ensono

Your Guide to Zero Trust Security for the Mainframe

Start your Mainframe-as-a-Service (MFaaS) journey with a security-first approach

Make better happen

ensono.com

Mainframe security isn't optional—it's essential

IBM recently reported that the global average cost of a data breach reached $4.4 million in 2025. However, the average cost was $10.22 million in the U.S.—a record high. Of the organizations that experienced a data breach, nearly all suffered operational disruption following the breach—and yet, only 49% of breached organizations plan to invest in security.

With the risk of security incidents increasing every day, securing your most critical data and applications has never been more important. On the mainframe—which houses many of these sensitive workloads—having the proper security measures in place protects against catastrophic breaches that could lead to significant financial, legal, and reputational damage.

Zero Trust: A strategic mindset

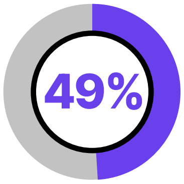
Never assume trust
Every access request must be verified.

Enforce least privilege
Users get only what they need.

Continuously validate
Monitor and audit everything.

$4.4 million
The average cost of a data breach globally

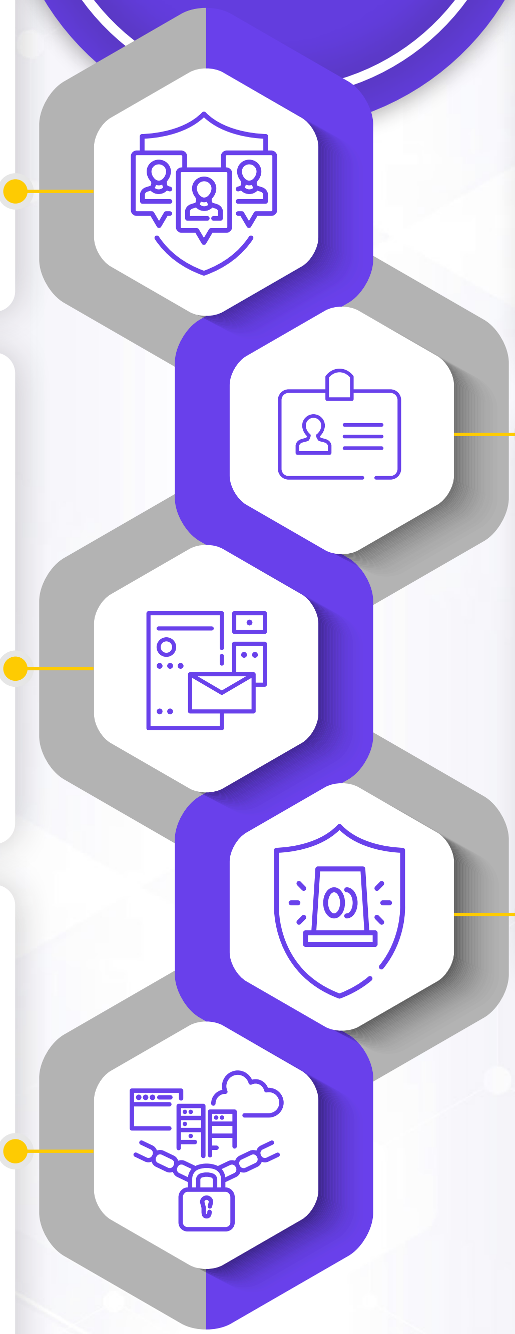
$10.22 million
The average cost of a data breach in the U.S.



Of breached organizations plan to invest in security

As in all IT environments, best-practice mainframe security starts with Zero Trust—a security framework that assumes threats could exist inside or outside the organization, therefore requiring a "never trust, always verify" principle. With this approach, security becomes a proactive foundation rather than a reactive fix—built-in and embedded from day one, not bolted-on afterward.

Key Enablers of Zero Trust Architecture



Role-based access management

- Controls, monitors, and secures access and permissions across an organization.
- Makes sure the right people access the right resources at the right time.
- Limits user access by implementing Just-In-Time Access—temporary, time-limited access—and Just-Enough-Access, granting the minimum level of access needed.
- Helps prevent unauthorized use and reduces the risk of security breaches.

Multi-factor authentication (MFA)

- Combines using a password, security token or mobile device, and biometrics.
- Verifies who accesses a system or application.
- Reduces the risk of unauthorized access to increase security by being phishing-resistant.
- Supports adaptive access policies based on risk signals and context.

Always-on audit readiness

- Makes sure the necessary processes, controls, and documentation are in place for an audit.
- Prepares systems and data for an audit without disrupting operations.
- Equips organizations to quickly provide evidence of compliance with standards and regulations.
- Enables proactive detection of compliance gaps through continuous monitoring and validation.

Identity and access management (IAM)

- Integrates threat intelligence, data access policies, and compliance systems.
- Authenticates and authorizes users based on dynamic, real-time data points rather than relying on static credentials or one-time verification.
- Supports continuous validation and auditability to detect anomalies and enforce compliance.
- Provides centralized visibility and control over user access, offering actionable insights into usage patterns and supports rapid threat detection and response.

Segmentation and blast radius reduction

- Segments access zones and isolates systems to contain threats.
- Enforces strong authentication and least-privilege access.
- Reduces breach impact by making sure compromised credentials alone can't grant access.
- Demonstrates access controls and continuous validation to support compliance and audit readiness.

Mainframes aren't immune to security incidents. Thinking proactively keeps them protected.

A Vault Analogy for Modern Security

Think of Ensono's MFaaS security environment like a high-security vault:

Data Security and Protection is the vault itself—an isolated and resilient space where your data is safe from threats and ready for a quick recovery after a disruption, such as a cyberattack, system failure, or natural disaster.

Safeguarded Copy is a modern data protection feature serving as your tamper-proof backup inside the vault, creating immutable, point-in-time copies of your data that can't be altered or deleted and is ready for recovery or forensic analysis in case of an attack. These copies can then be exported to another location or system, preserving their integrity—a process known as safeguarded export.

MFA is the key to the vault, controlling who gets in, when, and why.

Continuous Audit Readiness is the window inside the vault—showing proof of protection and compliance without opening the door.

Together, these elements form the foundation of a proactive Zero Trust security posture: never assume trust, always verify, and make sure security is proactive and designed for resilience. Even if attackers breach the perimeter, they can't compromise your core—offering you peace of mind in the face of growing cyber threats.

Ready to continue the conversation?
Contact Ensono to learn more.

Let's connect

ensono® Make better happen