illumio

PARTNER BRIEF

Microsegmentation for Mainframe (IBM z/OS)

Secure your mainframe, contain breaches, and accelerate Zero Trust with Illumio and Kyndryl.

Perimeter security fails the mainframe

Most large enterprises run IBM z/OS mainframes at the center of their operations. These systems process billions of transactions every day. Uptime is measured in seconds, and failures cost real money.

As mainframes connect to cloud and distributed systems, perimeter-based security falls short. Today's attackers exploit that gap, using lateral movement, ransomware, and supply-chain techniques to reach core systems.

Compliance pressure is rising, too. Regulators want stronger segmentation and clearer proof of breach containment.

The mainframe needs Zero Trust

Mainframes are often treated as "secure by default." Teams focus elsewhere and leave the mainframe under-monitored and under-protected. Attackers count on that.

Most mainframe-related breaches start in cloud, web, or distributed environments, not the mainframe. Then, they move laterally into trusted core systems. Mainframe data is often the final target.

Penetration testing shows these risks are largely preventable. The gaps are in access control, segmentation, and visibility instead of the hardware itself.

That's why teams focused on cyber resilience are bringing Zero Trust security to their mainframe environments. This includes building explicit verification, least-privilege access, and an assume-breach mindset.

Key benefits

Discover traffic continuously

Find all application, user, and system interactions automatically. Know what's running and what's talking to what.

Get full traffic visibility

See flows across mainframe, distributed, and cloud workloads in one view. Spot gaps before attackers do.

Detect anomalies

Catch access paths that don't belong, such as a batch job calling a system it's never touched before.

See accurate dependency maps

Map CICS, batch, DB2, MQ, and external dependencies with precision. Know what each workload actually needs.

Enforce least-privilege access

Eliminate role sprawl. Define precise access policies and remove anything that isn't required.

Detect misused credentials

Catch credential abuse across applications before it reaches critical systems.

Build a Zero Trust foundation

Move from static rules to continuous verification, the building block of Zero Trust at the workload level.

The Kyndryl + Illumio difference

Illumio brings microsegmentation technology built for IBM z/OS. Kyndryl brings mainframe advisory, engineering, and managed security services.

Together, they give organizations the controls to contain lateral movement, enforce least-privilege communication, and shrink the blast radius around systems of record.

Kyndryl extends Illumio application dependency mapping to cover mainframe services. Security teams get one clear view of risk across the full enterprise, including cloud, distributed, and mainframe together.

The result is workload-level control aligned with Zero Trust and regulatory requirements — no mainframe downtime and no performance trade-offs.

Business outcomes

Adopting microsegmentation for the mainframe delivers measurable results across security, operations, and cost.

Reduce operational risk

Contain threats before they reach revenue-critical systems. Limit the blast radius of any breach, no matter where it starts.

Adopt Zero Trust faster

Extend Zero Trust across the full enterprise, including the mainframe. Build on a proven foundation that already meets regulatory expectations.

Build a stronger security posture

Improve your security posture without touching mainframe availability. No downtime and no performance trade-offs.

Lower change costs

Reduce the risk and cost of modernization. Clear dependency maps make it easier to move, update, or retire workloads safely.

Get flexible delivery

Choose the model that fits your team. Deploy through a traditional purchase or a fully managed service — Kyndryl can run it for you.

Get started now

Engage Kyndryl and Illumio to identify mainframe trust paths, apply microsegmentation controls around z/OS workloads, and build continuous risk reduction that protects your most critical transactions and data.

Start with a mainframe security assessment. Understand your current exposure. Then move from perimeter trust to workload-level control at your pace.

Ready to bring Zero Trust microsegmentation to your mainframe?

Email us at kyndryl@illumio.com.

About Illumio

Illumio is the leader in ransomware and breach containment, redefining how organizations contain cyberattacks and enable operational resilience. Powered by an AI security graph, our breach containment platform identifies and contains threats across hybrid multi-cloud environments — stopping the spread of attacks before they become disasters.

Recognized as a Leader in the Forrester Wave™ for Microsegmentation, Illumio enables Zero Trust, strengthening cyber resilience for the infrastructure, systems, and organizations that keep the world running.