Enabling Modern Cyber-resilience With IBM Storage

Why AI-powered Storage Resiliency Is Increasingly Critical to Combat the Cyber-crime Epidemic

Simon Robinson, Principal Analyst

January 2026

This Omdia White Paper was commissioned by IBM and is distributed under license from TechTarget, Inc.

Contents

Introduction – The Cyber Epidemic and Its Growing Impact on Every Organization

Of all the myriad ways in which technology innovation impacts an organization, one issue continues to dominate: cybersecurity. Though digital security has long been top of mind for IT leaders, the scale, extent, and sophistication of cybercrime continues to evolve to a level where it now presents an existential threat to many organizations. According to Enterprise Strategy Group (now Omdia) research, improving cybersecurity posture and organizations' resiliency against cyberattacks is comfortably the most important technology priority among IT leaders (see Figure 1).[1]

What were once ad hoc attempts to take down individual applications and services by opportunistic individuals have transformed into a relentless barrage of precisely orchestrated attacks, often by well-organized crime syndicates. These attacks can take down an entire organization, targeting their critical infrastructure, intellectual property, and sensitive information—all at huge financial and reputational cost. Increasingly, attacks leverage AI technologies to cause even more damage. The scale of the threat is so alarming

[1] Source: Enterprise Strategy Group (now Omdia) Research Report, *2025 Technology Spending Intentions Survey*, December 2024.

that governments and regulatory bodies are stepping in, with legislation and other mandates that require organizations to protect themselves.

With many organizations experiencing a daily onslaught of attempted attacks, the posture of all organizations must expand from prevention to recovery. To quote an old adage, “The bad guys only need to be lucky once; we need to be lucky every day.” Sooner or later, many organizations will be compromised. In such a situation, the emphasis must expand to minimizing the damage of an attack through early detection and then ensuring the business can restore normal operations as quickly as possible.

But, in a world of constantly evolving threats and an increasingly complex IT landscape, organizations often struggle to know where to begin developing a strategic cyber-resilience response.

