IDC

ANALYST BRIEF

Sponsored by: NetApp

Cyber-resilience isn't just about data protection and security. Active defense capabilities at the storage layer can lead to faster threat detection and isolation, rapid recovery, and reduced downtime.

Storage Is the Front Line of Cyber-Resilience

March 2026

Written by: Johnny Yu, Research Manager, Infrastructure Software Platforms, Worldwide Infrastructure Research

Introduction

Cyber-resilience often utilizes a layered approach to security to prevent intrusions, combined with backup and recovery tools for restoring an organization's data following a breach. While the backup layer is important, it isn't typically engaged until well into an attack when data has already been accessed, stolen, encrypted, or deleted.

Attackers are ultimately after data in primary storage, and there's no reason it should be a passive victim. The storage layer is closest to the data and should therefore be an active layer of defense. Integrating storage into your cyber-resilience strategy will help reduce dependence on complete backups and streamline recovery processes.

What active defense looks like

When it comes to cyber-resilience, taking a proactive stance involves capabilities that can reduce the impact of attacks before they do damage. The hallmarks of a cyber-resilient storage solution are the following:

- **Detection of breaches in real time** through the constant monitoring of activities for anomalous behavior. Suspicious data reads, encryption, deletion, and log-ins are all indicators of potential compromise.
- **Lower recovery point objectives** enabled through frequent snapshots. Coupled with threat detection pinpointing when compromise occurs, this allows for accurate rollbacks to the last known clean data with minimal data loss.
- **Robust recovery** that is fast and able to granularly recover files and objects to minimize data loss. The recovery process should also include malware removal and checks to ensure infections aren't accidentally restored.
- **Support for the larger security ecosystem** through escalation and handoff to SecOps that are as streamlined and collaborative as possible. The storage system must be able to surface important incident information, such as access logs and affected directories, to security tools.
- **Role-based access control** to ensure SecOps can access storage tools as needed to mount a proper incident response, but not access everything a storage administrator sees for daily storage operations. This also includes access-level tiers that depend on roles and policies to ensure that roles don't become overprivileged.

AT A GLANCE

KEY TAKEAWAYS

- The storage layer is closest to the data, so security capabilities at that layer, such as anomalous behavior monitoring, encryption detection, and threat isolation, all play a critical role in stopping attacks.
- Properly implemented cyber-resilient storage can lead to faster recovery, which lowers downtime and costs.
- Cyber-resilient storage isn't meant to replace security tools, but it can enhance SecOps tools with information gathered about the breach at the storage layer.

- **Proof of protection and resilience,** such as the ability to run resilience tests and give measurable results. This shows administrators and auditors that defensive measures are in place and working.

Benefits

With proactive defensive measures, storage can gain the following benefits:

- **Faster detection and response to threats** so that they are contained early, and damage is minimized. By raising alerts about or blocking suspicious and destructive actions automatically, there is a lower chance that a large-scale recovery is necessary.
- **Rapid and accurate recovery through snapshots**, leading to less data loss and downtime. Quickly returning business operations to normal lowers the financial cost of recovery as well as the hidden costs of loss of productivity, business reputation, employee morale, and other factors.
- **Removing the threat at the storage layer.** This lowers the risk of reintroducing vulnerabilities, making it less likely the organization will fall victim to the same attack again later.
- **SecOps escalation becoming easier.** While cyber-resilient storage isn't meant to replace security tools and won't become the perfect defense on its own, it makes escalation to SecOps easier because of all the information gathered about the breach at the storage layer.

Considerations

It can be challenging for storage teams to advocate for increasing investment in storage initiatives, including cyber-resilient storage. Many organizations are prioritizing spending on agentic AI development, which impacts their willingness to increase spending in other IT areas. And when it comes to investing more in cyber-resilience, most organizations take that to mean improving security and data protection tools. Despite being the first line of defense, storage may be last in line for cyber-resilience investment.

One possible approach for organizations is to address this by framing cyber-resilience as encompassing more than data protection and security, requiring defensive capabilities at multiple layers. Cyber-resilient storage is one of many components that, taken together, translate to reduced impact from cybercriminals and quicker recovery after an attack.

Another challenge for implementing cyber-resilient storage is understanding that it isn't simply about deploying new tools and capabilities within storage. It also involves adopting a cyber-resilient culture and best practices across the IT organization. Cyber-resilient storage doesn't replace security tools, and storage administrators don't replace SecOps. Organizations must foster collaboration, create escalation flowcharts, and train staff on how to play their role in cyber-resilience.

