IBM Z

# Built for the AI era: How IBM Z continuously reduces risk from frontier AI threats

Executive perspective for CIOs, CISOs, and business leaders

# Table of contents



# Executive summary

Frontier AI and agentic AI systems are fundamentally changing the landscape of cybersecurity detection and response. Attackers are abandoning human skills for AI speed, dramatically compressing the time between vulnerability discovery and exploitation, increasing the creativity of attacks, and creating new opportunities for compromise. For organizations, this makes it more critical than ever to continuously reduce risk while maintaining trust, resilience, and operational continuity.

IBM Z is already using frontier AI models to accelerate vulnerability discovery and remediation—discovering 2X the number of vulnerabilities that would have gone undetected in Q2 2026 vs Q1[1]. Over the same time frame, by using the same AI technology, IBM Z was also able to deliver 3X the number of remediations compared to the previous quarter, demonstrating a stronger security posture through faster risk identification and reduction[1].

The consequences of AI in cyberattacks are already visible in the global market as well. AI-driven attacks increased 56% over the past year and now add an average of $1 million to the cost of a breach. For business leaders, this creates a new imperative. IT security can no longer be viewed as a collection of software layered on top of the hardware. Organizations must move toward integrated architectures that deliver protection, governance, resilience, and recovery as a unified platform. Success will increasingly be measured not by whether attacks occur, but by how effectively organizations maintain trust, continuity, and business operations despite them.

This also requires modern security practices. Organizations must continuously validate applications through automated testing, modernize DevSecOps workflows, and keep software and and security controls current to reduce exposure as AI accelerates the pace of vulnerability discovery.

Leaders are increasingly relying on frameworks such as the NIST Cybersecurity Framework to guide their response. IBM Z Security aligns naturally with this framework by integrating governance, protection, detection, response, and recovery into the platform itself, helping organizations strengthen trust, resilience, and operational continuity in the AI era.

For decades, IBM has recognized that security cannot be an afterthought. Beginning with System Integrity in 1973, IBM has continuously evolved its security practices to address emerging threats. Security has always been a constant investment across the IBM Z platform with frameworks such as the Secure Engineering Framework (2010) and Security and Privacy by Design (2019). IBM's decades long commitment to security provides the foundation to innovate and address the advancements of Frontier AI, while globally recognized certifications and independent validation demonstrate that trust in practice.

IBM Z processes billions of transactions that cannot fail for the world's most important systems and data. Reacting to security threats has never been enough for these workloads, and Z Security has always been built with a forward-leaning posture on security scanning, detection, and remediation.

Built on decades of security-by-design innovation, IBM z17 extends this foundation with AI-driven protection, automated cyber resilience, and quantum-safe readiness to address the next evolution of enterprise threats. With capabilities such as automatic suspension of malicious actors and instant detection and freezing of cyber threats, IBM z17 and its rich IBM zSecure portfolio, provide enterprises with a powerful blueprint for leading rather than reacting to the next generation of cyber threats.

# Why now?

AI-driven attacks increased 56% in the past year and now add an average of $1 million to breach costs.[1]

In response, 85% of breached organizations plan to increase security spending because of emerging frontier AI threats.[1] The shift to AI-speed cybersecurity is already underway.

# Strategic security requirements from frontier threats

The cybersecurity landscape is undergoing its most significant transformation in decades. Frontier AI models are demonstrating unprecedented capabilities in software analysis, vulnerability discovery, and attack path identification. Both defenders and adversaries now have access to AI-enhanced capabilities, but attackers often benefit from speed and asymmetry.

The emergence of Frontier AI systems, such as Mythos in the past year, transformed autonomous AI attacks from a theoretical risk into an immediate security challenge by dramatically accelerating the path from vulnerability discovery to exploitation. AI-driven attacks increased 56% year-over-year, as organizations continue to struggle with breach response times that average 247 days from identification through containment. As attackers gain AI speed capabilities, the cost of delayed detection, investigation, and remediation continues to rise.

This shift elevates three strategic priorities for enterprise leaders:

- **Security operations must operate at AI speed**
  Continuous monitoring, automated detection, AI-assisted analysis, and accelerated response are becoming prerequisites rather than differentiators. Organizations that cannot respond at AI speed increasingly face a growing disadvantage against AI-enabled adversaries.

