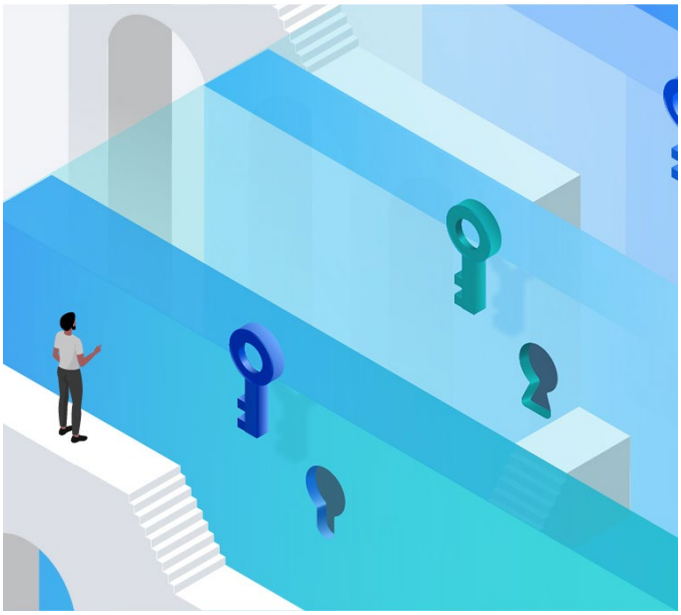
The Power of FlashSystem and Defender Together

Enhancing IBM FlashSystem data protection with IBM Storage Defender Data Resiliency Service



Prioritizing investments in cyber resilience is essential in today's landscape. According to IDC, enhancing cyber-recovery and resiliency has become one of the top priorities for organizations due the growing adoption of AI/GenAI[1] and the risks that it introduces, such as data exfiltration, data poisoning and privacy breaches. In addition to these threats, IT organizations must contend with natural disasters, system failures, human errors, and sabotage—events that can result in substantial reputational and financial losses.

Storage Defender and FlashSystem address these challenges with a proactive approach. Together, provide comprehensive end-to-end protection using AI sensors that meticulously analyze data patterns and identify anomalies across all storage tiers. After a threat is detected, organizations receive active notifications and visibility in a single pane of glass to analyze the detection further. In addition, third party integration with Security Information and Event Management (SIEM) systems such as QRadar and Splunk, help to enhance threat identification and response capabilities. Once a threat has been identified and contained, a safe snapshot is validated before recovery, which enables an early response and reduces Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) in complex attack scenarios.

Multi-layered AI Threat Detection

- Combine the power of your array-based ransomware detection with additional layers of protection to catch threats sooner.
- Detect suspicious objects before restoring them to production with AI-driven software sensors and malware scanners to

Data Resilience

- Ensure SGC frequency and backup policies for storage are on track.
- Coordinate security posture across teams.
- Integrate with existing security tools for alerting and automation.

Automated Safeguarded Copies

- Combine threat detection with automated damage control.
- Aggregate alerts, generate e-mail and SIEM alerts, and auto-trigger SGC on resources to contain data damage.

Safe and fast recovery

- Associate existing volumes and SGC with workloads grouped by critical functionality.
- Perform recoveries in 60 seconds[2] when needed for attack response and testing.

Don't wait for disaster. Experience 60 days of advanced ransomware protection free.

1. IDC Tech Buyer, Cyber-Resilience — Turning Every Crisis into an Opportunity to Emerge Stronger, US52280524, Apr 2025
2. 2. IBM Terms, “IBM FlashSystem Cyber Recovery Guarantee” March 21, 2024