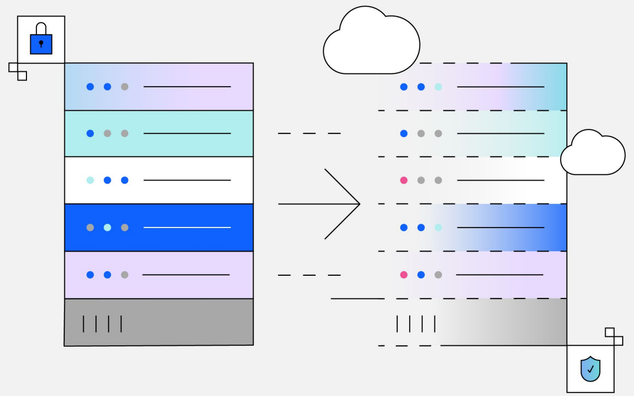
The Storage Imperative for Cyber Resilience



A strategic guide to protecting critical data and recovering with confidence



IBM

01 →
Executive summary

02 →
The new reality for infrastructure leaders

03 →
Five requirements of a resilienct infrastructure

04 →
Building an end-to-end cyber resilience strategy

05 →
IBM FlashSystem:
Protect, adapt and perform

06 →
A stronger path forward together



01

Executive summary



Cyberattacks are intensifying across every industry, driving operational, financial and reputational risk. In 2026, the global average cost of a data breach was **USD 4.99 million**, while US-based organizations spent a record-high average of **USD 11.5 million per incident**. These rising costs are driving greater investment in security: nearly 85% of breached organizations that are aware of new AI model capabilities are planning 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 storage capabilities required to protect critical data, accelerate recovery, strengthen compliance and maintain continuity during cybersecurity incidents.

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

02

The new reality for infrastructure leaders

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

Recent regulations—such as the Digital Operational Resilience Act (DORA) and the NIS2 Directive in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, 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:



1. Threats remain undetected for longer.

Organizations now take an average of 247 days to identify and contain a breach, highlighting the challenges many face in detecting and responding to threats.[1]

The longer threats remain undetected, the greater the potential impact on business operations and recovery efforts. As a result, improving resilience against cyberattacks has become the top technology priority for many IT leaders.[2]



2. Attackers are increasingly targeting backup and recovery systems.

Modern ransomware attacks may include data theft before encryption, which means recovery alone cannot determine what information was exfiltrated. Resilient infrastructure therefore needs protection, early detection and trusted recovery capabilities working together.

Ransomware attacks are now routine:

- 93% of surveyed organizations said they had experienced an attempted ransomware attack in the last 12 months
- More than a third (35%) experienced weekly attacks.
- More than one in five (22%) experienced ransomware attempts daily.[2]

As attacks become more pervasive, they are increasingly attempting to destroy or disable backup and recovery capabilities, increasing the likelihood of ransom payment and prolonged recovery.



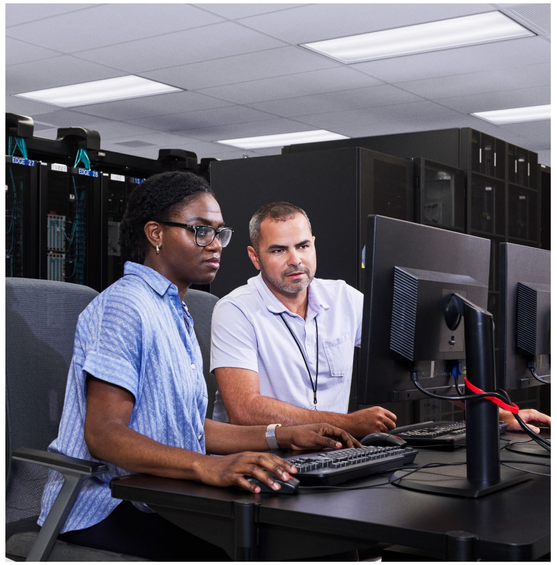
3. Attacks are becoming more sophisticated.

Attackers are increasingly weaponizing AI, using it to automate the attack lifecycle, scale operations and refine the sophistication of their attacks.

This year's research shows the impact: more than one in four organizations that experienced a malicious attack reported it was AI-driven, a 56% increase over last year. AI deepfake impersonation and AI-enabled malware drove the highest volume of those incidents. The financial consequences: AI-driven attacks added an average of USD 1 million per breach.[1]

03

5 requirements of a resilient infrastructure



Cyberthreats, rising costs and compliance demands and growing operational complexity are forcing organizations to rethink how they protect and recover critical data. While cybersecurity tools play an essential role in prevention and detection, resilience ultimately depends on an organization's ability to access trusted data, recover quickly, and maintain business continuity when disruption occurs.