- **Trust must be established through governance**
  As AI gains access to enterprise data, applications, and workflows, identity, authorization, auditability, and policy enforcement become increasingly important. Governance is becoming a foundational requirement for both cybersecurity and AI adoption.

- **Resilience must be engineered into the operating model**
  The focus is evolving from preventing every attack to minimizing business impact and maintaining continuity when incidents occur. Cyber resilience is becoming a core business capability.

Many existing security architectures were not designed for this environment. Increasingly, organizations are moving from security as an overlay toward security as an architectural discipline.

# Why IBM z17 is built to meet this moment

## Security is architected into the platform and validated

Most security architectures are built by layering controls around infrastructure. IBM z17 takes a fundamentally different approach that anticipates security challenges rather than reacting to them. The AI era is increasing the value of trusted systems.

Security, resilience, governance, and recovery are engineered directly into the platform. From hardware-rooted trust and post-quantum cryptography to identity management, cyber resilience, and recovery, IBM z17 integrates security throughout the stack. The result is a trusted foundation designed to protect critical applications while reducing complexity.

Furthermore, IBM embraces a philosophy that brings together both product engineering and operational security practices. Security is embedded throughout the development lifecycle, supported by secure engineering disciplines, centralized vulnerability management, automated testing, and additional AI-assisted analysis and remediation. IBM also helps organizations operationalize these same principles through modern DevSecOps practices, enabling continuous validation of applications and helping teams keep software and security controls current as threats evolve. Rather than relying on any single technology or detection method, IBM's approach is designed to incorporate advances in vulnerability discovery and remediation regardless of their source.

Perhaps most importantly, IBM Z security capabilities are not based solely on vendor assertions. They are supported by extensive independent validation through globally recognized certification programs. IBM Z has achieved certifications across Common Criteria, FIPS, PCI HSM, NIAP, and other industry standards, providing third-party assurance that critical security controls have undergone rigorous evaluation.

IBM Z's certification strategy covers the integrated platform making it unique in the industry—the HSM is certified working with the OS, the hypervisor is certified with the partitioning hardware, the access control layer is certified with the OS it runs in. There are no uncertified seams between layers. This is an engineering achievement as much as a compliance achievement.

Certifications matter when addressing key business challenges including:

- Are we protected against a crypto breach or key theft?
- If we run multiple clients on shared infrastructure, are they truly isolated?
- Can we prove access controls to auditors and regulators?
- Are we ready for quantum computing threats to our encryption?

With IBM z17 and its architected platform approach to security, the certifications help validate those answers. This commitment to independent verification reflects a simple principle: trust should not have to be assumed. It should be demonstrated.

# IBM’s full stack approach to security through IBM Z software

## IBM’s full stack approach to security through IBM Z software

The IBM Z Security software portfolio extends the platform’s built-in security foundation through integrated capabilities designed to help organizations establish trust, accelerate response, and strengthen resilience in the AI era.

While IBM Z plays a unique role in protecting mission-critical applications, it is not intended to operate in isolation. With the IBM zSecure portfolio, you can integrate with broader enterprise security, risk management, compliance, and cyber resilience strategies, helping organizations establish a consistent foundation of trust across hybrid environments.

## Protect trust

IBM Z combines centralized identity governance, multifactor authentication, secrets management, certificate lifecycle management, pervasive encryption, and enterprise cryptographic services to help organizations strengthen access controls, protect sensitive data, and advance Zero Trust principles across critical workloads.

These capabilities help address several of the most common contributors to breach costs, including excessive privileges, poor role management, mismanaged secrets, and weak cryptographic controls. Identity and access management, key lifecycle management, and encryption were identified among the strongest factors associated with lower breach costs in IBM’s Cost of a Data Breach research.

## Accelerate detection and response

AI-driven threats require faster detection and response. Behavioral analytics, anomaly detection, privileged activity monitoring, security automation, compliance validation, and integration with enterprise SOC and SIEM workflows help organizations improve visibility, accelerate investigations,and support earlier threat containment.