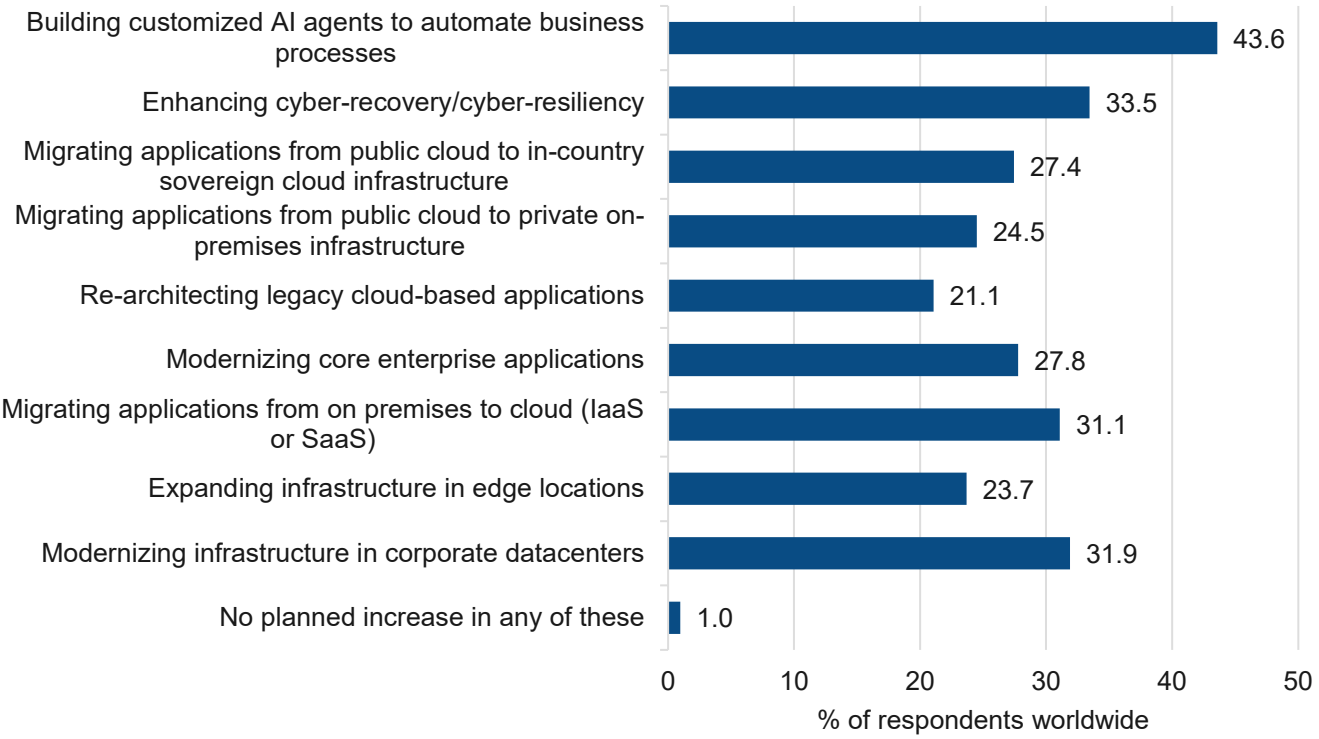
Trends

- Organizations recognize cyber-resilience as a top IT spending priority (see Figure 1), but AI agent deployment is ahead by a significant margin.
- Organizations are largely interested in investing more in cyber-resilience. This is an opportunity for cyber-resilient storage to be a part of that because overall resilience isn't tied to just security or data protection.

FIGURE 1: ***Where is IT spending increasing the most?***

Other than agentic AI, cyber-resilience is the top spending priority.

Q ***Regardless of overall IT spending plans, in which of the following areas do you expect to increase spending most significantly in 2026?***



n = 1,897

Source: IDC's Future Enterprise Resiliency and Spending Survey, Waves 8 and 9, December 2025

Conclusion

Cyber-resilience relies on multiple layers of defense, and storage should be the first line. Active defense at the storage layer can limit the impact of an attack or contain its blast radius, lowering the burden on recovery efforts. In addition, cyber-resilient storage has rapid recovery processes in place to return business to normal as quickly as possible, reducing costs due to downtime, data loss, lowered productivity, and reputation damage.

Storage systems should play an active role in defending the data they are holding.

Cyber-resilient storage isn't about replacing security or data protection; rather, it's about implementing defensive capabilities at the storage layer to bolster overall data and business resilience. Backup and recovery, forensics, and incident response are still necessary, but being able to identify and isolate threats and recover data at the storage layer can contribute to faster recovery and help quickly return a business to normal after an attack.

Storage systems should play an active role in defending the data they are holding. A breach can happen at any level, so countermeasures should also be present at multiple layers.

About the analyst

Johnny Yu, *Research Manager, Infrastructure Software Platforms, Worldwide Infrastructure Research*

Johnny Yu is a research manager within IDC's Worldwide Infrastructure Research organization and part of the Infrastructure Software Platforms practice. His coverage includes storage software, data replication, protection and archiving software, storage device management, and container data management.

MESSAGE FROM THE SPONSOR

NetApp Ransomware Resilience delivers a comprehensive solution for ransomware defense, enabling you to minimize the impact and return to normal business operations quickly and easily following an attack.

Protecting data where it resides, Ransomware Resilience detects data breaches, suspicious user behaviors, encryption and data deletion in real time, and immediately responds to contain the attack and limit its impact. Ransomware Resilience then cleans and restores the maximum amount of up-to-date data possible, all through a guided process.

With Ransomware Resilience you can limit data loss, prevent reinfection of the data, and minimize business disruptions, while reducing the operational burden of managing cyber defense for ONTAP storage. Ransomware Resilience gives you peace of mind. If an attack occurs on your storage, you'll know immediately, your valuable data will be protected, and recovery will be quick and easy.

To learn more, and register for a free trial please go here: https://www.netapp.com/data-services/ransomware-resilience/.

IDC Custom Solutions

The content in this paper was adapted from existing IDC research published on www.idc.com.

IDC Research, Inc.
One Beacon Street
Suite 33100
Boston, MA 02108, USA
T 508.872.8200
F 508.935.4015
blogs.idc.com
www.idc.com