As a result, modern infrastructure requires more than traditional data protection. Organizations need storage capabilities that help them:

- Accelerate recovery time
- Improve visibility across hybrid environments
- Protect critical data
- 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

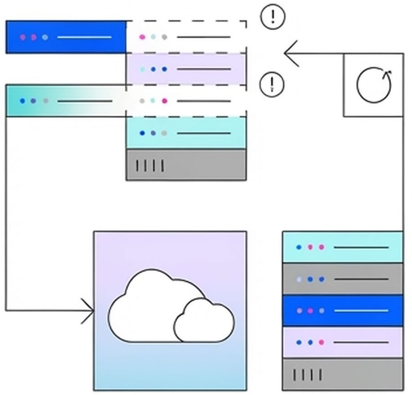
Modern resilience depends on having immutable, securely isolated copies of critical data paired with real time anomaly detection that identifies corruption the moment it appears. Automated or semi automated recovery workflows reduce manual intervention and ensure that organizations can restore operations quickly and cleanly. Organizations need storage platforms that create immutable recovery points, continuously verify data integrity and enable recovery validation before production restoration. Recovery confidence comes from knowing protected copies are trustworthy, tested and ready to restore when needed.

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 (RTO/RPO) 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 consistent storage-level protection policies across on-premises, edge and cloud environments, as well as 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

Modern resilience requires storage that simplifies operations through AI-driven automation, predictive analytics, and intelligent workload optimization. Organizations need the ability to identify capacity and performance issues before they impact applications, automate routine management tasks, and manage infrastructure through a consolidated control plane. Intelligent data placement and resource optimization further help reduce operational overhead while maintaining performance and availability.

Why it matters

As data volumes continue to grow, IT teams are expected to manage increasingly complex environments with limited resources. AI-assisted operations help reduce manual effort, improve efficiency, and lower total cost of ownership while enabling infrastructure teams to focus on higher-value initiatives.

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



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. Organizations must be prepared to demonstrate that critical data remains protected, recoverable, and compliant throughout its lifecycle. Storage systems that automate policy enforcement, support audit readiness, and enable validated recovery help reduce compliance risk while strengthening overall resilience.

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

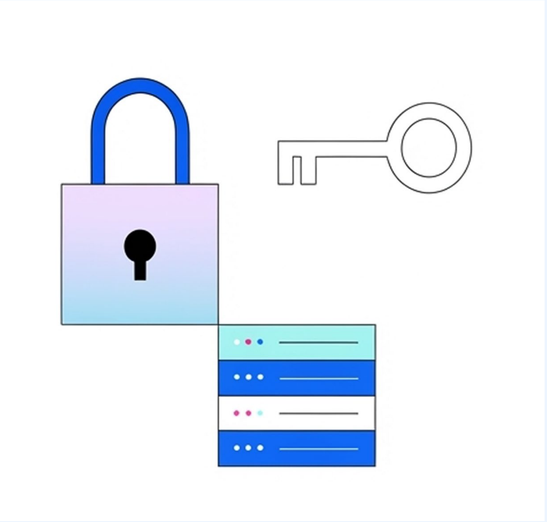
Organizations need AI enabled detection systems that can identify advanced attack patterns. These systems should be supported by real time monitoring that spots unusual data behavior early, including indicators that may precede ransomware encryption. They also require automated environment isolation 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. Storage platforms should continuously analyze behavioral patterns, detect anomalies, and help identify ransomware activity before widespread impact. Integrate storage telemetry with security operations and automate isolation of suspicious data.

Why it matters

AI-powered cyberattacks are growing. According to organizations surveyed in the 2026 Cost of a Data Breach report, AI-driven attacks increased 56% in 2026 compared to the previous year. 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



1. 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.



2. 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 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.



3. 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.



4. 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 (I/O) patterns—all within seconds.

Best practices:

- Deploy behavioral analytics that monitor changes in I/O 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.



5.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 them based on findings.

Key storage foundations of cyber resilience

Modern cyber resilience depends on more than security controls and recovery plans. Organizations need storage capabilities that help protect critical data, identify threats early, validate recovery readiness, restore operations quickly, and continuously adapt to evolving business and regulatory requirements.

These five foundations provide a framework for evaluating resilience readiness and building a strategy that can withstand modern cyberthreats while supporting business continuity.

Protect

Immutable copies and isolated recovery data help safeguard critical information from ransomware and unauthorized modification.

Detect

AI-powered anomaly detection helps identify unusual activity before threats spread across the environment.

Validate

Recovery testing and assurance processes help confirm that protected copies are recoverable and ready when needed.

