Stay Ahead of Cyber Threats with IBM FlashSystem Resilience 360

Secure Your Data and Keep Your Business Running

Highlights

- Rapid ransomware detection and automated recovery workflows
- Real-time AI-powered anomaly detection across all I/O
- Immutable snapshots with Safeguarded Copy
- Architecture designed to address multiple regulatory requirements.

The Rising Cost of Cyber Attacks

In today's threat landscape, IT leaders are placing data resilience at the forefront of their cybersecurity strategies—and for good reason. Data remains a critical asset, constantly exposed to risks from ransomware, cyberattacks, human error, hardware failures, and natural disasters. The financial stakes are high: in 2025, the average global cost of a data breach was **$4.44 million**, according to the latest IBM Cost of a Data Breach report[1]. While this marks a 9% decrease from the previous year, largely due to AI-driven efficiencies, the operational impact remains significant. On average, it still takes **241 days** to identify and contain a breach.

Beyond financial losses, regulatory pressure is intensifying. Governments worldwide are enforcing stricter data protection laws to ensure organizations uphold robust cyber resilience.

These developments highlight the critical importance for organizations to implement comprehensive data resilience strategies that integrate AI, automation, and governance, ensuring the protection of their most valuable digital assets and establishing a strong foundation to keep data secure and business operations uninterrupted.

To help organizations in strengthening their cyber resilience posture, IBM offers IBM FlashSystem Resilience 360, designed to accelerate detection, streamline recovery, and ensure compliance in the face of growing cyber threats.

A Standard Framework for Data Resilience

Many organizations today are designing their data resilience strategies around the cybersecurity framework developed by the US government's National Institute for Standards and Technology (NIST).

The NIST cybersecurity framework focuses on managing risk, and encompasses five key areas:

- Identify: Understand and manage cybersecurity risks to all systems, assets, data, and capabilities.
- Protect: Implement safeguards to ensure the delivery of critical infrastructure services.
- Detect: Deploy activities to identify the occurrence of a cybersecurity event.
- Respond: Deploy activities to respond to a detected cybersecurity event.
- Recover: Deploy activities to restore services impacted by a cybersecurity event.

The framework has recently added a governance layer at the core, to reflect emerging changes in business practices in response to cyber threats, as well as increased regulatory attention in this area.

The IBM FlashSystem Resilience 360 adopts Best Practices outlined by the NIST Cyber Security Framework, and can assist clients at every stage of their framework journey.

Identify
To assess your risk and architect steps to protect your business, IBM offers a free, two-hour virtual Cyber Resiliency Assessment with IBM security experts. It delivers a confidential, vendor-neutral analysis without the need to install anything or run any scripts. You will obtain a detailed report, a roadmap of recommended improvements and considerations, as well as a management presentation connecting practical methods to achieve your critical business outcomes.

Protect
Verified restore points that align with your Recovery Point Objectives safeguard your data integrity. They ensure no malicious code is reintroduced during the recovery process, enabling you to confidently recover your essential business operations. And the two-person integrity helps reduce the risk of social engineering attacks by requiring two administrators to modify retention policies or delete backups.

Detect
Experience real-time protection with continuous monitoring of statistics gathered from every single I/O using AI and machine learning models to detect anomalies like ransomware in less than a minute[2], with no impact on system performance and seamless scalability when adding new drives.

Respond and Recover
After a ransomware attack takes place, our 60-second Cyber Recovery guarantee[3] helps reduce downtime with almost immediate access to uncorrupted backups from known good air-gapped snapshots.

Core Elements of IBM FlashSystem Resilience 360

1. IBM FlashSystem

IBM FlashSystem® brings together intelligent cyber-resilience, adaptive operations, and sustained performance in a cohesive all flash array storage solution designed for modern enterprise demands. The new IBM FlashSystem models' threat detection achieves highly accurate detection, trained on tens of billions of data points collected through advanced telemetry and years of real-world operational data, keeping false positives to under 1%[4,],helping organizations reduce the likelihood of widespread corruption and the rising costs associated with prolonged breach detection. When recovery is required, FlashSystem supports isolated, immutable recovery points and orchestrated response that shortens the time to identify and contain disruptive events—key factors shown to dramatically lower breach costs.

