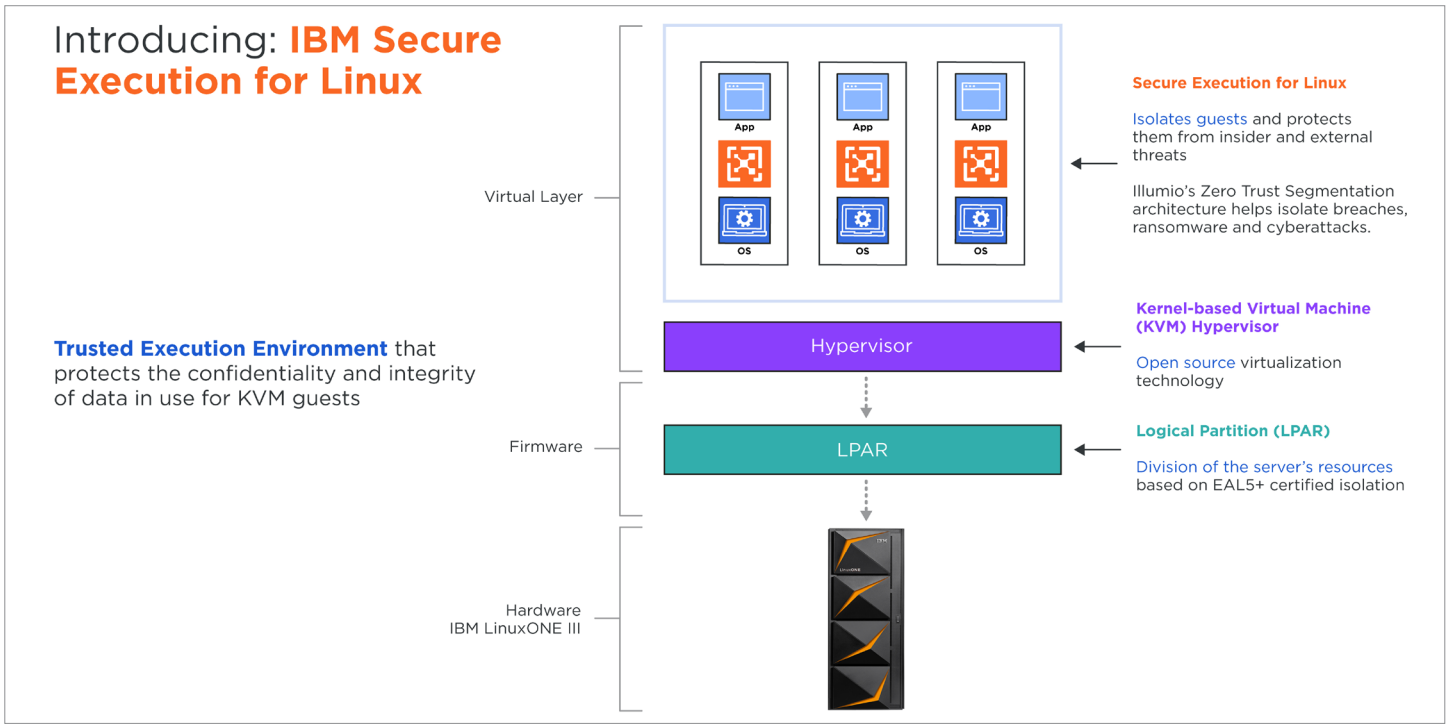
With Illumio, you gain:

- The ability to isolate critical assets to reduce the risk and minimize the impact of ransomware and cyberattacks.
- Comprehensive visibility into IBM Z and IBM LinuxONE in a single view, the same view as your overall IT infrastructure, whether public cloud, on-premises or hybrid cloud.
- Automated rules building and recommendations for optimal Zero Trust policies across all IBM Z and IBM LinuxONE environments.
- Assurance to safely program and orchestrate workload policies at scale.

And with IBM's built-in security features, you can pervasively encrypt transactions and data on IBM Z and IBM LinuxONE without impacting service level agreements (SLAs). You can also protect against both insider and outsider threats for high-volume transactional and data-serving workloads.

IBM Z and IBM LinuxONE offer a full set of native security capabilities, including:

- Integrated **FIPS 140-2 level 4 compliant hardware security module (HSM)** certified to the highest level of protection based on the U.S. Federal Information Processing Standard.
- Built-in trusted execution environments for **confidential computing** at scale.
- Industry-leading **crypto performance per core.**



Key Security Capabilities: IBM Z and IBM LinuxONE

IBM Secure Execution

IBM Secure Execution for Linux is a z/Architecture® security technology that is introduced with IBM z15 and IBM LinuxONE III. It protects workload data that run in a kernel-based virtual machine (KVM) guest from being inspected or modified by the server environment. No hardware administrator, no KVM code and no KVM administrator can access the data in a guest that was started as an IBM Secure Execution guest.