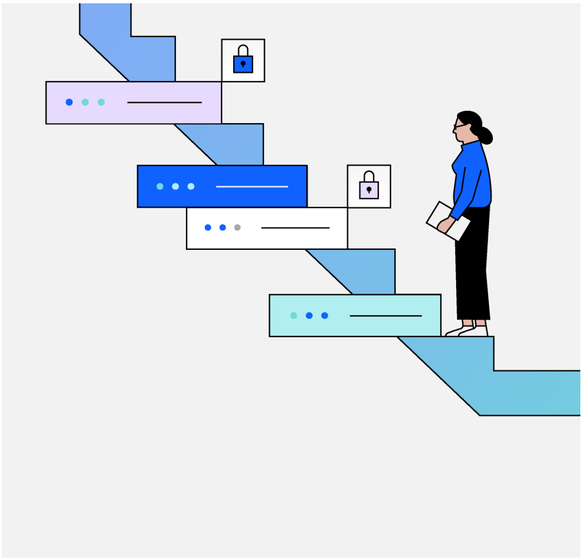
Recover

Automated restoration workflows help reduce downtime and accelerate business recovery following a disruption.

Adapt

AI-driven operations, automation, and compliance readiness help organizations continuously optimize resilience as requirements evolve.

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
- Identifying early signs of exfiltration

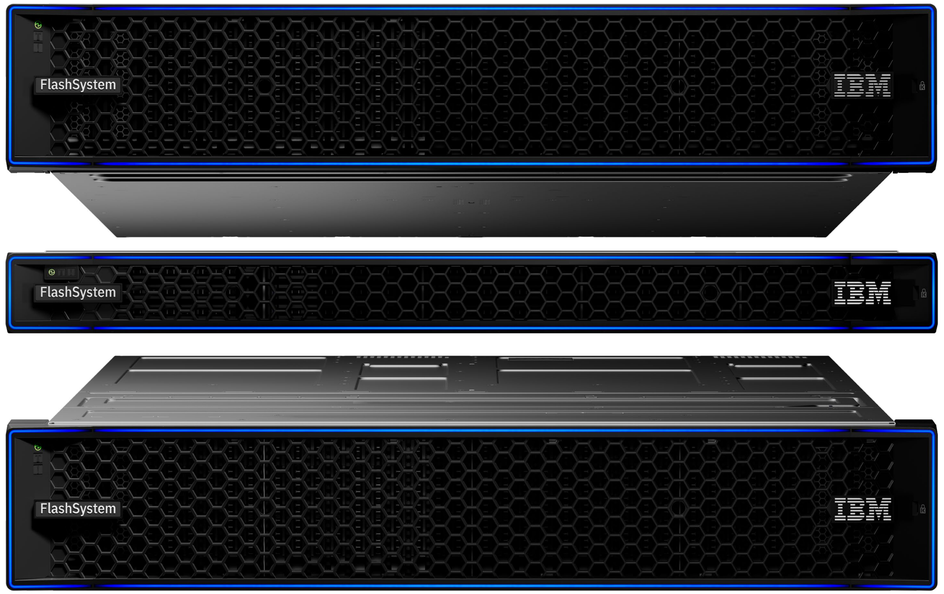
Are you resilience-ready?

Curious how protected your business is? Take our free assessment to evaluate your cyber readiness against the areas defined in the NIST Cybersecurity Framework.

Get started now →

05

IBM FlashSystem: Protect, adapt and 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 only after explicit user approval. This approach ensures that full administrative control remains with the organization.
- AI agents explain decisions, suggest performance improvements and learn from user feedback—helping reduce storage management effort by up to 90% compared to doing those routine operations in the GUI.[3]



Proactive optimization
Reduce costs through intelligent automation and resource optimization.

- Turn reactive maintenance into a strategic advantage.
- FlashSystem.ai can proactively predict capacity needs and recommend or automate routine optimization, reducing administrative effort while supporting performance and service-level objectives.



Context-aware security
Protect critical data and customer trust.

- The FlashCore Module (FCM) computational storage technology is designed to continuously monitor statistics gathered from every single I/O. IBM FlashSystem uses machine learning models to detect anomalies like ransomware in less than a minute[4], with no impact on system performance and seamless scalability when adding new drives.
- The latest generation of FlashSystem flags verified data exfiltration events after a 30-minute confidence window, with a false-positive rate below 1%.[5]
- Early threat detection, immutable protection, trusted recovery and continuous resilient infrastructure.

- AI-driven ransomware detection and autonomous healing actions help alleviate the risks from outages and cyberattacks, to minimize downtime and maintain customer trust.
- Two-person integrity helps protect your critical data. Designed to help reduce the risk of social engineering attacks, it requires two administrators to modify retention policies or delete backups.
- The world's first quantum-safe self-encrypting custom Flash module helps safeguard the delivery of critical services.

Consistent compliance
Stay ahead of regulations with automated compliance controls.

