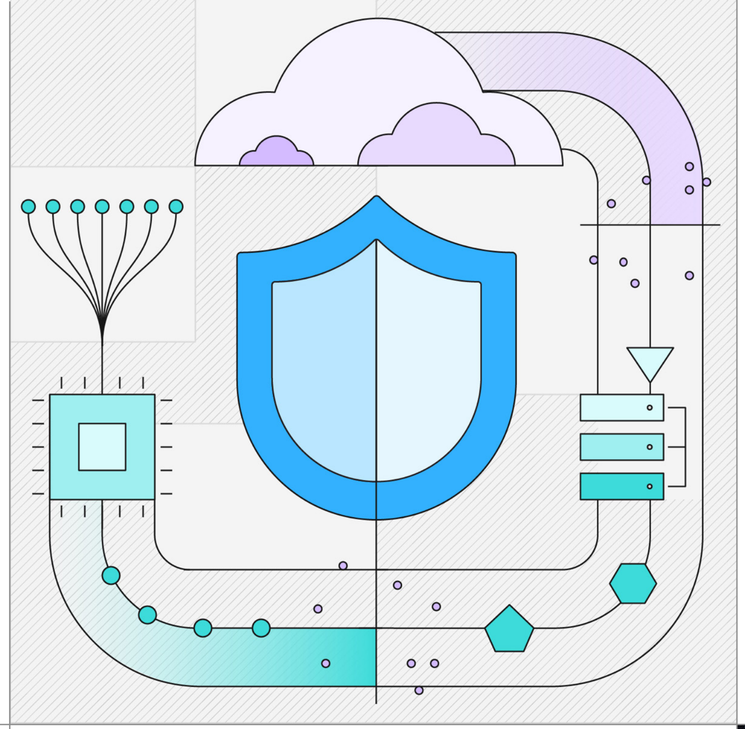
The Cyber Resilience Playbook for Modern Infrastructure



A decision-maker’s guide for strategies and checkpoints

01

Executive summary

Cyberattacks are intensifying across every industry, driving operational, financial and reputational risk. In 2025, the global average cost of a data breach was **USD 4.44 million**, while US-based organizations spent a record-high average of USD **10.22 million per incident**, and nearly **49% of breached organizations plan to increase security spending**.[1]

Yet many enterprises still rely on fragmented controls rather than a unified strategy that can withstand today's evolving threats. Traditional cybersecurity alone cannot keep pace with attacks that exploit human and system weaknesses.

Cyber resilience—the ability to prevent, withstand and recover from incidents—must be enterprise-wide and executive-led, blending governance and risk management with tested incident response and verifiable recovery to ensure continuity under stress.

This playbook outlines what a future-ready, AI-driven cyber resilience strategy looks like, from foundational organizational practices to the IT capabilities required to protect critical data and maintain continuity.

You'll also learn how AI is reshaping detection, prediction and response, helping businesses reduce impact and recover faster.

02

The new reality for infrastructure leaders

Cyberthreats are escalating across every industry—from healthcare to finance to government. These attacks carry severe consequences for organizations, including reputational damage, loss of customer data and regulatory fines.

New regulations, such as the Digital Operational Resilience Act (DORA), NIS2, HIPAA and other global mandates require businesses to demonstrate stronger, integrated cyber resilience capabilities. **Compliance is not optional.**

Businesses that fail to meet these regulations face financial and reputational risks, as well as prolonged downtime and slow recovery.

To withstand today's evolving cyberthreats, infrastructure leaders must move beyond traditional defense methods and adopt a unified, end-to-end strategy that combines governance, automation and AI-driven detection and recovery.

Three realities frame today's decision-making:

01

Your last line of defense is now the first point of attack.

More than 90% of surveyed organizations have experienced malware attacks.[2] In roughly half of those incidents, attackers attempted to destroy or disable backup and recovery capabilities. More than half of those attempts succeeded, increasing the likelihood of ransom payment and prolonged recovery.

02

Unplanned outages from outdated storage can cost millions.