IBM Secure Execution for Linux is a continuation and expansion of well-known security features of IBM Z and IBM LinuxONE. It supplements pervasive encryption, which protects data at-rest and data in-flight, to also protect data-in-use. With IBM Secure Execution for Linux, you can securely deploy workloads in the cloud and protect workload data.

The IBM Secure Execution for Linux isolates workloads at scale and helps protect them from internal and external threats.

Built-in trusted execution environments for confidential computing

Confidential computing focuses on using technology to protect data-in-use. Secure Execution for Linux further supports confidential computing through the implementation of a trusted execution environment (TEE) on Linux on IBM Z platforms. With TEE technology, users can implement higher levels of trust, isolation and access control over their data assets compared to general-purpose software environments.

With more companies moving their on-premises workloads to public and private clouds, the need for a highly secure, multi-tenant hosting solution becomes necessary to ensure the confidentiality and integrity of each application and its data. Confidential computing provides:

- Enhanced security at enterprise scale by isolating workloads.
- Access limited to privileged insiders, such as Kubernetes and hypervisor administrators.
- Assurance of data confidentiality and integrity.

Integrated FIPS 140-2 level 4 compliant hardware security module (HSM)

The Federal Information Processing Standard Publication 140-2 is a U.S government computer security standard used to approve cryptographic modules. IBM LinuxONE and IBM Z Crypto Express HSMs are FIPS 140-2 level 4 certified. Security Level 4 provides the highest level of security.

At this security level, the physical security mechanisms provide a complete envelope of protection around the cryptographic module with the intent of detecting and responding to all unauthorized attempts at physical access. Penetration of the cryptographic module enclosure from any direction has a very high probability of being detected, resulting in the immediate deletion of all plain text critical security parameters (CSPs).

Industry-leading crypto performance per core

The IBM Z processor dedicates significant computing resources per core to cryptographic acceleration for Advanced Encryption Standard (AES), triple DES (TDES) and Data Encryption Standard (DES) encryption/decryption, Secure Hash Algorithm (SHA) and some PKCS #11 Public Key Algorithms. The latter helps IBM Z and IBM LinuxONE deliver industry-leading cryptographic performance at scale in support of a variety of use cases, such as payment systems, enterprise blockchain solutions, pervasive encryption of mission-critical data-serving and transactional workloads, and securing of digital asset custody solutions.

IBM Z and IBM LinuxONE also offer a protected-key facility. This unique feature supports high

performance and high security by wrapping AES and DES keys, which are held in the processor core, with a processor master key. This allows for acceleration of AES and DES operations while ensuring that the respective keys are never exposed or visible via the operating system storage.

The Ideal Combination for Modern Security

By combining the Zero Trust Segmentation capabilities of Illumio with the security capabilities of IBM Z and IBM LinuxONE, these enterprise platforms offer unprecedented security protection for modern enterprises.

With Illumio and IBM, you can rest assured that IBM Z and IBM LinuxONE enterprise platforms are fully protected to ensure your organization can thrive with confidence.

> "Illumio and IBM Z are upping the game on Zero Trust security by extending the protection surface with confidential computing to address a broad set of threats. This is a truly unique security offering for our mutual customers."
>
> **— Marcel Mitran, CTO for IBM LinuxONE**

Security for Critical Systems

Learn more about how Illumio is revolutionizing Zero Trust Segmentation. www.illumio.com

Explore more at the IBM Z and Cloud Modernization Center ibm.com/community/z-and-cloud/

About IBM

IBM is a leading global hybrid cloud, AI, and business services provider, helping clients in more than 175 countries capitalize on insights from their data, streamline business processes, reduce costs, and gain a competitive edge in their industries. IBM's breakthrough innovations in AI, quantum computing, industry-specific cloud solutions, and business services deliver open and flexible options to our clients. All of this is backed by IBM's legendary commitment to trust, transparency, responsibility, inclusivity and service.

For more information, visit www.ibm.com

About Illumio

illumio | IBM Business Partner

Illumio, the pioneer and market leader of Zero Trust segmentation, prevents breaches from becoming cyber disasters. Illumio protects critical applications and valuable digital assets with proven segmentation technology purpose-built for the Zero Trust security model. Illumio ransomware mitigation and segmentation solutions see risk, isolate attacks, and secure data across cloud-native apps, hybrid and multi-clouds, data centers, and endpoints, enabling the world's leading organizations to strengthen their cyber resiliency and reduce risk.