The portfolio increasingly supports AI-speed security operations through AI-assisted analytics and automation. This is becoming critical as AI-driven attacks compress attack timelines from weeks to days. Organizations extensively using AI and automation reduced breach costs by an average of $1.93 million and shortened breach lifecycles by 65 days.[1]

## Enable cyber resilience

Cyber resilience remains one of IBM Z’s most significant differentiators. Capabilities such as IBM Z Cyber Vault, integrity validation, safeguarded recovery technologies, and coordinated recovery processes help organizations establish trusted recovery points, validate system integrity, and restore critical business services rapidly following disruptive events.

This capability is increasingly important because detection, escalation, and lost business costs now account for nearly two-thirds of total breach costs. Cyber resilience technologies help organizations reduce the operational and financial consequences of incidents by enabling trusted recovery and maintaining operational continuity.

## Security as a business resilience strategy

The NIST Cybersecurity Framework has become one of the most widely adopted approaches because it focuses on outcomes rather than technologies. IBM Z aligns naturally with this framework by integrating governance, protection, detection, response, and recovery into a cohesive architecture designed to support operational continuity.

Here are a few examples of how IBM Z helps businesses align their security posture with the NIST Cybersecurity Framework:

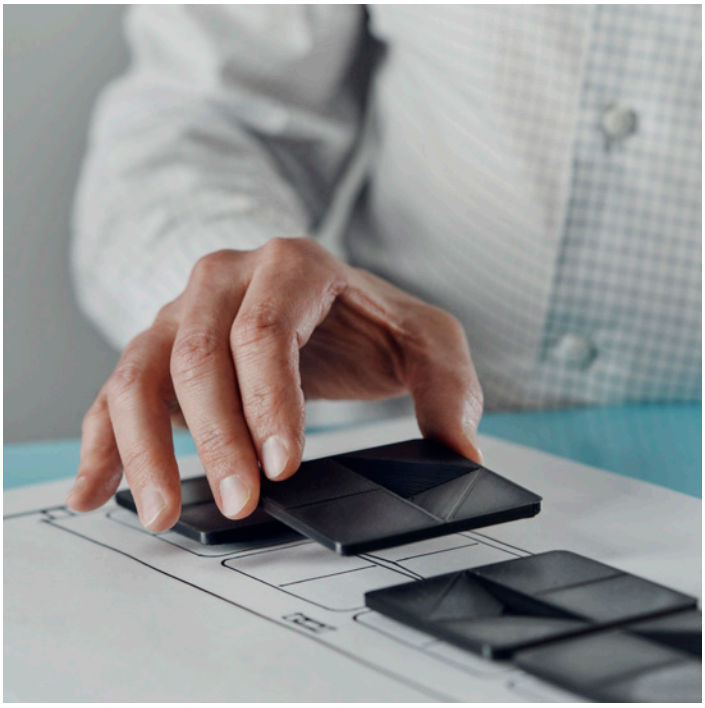
- **Identify—discover sensitive data and cryptographic posture across IBM Z**
  Reduce security blind spots by continuously discovering sensitive data, critical assets, and cryptographic exposures, enabling organizations to understand and prioritize cyber risk before it can be exploited.

- **Protect—remove the human reaction-time weak link**
  By automating defensive actions, IBM Z security software removes the delays inherent in human decision-making and manual intervention. This proactive protection capability significantly reduces the risk that attackers can exploit the critical period between detection and response, helping safeguard sensitive workloads, applications, and data from additional harm.

- **Detect—catch ransomware before it can do damage**
  Advanced behavioral analytics and early-warning capabilities enable IBM Z security software to detect ransomware in its earliest stages, before encryption, data destruction, or business disruption can occur. By proactively identifying suspicious activity and attack vectors that traditional z/OS security controls may miss, organizations gain earlier visibility into threats and the opportunity to stop them before damage is done.

- **Respond—freeze attackers in real time**
  IBM Z security software combines instantaneous threat detection with the ability to automatically freeze attackers in their tracks, delivering a uniquely powerful response capability. Rather than simply generating an alert, the platform takes immediate action to contain malicious activity, dramatically reducing attacker dwell time and limiting the opportunity for further compromise—an industry-first capability for mainframe environments.