Independent ITIC research found that for over 90% of surveyed mid-size and large enterprises, a single hour of downtime exceeds USD 300,000, with many reporting USD 1 million or more per hour—exclusive of litigation or penalties.[3]

03

In a race for innovation, standing still means falling behind.

Cross-industry survey data indicates that 90% of surveyed organizations struggle to adapt quickly to market changes, while only 10% can pivot effectively.[4] Infrastructure strategies that hardwire adaptability—automation, intent-aware controls and AI-assisted operations—help leaders absorb shocks and keep outcomes on track.

03

Requirements for resilience readiness

Cyberthreats, rising costs and compliance demands put pressure on every organization. To stay resilient, an effective modern infrastructure must meet the following requirements:

- Possess the capabilities to decrease recovery time
- Improve visibility across hybrid environments
- Reduce total cost of ownership (TCO)
- Strengthen compliance
- Stay ahead of increasingly sophisticated attacks

Recognizing these requirements—and why they matter—will help decision makers evaluate whether their IT infrastructure can truly withstand today's cyberthreats and adapt quickly enough to protect business-critical operations.

Downtime risk and slow recovery

Requirements

Modern resilience depends on having immutable, securely isolated copies of critical data, paired with real time anomaly detection that identifies corruption the moment it appears. Automated or semi-automated recovery workflows reduce manual intervention and ensure organizations can restore operations quickly and cleanly.

Why it matters

These capabilities dramatically reduce the time it takes to identify, contain and recover from an incident. Operations can be restored in mere minutes, preventing costly business interruptions with minimal manual intervention, while still maintaining human oversight.

Best practices

- Test recovery plans using isolated environments at regular intervals.
- Automate integrity checks for all immutable recovery points.
- Define clear time to recover (TTR) objectives aligned to business impact.
- Maintain and periodically update response playbooks based on real world exercises.

Fragmented security across hybrid environments

Requirements

Hybrid environments require consistent, unified security and data protection controls regardless of where workloads reside. Organizations need zero-trust aligned safeguards, encryption across data paths and continuous AI-assisted monitoring to catch anomalies in real time.

Why it matters

Consistent data protection controls reduce gaps created by hybrid complexity, helping teams detect threats earlier, respond faster and maintain a unified security posture regardless of where data resides.

Best practices

- Standardize controls and policies across all data locations.
- Continuously monitor workload behavior for suspicious activity.
- Regularly validate segmentation and zero-trust configurations.
- Create cross-platform dashboards for unified visibility and governance.

Rising operational costs and complexity

Requirements

Managing growing environments requires automation that reduces routine administrative work while keeping performance stable. Organizations also need predictive analytics to flag capacity or performance issues early, along with consolidated management to eliminate tool sprawl. Efficient data placement capabilities further ensure workloads run on the most cost-effective resources without sacrificing performance.

Why it matters

Modern operations require adaptability at scale. Automated optimization reduces overhead, lowers TCO and eliminates the complexity of managing multiple, siloed environments—all without costly rip-and-replace disruptions.

Best practices

- Use predictive insights to proactively rebalance workloads.
- Consolidate storage and data management under unified control planes.
- Automate routine health checks and performance tuning.
- Review cost optimization opportunities quarterly.

Regulatory and compliance pressure

Requirements

Organizations need built-in, continuous monitoring to ensure compliance controls remain active and up to date, along with audit-ready logging, reporting and verifiable replication that can demonstrate adherence at any moment. They also require isolated recovery environments that protect data integrity during restoration, supported by automated mechanisms that align policies with evolving regulatory frameworks and mandates.

Why it matters

Regulations like DORA, NIS2 and HIPAA require organizations to meet strict, resource-intensive mandates. Automated, verifiable compliance reduces audit fatigue, minimizes the risk of fines and enables enterprises to operate confidently knowing their recovery processes will meet regulatory requirements.

Best practices

- Conduct periodic compliance reviews tied to evolving mandates.
- Automate logging and reporting to ensure audit readiness.
- Isolate recovery environments for secure, clean restoration.
- Validate compliance controls whenever infrastructure changes occur.