- IBM FlashSystem architecture is designed to help address regulatory standards such as DORA, NIS2, GLBA, and more.
- The Security Posture dashboard aligns with NIST standards and instantly triggers alerts when configurations drift from best practices.



06

A stronger path forward together

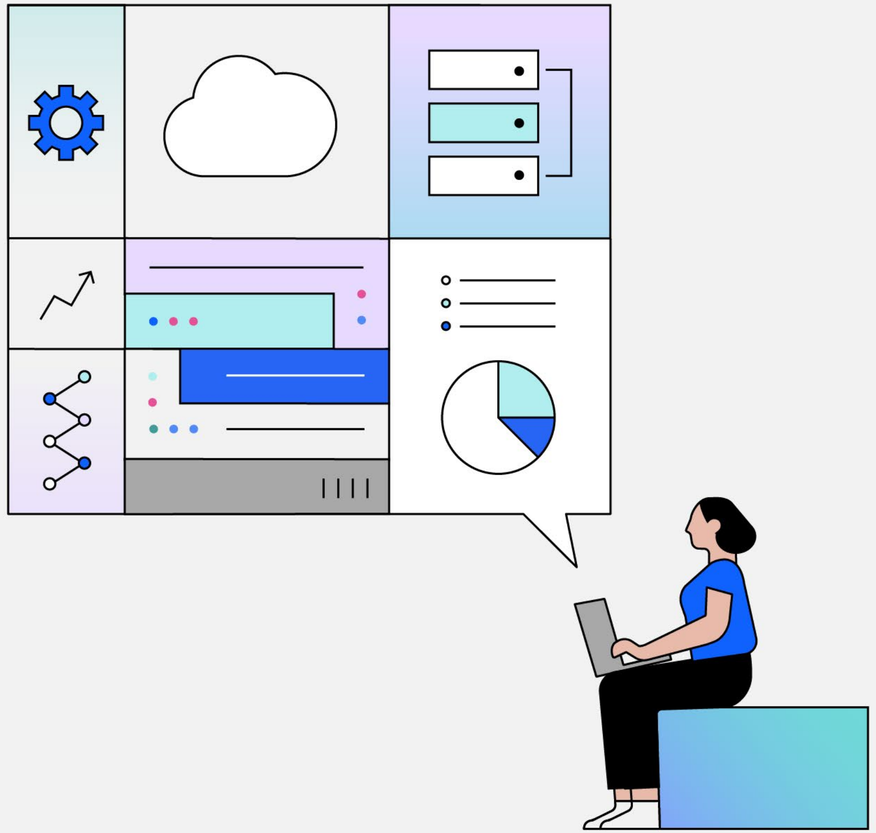
Getting started is as easy as 1, 2, 3

1. Take IBM's Cyber Resilience Assessment to benchmark maturity and identify gaps.

2. Prioritize actions across **Identify, Protect, Detect, Respond** and **Recover.**

3. Stay ahead of evolving cyber threats and resilience requirements with the latest cyber resilience resources and guidance.

These steps will help your organization adapt faster, perform more efficiently and protect what matters most—so your business can continue to thrive even when incidents strike.



1. Cost of a Data Breach Report 2026: The AI Tipping Point, IBM, July 2026

2. Enabling modern cyber-resilience with IBM Storage, IBM, January 2026.

3. Based on internal, task-based evaluations of representative routine operations (multi-volume provisioning with Safeguarded Copy and DR policies) under lab-controlled conditions on latest generation FlashSystem models (5600, 7600, 9600) with FlashSystem.ai, versus the latest generation of IBM FlashSystem (5600, 7600, 9600) without FlashSystem.ai. Actual results vary by environment, integrations, policies and user proficiency.

4. Internal experimentation by IBM Research has demonstrated detection of ransomware within 1 minute of the ransomware starting its encryption process. This experiment was done on a FlashSystem 5200 with 6 FCMs with the 4.1 firmware load. The 5200 had 8.6.3 GA level software loaded. The host connected to the 5200 was running Linux with XFS Filesystem. In this particular case, the IBM ransomware simulator called WannaLaugh was used. Underlying system must be compatible with FCM4.1 and version 8.6.3 GA level software loaded in order to receive results obtained.

5. Data exfiltration detection based on real field telemetry from customers running firmware 9.1.2+ on FlashSystem models 5600/7600/9600. Individual results may vary.

© Copyright IBM Corporation 2026

IBM, the IBM logo, IBM FlashCore and IBM FlashSystem are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on https://www.ibm.com/legal/copytrade.

This document is current as of the initial date of publication and may be changed by IBM at any time.

Not all offerings are available in every country in which IBM operates.

Examples presented as illustrative only. Actual results will vary based on client configurations and conditions and, therefore, generally expected results cannot be provided.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.