- **Recover—rapidly restore trusted operations**
  Maintain trusted, tamper-resistant recovery copies of critical data so organizations can rapidly restore operations after ransomware, minimizing disruption and reducing the cost of recovery efforts.



And finally, IBM helps businesses to **Govern** cyber risk throughout the platform to Demonstrate compliance and provide continuous evidence of security and resilience to auditors, regulators, and boards.

As a result, these cybersecurity solutions influence business outcomes including operational continuity, client trust, regulatory readiness, protection of sensitive data, financial resilience, and innovation capacity.

## How the IBM Z security portfolio enables clients to meet the NIST Cybersecurity Framework

| NIST function | IBM Z outcome |
|---|---|
| Identify | Visibility into sensitive data and cryptographic posture across IBM Z. |
| Protect | Proactive protection capabilities to replace human reaction-time. |
| Detect | Catching ransomware before it can do significant organizational damage. |
| Respond | Freezing attackers in real time. |
| Recover | Rapidly restoring trusted operations across the business. |

Continuous governance & risk reduction across mission-critical environments.

# The mainframe advantage

As cyber threats evolve from human speed to AI speed, can your business continue to operate when disruption occurs?

The mainframe advantage is not a single security capability, product, or control. It is the ability to integrate governance, protection, detection, response, recovery, and resilience into a single operational architecture. IBM Z embeds trust directly into the platform through security-by- design engineering, integrated cryptography, identity governance, compliance automation, cyber resilience technologies, and recovery capabilities that work together as a coordinated system

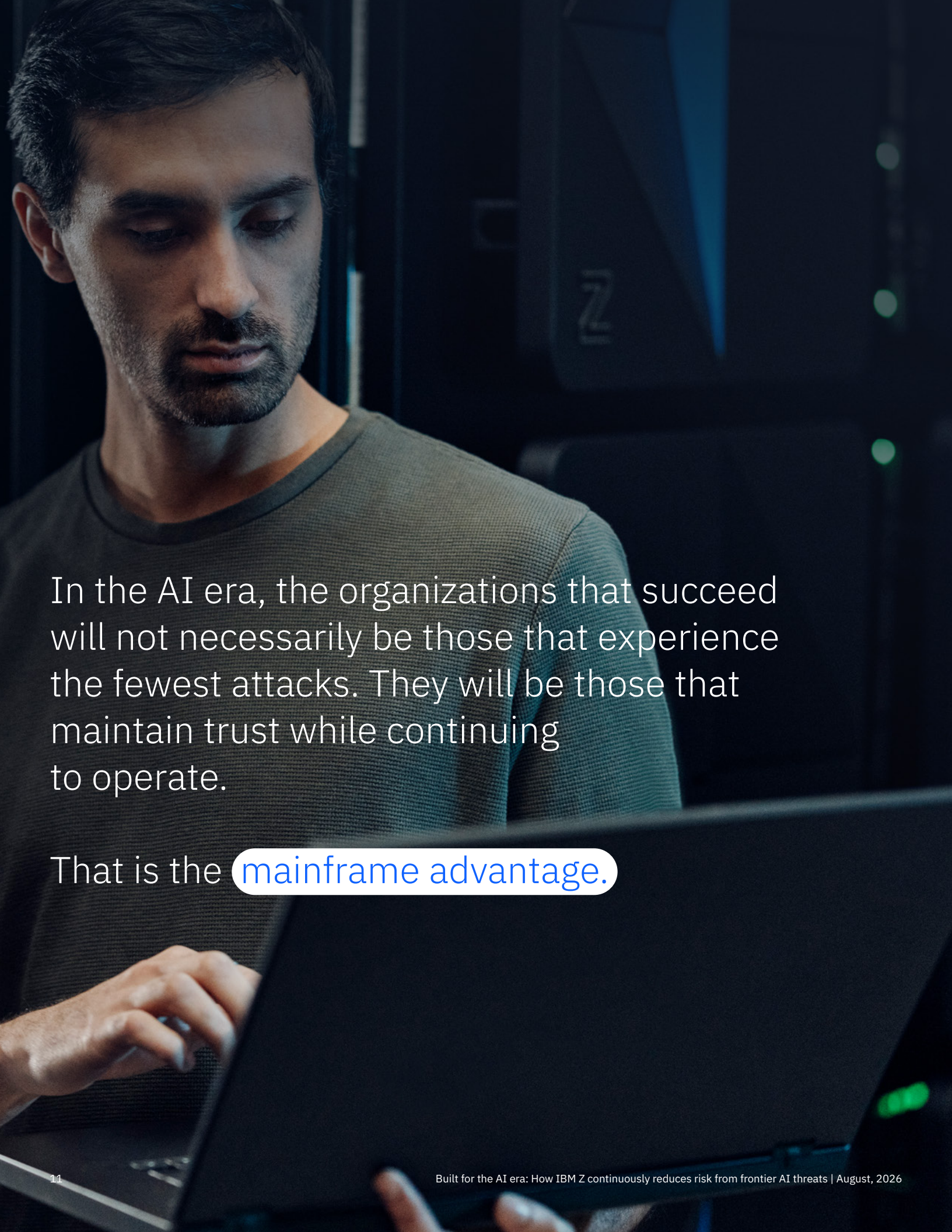
This integrated approach enables organizations to detect threats in real time, automatically contain malicious activity in seconds rather than hours or days, identify ransomware before it propagates across the environment, and reduce reliance on human reaction times through AI- powered response capabilities.