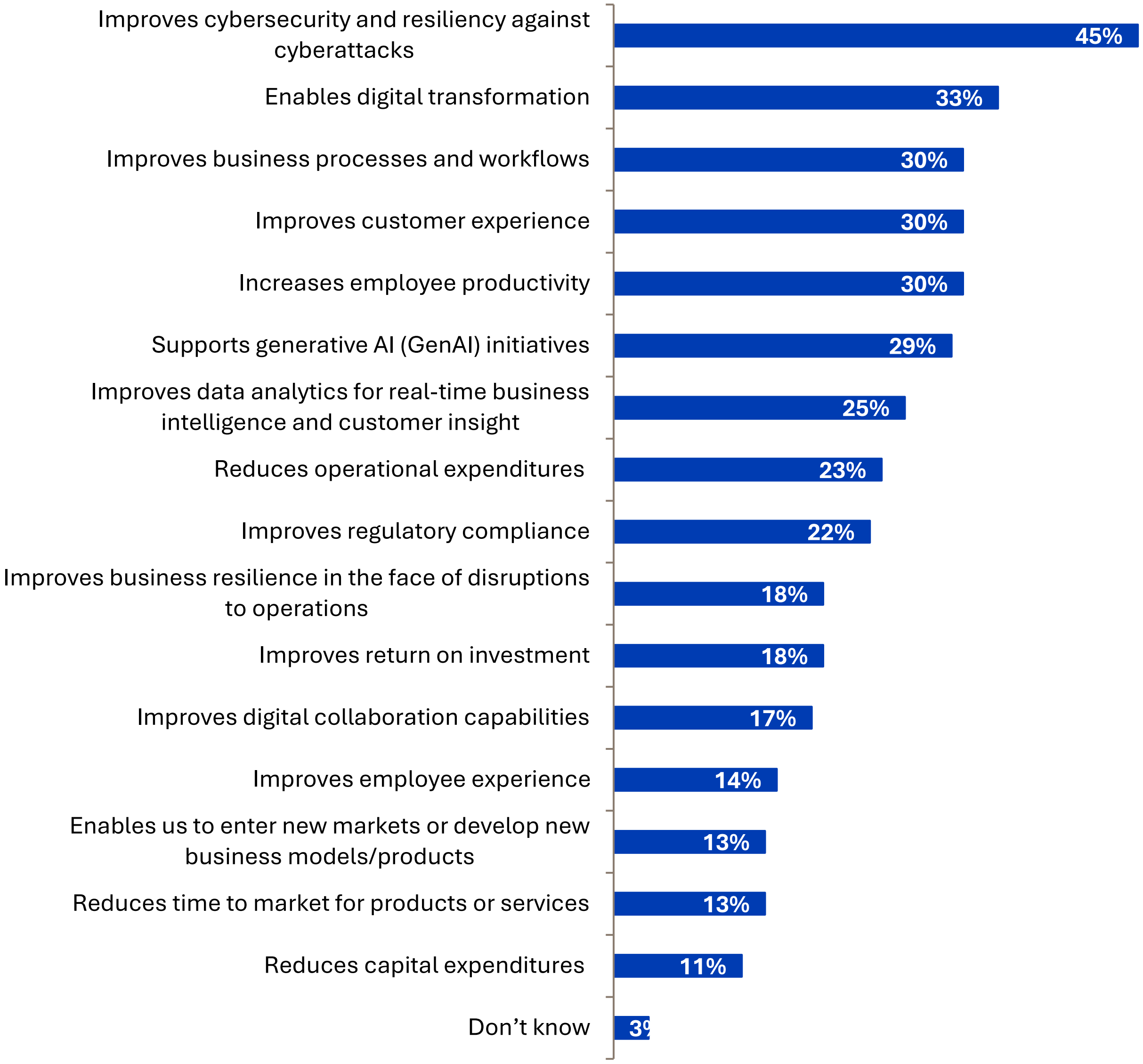
Two key aspects should be foundational to any comprehensive resiliency strategy. First, it starts with data. Bad actors know that data is the lifeblood of every organization, and switching off access to their data is the fastest and most effective way to disable operations. As the custodian of an organization’s data, the enterprise storage environment is, therefore, central to building an in-depth resiliency response.

The second key aspect is AI. As well as being a weapon, AI can play a key role in helping IT leaders develop a shield that can provide early warning that an attack is underway.

In this paper, we document the growing role that storage-level technologies are playing in cyber-resilience strategies and highlight the key innovations around data and AI that IBM is providing, enabling IT organizations to embed resilience into the heart of its storage infrastructure to form the foundation of modern cyber-resilience.

Figure 1: IT Investment Priorities

Which of the following considerations do you believe will be most important in justifying IT investments to your organization's business management team over the next 12 months? (Percent of respondents, N=1,351, five responses accepted)



Source: Omdia

The Rising Threat Landscape: Successful Attacks Are Increasingly a Case of ‘When,’ Not ‘If’

Recent Omdia research on the impact of ransomware on enterprises highlights the sheer scale and impact of the current cyber epidemic. Key findings include:[2]

- **Ransomware attacks are now routine:** 93% of respondents said they had experienced an attempted ransomware attack in the last 12 months; more than a third (35%) experienced weekly attacks, and more than one in five (22%) experienced ransomware attempts daily.
- **Attacks present an existential threat:** 88% of IT leaders regarded ransomware as a top five business risk overall, with 57% regarding it as a top three or higher risk.
- **Attacks go undetected:** 85% of ransomware attacks went undetected for more than 24 hours, with 46% remaining undetected for more than a week, highlighting that current detection strategies are largely ineffective.
- **Almost all victims lose data:** 99% of victims of successful ransomware attacks lost data. Moreover, a massive 45% of organizations were able to recover only half of their data or less.
- **The cost of attacks is alarming:** 75% of attacks had a financial impact of between $500,000 and $4.99 million; for a significant minority, the overall cost is much greater. Additionally, more than two-thirds (69%) of organizations paid a ransom.
- **Attacks are becoming more sophisticated:** Double or multi-stage extortion (i.e., repeated attacks) are now normal, with 89% of ransomware victims facing additional demands or attempts after the initial ransomware demand. Additionally, cyber-criminals increasingly leverage AI to multiple ends, such as automating large-scale phishing attacks, finding vulnerabilities, and creating increasingly convincing deepfakes and impersonations as part of social engineering scams.