AI-driven cyber threats

Requirements

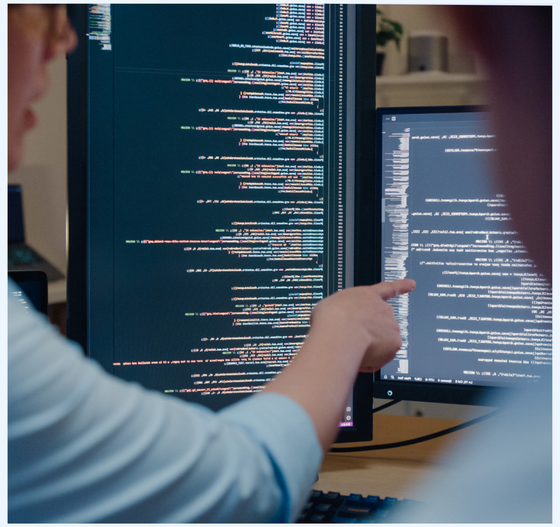
Organizations need AI-enabled detection systems that can identify advanced attack patterns, supported by real-time monitoring that spots unusual data behavior early. They also require automated environment isolation and rapid recovery capabilities to limit the spread of corruption. Additionally, they need predictive threat modeling tools that can help them stay ahead of evolving ransomware and AI-driven attacks.

Why it matters

AI-powered cyberattacks are growing, with breach costs averaging USD 4.4 million. These cyberthreats occur too quickly for traditional defense tools. Prevention, detection and recovery now depend on intelligent systems that can act in seconds rather than hours—reducing incident costs and limiting the impact of sophisticated cyberattacks.

Best practices

- Deploy anomaly detection models that continuously learn from data behavior.
- Automate isolation of suspicious workloads.
- Review threat intelligence inputs to refine predictive models.
- Integrate AI driven alerts into existing response workflows and playbooks.



04

Building an end-to-end cyber resilience strategy

Modern enterprises face a level of cyber and operational risk that traditional, perimeter-focused security models can no longer contain. Organizations often have *some* resilience capabilities in place. However, most still lack a unified, end-to-end strategy that integrates processes, governance, data management and infrastructure in a way that can withstand today's rapidly evolving threat landscape.

This section outlines what a modern, 2026 ready cyber resilience strategy looks like—one that combines organizational readiness, storage layer resilience and AI-driven capabilities to protect critical data, maintain continuity and recover with confidence.

The five pillars of a comprehensive resilience strategy

01

Establish foundational security and data ownership.

Organizations must ensure clear accountability for data protection, governance, and security practices—across IT, security and business stakeholders.

Best practices:

- Assign cross-functional ownership across IT, storage and security teams.
- Define governance policies aligned to industry and regional regulations.
- Review roles and responsibilities annually or after major architecture changes.
- Ensure visibility into data flows, workloads and dependencies.

02

Classify data and define minimum viable operations.

Not all data is created equal, and not everything requires the same level of protection. Leaders must identify what is essential to keep the business running, then architect recovery workflows around those critical assets.

Best practices:

- Classify data by importance (crown jewels → essential → non critical).
- Define the Minimum Viable Operations (MVO) required to keep the lights on.
- Align storage and recovery capabilities to data criticality.
- Balance protection depth with cost by applying stronger safeguards only where necessary.

03

Implement resilient protection and isolation mechanisms.

Modern resilience requires protection mechanisms that prevent corruption from spreading and preserve clean recovery points.

Best practices:

- Use immutable and isolated copies for critical data.
- Apply logical or operational air-gapping based on data sensitivity.
- Isolate recovery environments for safe validation before restoration.
- Automate snapshot schedules aligned to criticality and change rates.

04

Detect anomalies in real time using AI and behavioral indicators.

Threats evolve too rapidly for manual detection. AI-driven anomaly detection systems identify unusual behavior such as encrypted payloads, compression changes or abnormal Input/Output (IO) patterns—all within seconds.