**For business leaders, this approach translates into tangible outcomes:**

- Maintain operational continuity during cyber incidents by detecting and freezing threats in seconds.
- Strengthen client trust and confidence by demonstrating the ability to contain cyber-attacks in real time.
- Improve regulatory readiness and audit performance with continuous oversight and automated incident response.
- Reduce the business impact of disruptions by stopping attackers before damage escalates with proactive security measures.
- Protect critical data, transactions, and digital assets by catching ransomware and insider threats before they spread.
- Support innovation while managing risk using AI-powered security that removes the weak link of human reaction time.

As AI accelerates both innovation and cyber risk, resilience is becoming a core business capability. This is particularly important for organizations operating critical financial, healthcare, government, and infrastructure services, where AI-driven attacks increasingly concentrate and where disruption can have systemic consequences beyond a single organization.

Customers will expect it. Regulators will increasingly require it. Boards will prioritize it.


In the AI era, the organizations that succeed will not necessarily be those that experience the fewest attacks. They will be those that maintain trust while continuing to operate.
That is the mainframe advantage.

# Getting started

## Accelerate readiness for the AI era

The transition to AI-speed cybersecurity is already underway. Organizations that wait for a major incident before modernizing their security architecture may find that the economics of cyber risk have shifted faster than their defenses.

The question is no longer whether AI will transform cybersecurity.

The question is whether organizations are prepared to operate securely and resiliently in that new reality.

## Executive leaders should consider:

- Can the organization sustain critical business operations during a significant cyber disruption?
- Are resilience and recovery treated as strategic business capabilities?
- Does the current security architecture provide the trusted foundation required for AI-driven innovation?
- Can the organization continuously demonstrate governance, compliance, and audit readiness?
- Are identity, cryptographic, and data protection controls aligned with future requirements, including AI governance and post-quantum security?
- Are automated testing and software currency built into your security processes?
- How effectively can the organization maintain client trust, regulatory confidence, and operational continuity during a cyber event?
- Is security embedded into the architecture—or layered on top of it?

## To accelerate readiness for the AI era, IBM has provided two offers:

1. The **Cyber Security Posture Assessment on IBM Z** can help organizations evaluate their current posture, identify gaps, assess resilience, and develop a roadmap toward a more integrated and resilient security architecture.

2. The **z17 Security Advantage** that combines our most advanced, secure, and AI-ready **IBM z17** with **IBM zSecure Detection** to establish a trusted foundation for enterprise security.

Because in the AI era, cybersecurity is no longer simply about preventing attacks. It is about enabling trusted innovation, preserving confidence, sustaining operations, and ensuring that the business can continue to run securely—even under adverse conditions.

**The future belongs to organizations that can innovate with confidence, operate with resilience, and maintain trust in an increasingly complex AI world.**

Contact your IBM representative to learn more or visit us at: ibm.com/products/z/security-software

1. IBM, 2026 Cost of a Data Breach Report, 2026