[2] Source: Omdia Research Report, *The Ransomware Reality: Cyber Resilience, Data Resilience, and Data Protection*, November 2025.

Cyber Strategies Are an IT Priority but Drive Cost and Complexity

Looking at such data, it's increasingly clear that attacks are not only growing massively but are also increasingly successful, presenting enormous challenges to IT and security leaders charged with protecting the organization's IT infrastructure and data.

It also poses some major questions to IT leaders, such as, "Why are the bad guys increasingly successful, especially at a time when IT organizations themselves are prioritizing cyber protection?"

There's no simple answer, as in most cases it comes down to a combination of factors, However, two issues stand out. First, cybercrime is evolving into a lucrative, and increasingly professionalized, business, encouraging an increasing number of bad actors to develop ever-more-sophisticated attacks. This is now an arms war, requiring organizations to constantly evolve and adapt to the changing threat. Unfortunately, many are simply failing to keep up with the rapidly evolving scale of the threat.

The other major factor is the nature of the IT environment itself. As organizations digitize, they are embracing a growing number of technologies, applications, services, and locations—both on and off premises. It is the large, growing, and disparate nature of the IT environment itself that has dramatically expanded the attack surface.

This digitization has made the overall IT environment more complex; according to Enterprise Strategy Group (now Omdia) research, six in ten organizations said their IT environment has become more complex over the last two years, with more than one in five stating this complexity increase has been substantial. When looking at the drivers of this complexity, cybersecurity once again appears at the top of the list (cited by 42% of organizations). Related issues, such as security and privacy regulations, also feature highly as a complexity driver (32%). Additionally, 37% of organizations reported facing a chronic shortage of cybersecurity skills that limits their ability to comprehensively respond to the challenge, second only to AI skills shortages (47%).[3]

[3] Source: Enterprise Strategy Group (now Omdia) Research Report, *2025 Technology Spending Intentions Survey*, December 2024.

From Cybersecurity to Data Resilience

The challenge is that this complexity increases risk: Consistently applying a comprehensive security policy across a diverse, distributed environment is a huge undertaking, with any gap potentially leaving the organization open to attack.

The growing reality for many organizations is that, despite their best efforts, the bad guys are sometimes going to get through. Though organizations should, of course, continue to protect their environment to prevent such attacks from taking place, they also need robust and trusted strategies that help their businesses recover when the inevitable breach occurs.

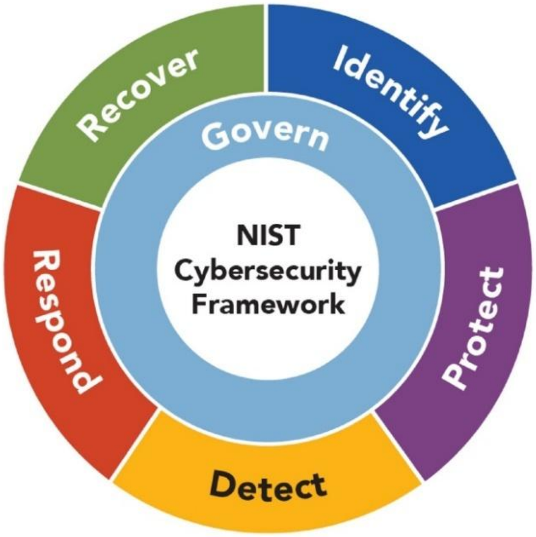
Developing such a resiliency strategy is not simply about deploying a single product or technology; instead, it's about creating a layered and in-depth approach that permeates the entire environment. These recovery plans need to be well integrated with preventative security measures and must be kept ready, regularly tested, and continuously validated to ensure business continuity.