Best practices:

- Deploy behavioral analytics that monitor changes in IO patterns.
- Use AI models that continuously learn from new telemetry.
- Integrate detection alerts into Security Information and Event Management (SIEM) and Security Orchestration, Automation and Response (SOAR) workflows.
- Treat detection as a continuous, real-time monitoring function—not a periodic task.

05

Orchestrate automated, validated recovery workflows.

Fast recovery requires both clean data and automated processes that bring systems back online quickly and consistently.

Best practices:

- Validate restore points in isolated workbench environments.
- Automate recovery playbooks linked to detection events.
- Compile related applications and data into recovery groups.
- Test recovery workflows regularly and refine based on findings.

How AI strengthens every step of resilience

As AI constantly evolves, it’s reshaping the resilience lifecycle by detecting anomalies faster, predicting issues before they impact operations and strengthening recovery accuracy.

Key enhancements include:

- Detecting anomalies in seconds rather than hours
- Predicting issues before they corrupt backups
- Improving model accuracy by 98%
- Identifying early signs of exfiltration

05

IBM FlashSystem: Protect • Adapt • Perform

Modern infrastructure leaders need technologies that can support the cyber resilience strategy outlined in the previous section—protecting critical data, detecting anomalies in real time, isolating threats quickly and enabling fast, verified recovery.

The following capabilities of the IBM FlashSystem® storage solutions directly align with the requirements previously listed and can help transform your storage from a passive repository into an intelligent, autonomous system. With AI-driven intelligence and advanced capacity powered by our high-performance IBM FlashCore® Module, you gain the speed, resilience and adaptability needed to meet rising performance demands, overcome skills gaps and stay ahead of compliance challenges—all without the unwanted complexity.

FlashSystem.ai: Intelligence that solves modern business challenges

FlashSystem.ai turns complexity into clarity with AI-driven automation that addresses today's biggest storage challenges: cost, risk, compliance and agility.

Human-AI collaboration

Accelerate decision-making with conversational-driven AI.

- FlashSystem.ai helps transform storage into an intelligent, autonomous system that listens, learns and acts with precision.
- AI agents explain decisions, suggest performance improvements and learn from user feedback—reducing manual effort and aligning storage with business goals.

Proactive optimization

Reduce costs through intelligent automation and resource optimization.

- Turn reactive maintenance into a strategic advantage.
- FlashSystem.ai proactively detects anomalies, predicts capacity needs and tunes performance automatically, which helps cut costs and guarantee SLAs without disruption.

Context-aware security

Protect critical data and customer trust.

- Stay on top of evolving business needs with continuous threat detection and rapid recovery.
- AI-driven ransomware detection and autonomous healing actions help alleviate the risks from outages and cyberattacks, minimizing downtime and maintaining customer trust.

Consistent compliance

Stay ahead of regulations with automated compliance controls.

- FlashSystem.ai enforces best practices, manages audit logs and generates reports—simplifying adherence and reducing risk of fines.
- The Security Posture dashboard aligns with NIST standards and instantly triggers alerts when configurations drift from best practices.