At the same time, **FlashSystem.ai** is capable of understanding your business intent, amplifies the expertise of your Storage Operations team, and is capable of dynamically adjusting to shifting workload demands, enabling teams to respond faster, manage storage more efficiently, and maintain predictable performance as business needs evolve. FlashSystem.ai in IBM's latest generation of **FlashSystem storage can reduce storage management effort by up to 90%** compared to doing those routine operations in the GUI.[5]

IBM FlashSystem enables rapid breach response through built-in features like ransomware threat detection, which leverages IBM FlashCore® Module Gen 5 computational storage, AI, and machine learning models to identify abnormal data behavior. It is designed to continuously monitor statistics collected from every I/O to detect unusual patterns, such as ransomware, in less than a minute[2], enabling quick response and strengthened data security.

2. IBM Storage Insights

A cutting-edge AI operation service that provides proactive monitoring of your storage environment, guaranteed ransomware alerts within 60 seconds[2], system performance analysis, application analysis, and intelligent advisories, empowering you to effectively safeguard and optimize your storage infrastructure.

3. IBM Storage Defender Sentinel

An added layer of security, offering advanced monitoring and analytics to proactively identify, prioritize, and remediate potential security risks for VMware, SAP HANA, Oracle Database, and EPIC workloads. IBM Storage Defender Sentinel is workload-specific software that detects, diagnoses, and identifies the sources of ransomware attacks and provides automated recovery orchestration.

IBM Storage Defender Sentinel automates the creation of immutable backup copies of your data. Then it uses machine learning to detect signs of possible corruption and to generate forensic reports that help you quickly diagnose and identify the source of the attack. Because this solution can intelligently isolate infected backups, your organization can identify the most recent verified and validated backup copies, which can accelerate your time to recovery.

With IBM Storage Defender Sentinel you are not just protecting your data –you're ensuring every recovery point is a trusted, verified point back to operations.

<1 minute

To detect ransomware[2]

60-second

Recovery Time Objective Guarantee[3]

Strengthen Your Data Resilience with IBM

As cyber threats grow more sophisticated and regulatory demands intensify, organizations need more than just storage; they need a resilient foundation.

The IBM FlashSystem Resilience 360 delivers multiple layers of security that provide a robust foundation designed to safeguard your most critical data:

- **The IBM-developed ransomware threat detection** AI model running on the latest generation FlashSystem models executes in real time on the storage controllers and does not affect performance.[6]
- **AI-powered anomaly detection** across all I/O for proactive threat identification
- **Immutable, air-gapped snapshots** with Safeguarded Copy to ensure data integrity
- **Architecture designed to help address regulatory standards** such as DORA, NIS2, GLBA, and more
- **Guaranteed 60-second recovery**[3] from known-good snapshots to minimize downtime.

Whether you're preparing for regulation compliance or aiming to reduce risk and downtime, IBM FlashSystem offers the performance, security, and efficiency to meet your goals. With up to **2.4PB effective capacity in just 1U with FlashSystem 5600** increasing to a maximum of **11.8PB effective capacity in 2U with FlashSystem 9600**, it's a smart investment in operational resilience—today and for the future.

IBM FlashSystem Resilience 360 empowers organizations to move beyond traditional static backup strategies and adopt a proactive, integrated approach to cyber resilience—ensuring business continuity even in the face of sophisticated attacks.

For more information
Learn more about IBM FlashSystem Resilience 360, contact your IBM representative or IBM Business Partner, or visit ibm.com/flashsystem/cyber-resilience

1. Cost of a Data Breach Report, July 2025.
2. 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.
3. Terms and conditions apply. IBM Cyber Resiliency Guarantee, IBM. https://community.ibm.com/community/user/storage/blogs/nat-prakongpan/2023/09/12/ibm-flashsystem-cyber-recovery-guarantee
4. False-positive performance is based on models trained with recurring production telemetry, used to refine discrimination and reduce false positives on latest generation FlashSystem models (5600, 7600. 9600). This applies to the most recent Ransomware model (3.3) released on 4Q 2025. Data collected for 24 months. False positives measured over 3 months
5. 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.
6. This statement reflects the design of AI-based ransomware threat detection models developed by IBM and deployed on the latest generation FlashCore Modules and FlashSystem models (5600, 7600, 9600), where evaluations are performed on-array using IBM Snap ML–based techniques with minimal controller CPU and memory overhead under tested conditions. “Affect performance” is based on internal assessments of representative workloads and system headroom.

Produced in the
United States of America
February 2026