In addition, the scale of the security epidemic has provoked a strong response from governments, regulators, and industry bodies, with mandates, guidance, and frameworks designed to help organizations formulate a strategic response to these threats. Developments such as the NIST Cybersecurity Framework provide broad guidelines for how organizations can manage their risk, spanning identity, protection, detection, response, and recovery with governance (see Figure 2). In Europe, mandates such as the NIS2 Security Directive and DORA in financial services require organizations to create the necessary protections within their infrastructure that enable them to recover in response to a range of disruptive events, including cyberattacks.

These initiatives are designed to highlight the scale and extent of the threat to senior leaders within all organizations; in the past, too many have implemented such measures only after they have experienced an attack. With such attacks increasing in intensity and scale, these are not risks that any business can afford to take.

However, when it comes to building a recovery and resiliency strategy, many IT leaders still find themselves wondering where they should start. Here, the answer is more straightforward: Such a strategy should start with their data.

Figure 2: NIST Cybersecurity Framework Overview



Source: National Institute of Standards and Technology

The Critical Role of Storage in Enabling Comprehensive Resiliency

The vast majority of cyberattacks such as ransomware target one thing specifically: an organization’s data. Digital data is an organization’s lifeblood, containing everything from intellectual property to confidential customer data, and, without access to trusted data, an organization’s applications and systems cannot run effectively. However, cyberthreats run beyond encrypted data. Increasingly, data is being stolen through exfiltration techniques. Even if this data is encrypted, there is an ongoing risk that it may be decrypted in the future through advanced quantum-based techniques. To address this, IBM continues to stay ahead of emerging threats by employing quantum-safe encryption methods aligned with standards and recommendations from NIST.

Protecting data distributed across geographically dispersed locations and hybrid multicloud environments can also be extremely complex. Compounding the problems is that legacy security toolsets typically focus on one specific part of the environment, so gaining a comprehensive view into the overall environment can be challenging, increasing the risk that something will fall through the gaps.

The data-centric nature of the challenge explains why the storage infrastructure must be central to an organization’s resiliency strategy. Indeed, Omdia research highlights that data protection and primary storage infrastructure are the first- and second-most frequently cited IT elements impacted by ransomware attacks (see Figure 3).[4]