06

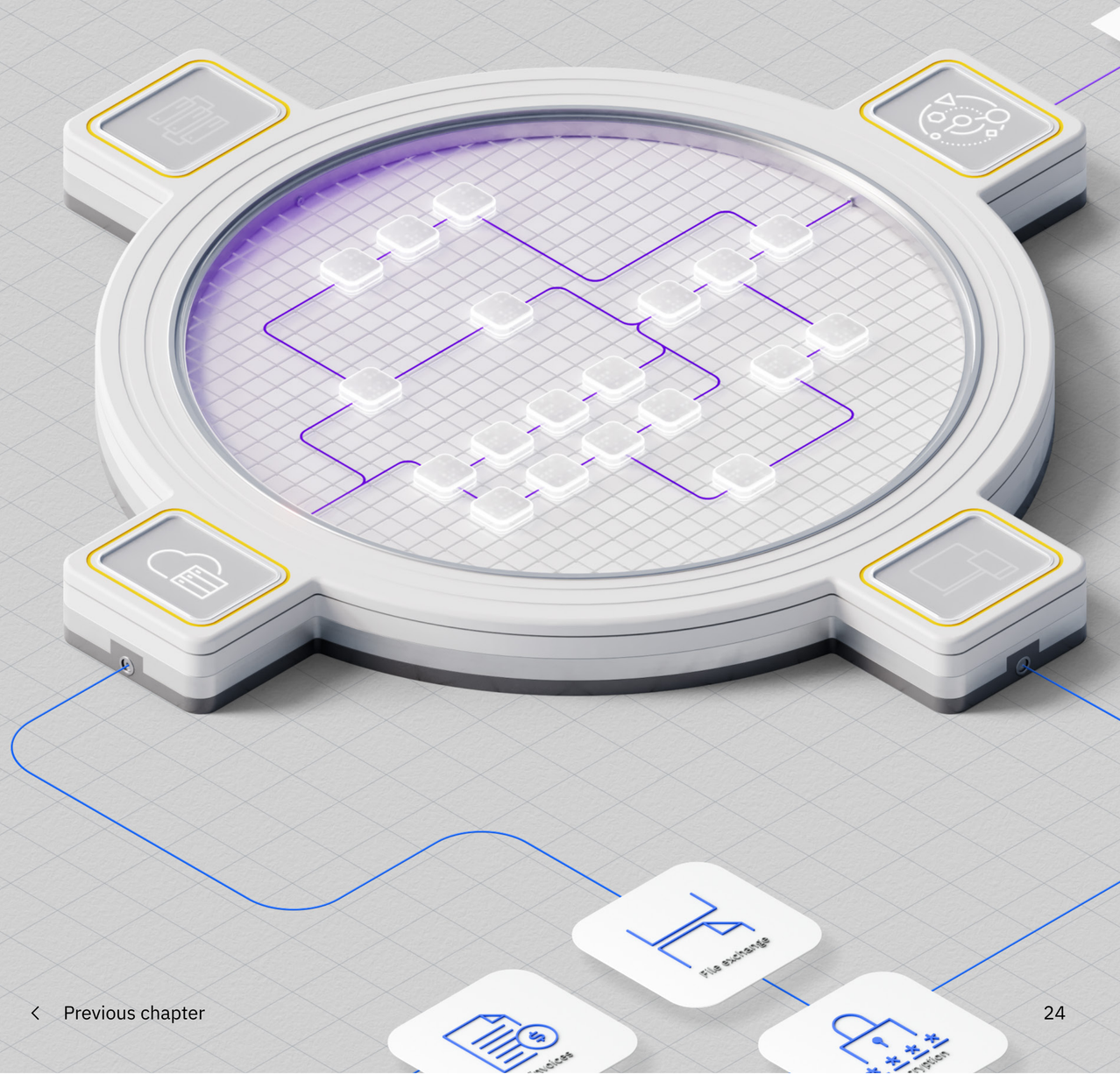
A stronger path forward together

Building true cyber resilience isn’t just about deploying the right technologies; it’s about aligning people, processes and infrastructure around a strategy that can withstand disruption and keep your business moving in the right direction.

As threats evolve and operational demands intensify, enterprises need partners who can help them turn a complex landscape into a clear, actionable path forward.

As an IBM business partner, we’re committed to helping clients navigate that path. By applying the principles highlighted in this playbook and leveraging the capabilities of IBM FlashSystem, we help clients strengthen protection, accelerate recovery and build the confidence required to operate securely in any environment.

When you’re ready to take the next step, we’re ready to help you shape a resilience strategy that supports your goals and keeps your business prepared for whatever comes next.



[1] IBM Cost of a Data Breach Report 2025: The AI Oversight Gap, IBM, July 2025.
[2] Data Protection Must Evolve Beyond Backup and Recovery, IDC, May 2024.
[3] ITIC 2024 Hourly Cost of Downtime Report, ITIC, 3 September 2024.
[4] The Global State of Strategy 2024, Quantive, 8 May 2024.