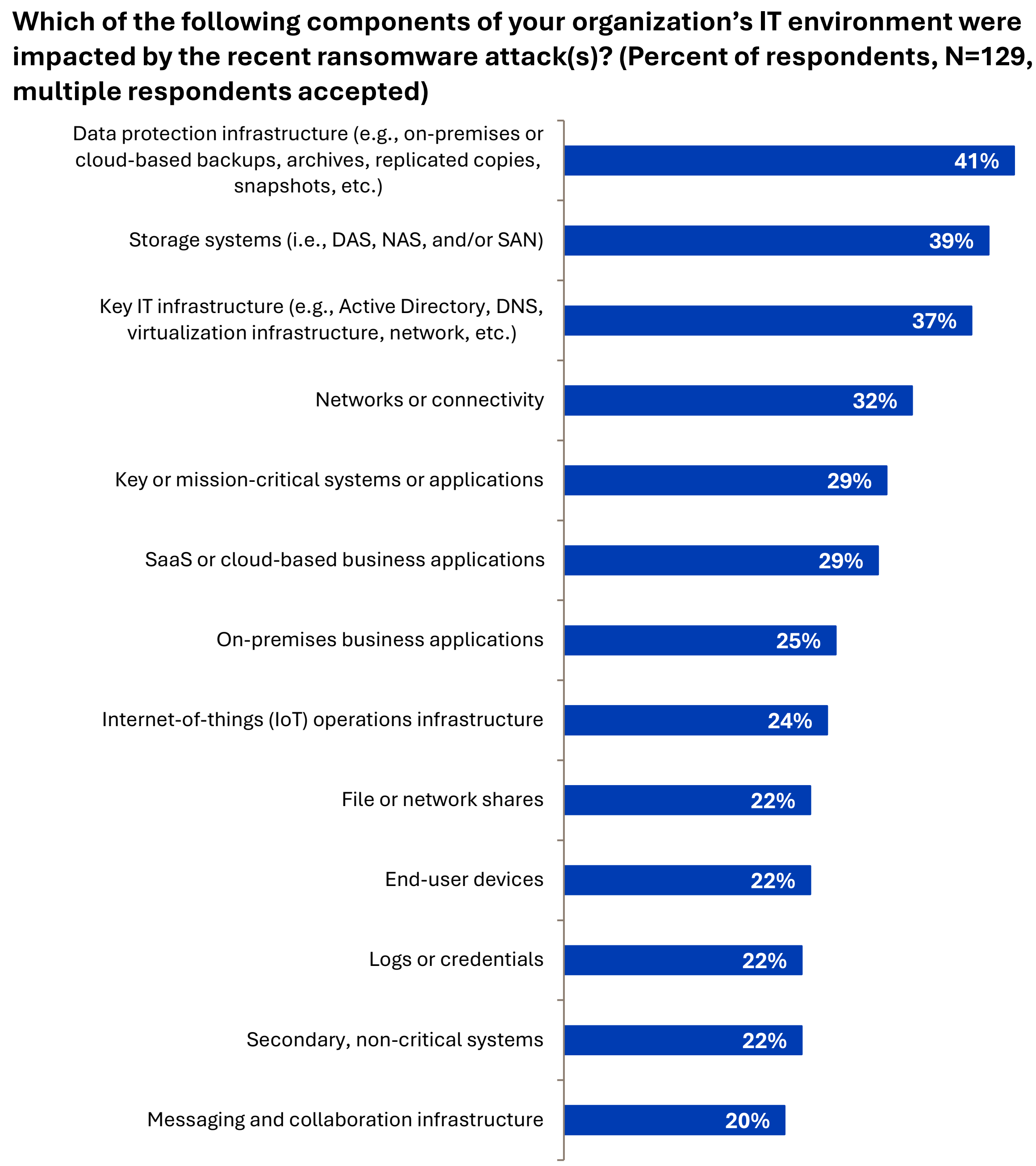
Though the enterprise storage infrastructure has always been central to cyber resiliency, this importance is now increasing further, for a number of reasons:

- Many ransomware attacks specifically target the backup environment because attackers know that a good, clean backup copy is the one thing standing between them and their ransom payment. Accordingly, embedding resilience and detection capabilities within the backup environment is becoming essential. Important capabilities here include the following:
  - Physical and logical air-gapping.
  - Data encryption.
  - Immutable data copies (backups and snapshots).
  - Continuous validation of backups and snapshots.
  - Anomaly/Threat detection capabilities within the backup realm.
- This focus is now extending from the backup environment to the primary storage environment. If organizations can detect unusual I/O activity within the primary storage environment itself, that could indicate a ransomware attack is under way at a very early stage.
- Early detection gives the organization a chance to put processes in place to halt the attack and initiate processes to protect their data to minimize the damage and ensure a more rapid recovery.
- Continuous validation of backups and snapshots ensures that recovery points remain uncompromised, verified, and ready for rapid restoration when required.
- However, none of these aspects work in isolation; they should be connected into an organization's overall management and alerting process to ensure the right protections are put in place in a timely manner.

Consequently, an evolution is taking place that promises to provide organizations with advanced data cyber-resilience capabilities that can both minimize the extent of an attack as well as ensure they can rapidly recover from an attack—or any other business-impacting event—and return to normal business operations as quickly as possible.

[4] Source: Omdia Research Report, *The Ransomware Reality: Cyber Resilience, Data Resilience, and Data Protection*, November 2025.

Figure 3: Components of the IT Environment Impacted by Ransomware Attacks



Source: Omdia

Introducing IBM Storage for Data Resilience

IBM has been a trusted provider and innovator in storage since the dawn of the IT industry, a position that continues with its most recent innovations around data resilience. The company has developed a comprehensive storage and data resilience portfolio, but two innovations are particularly relevant in the context of growing data resiliency challenges: IBM FlashSystem and IBM Storage Defender.

IBM FlashSystem

FlashSystem is IBM's flagship storage system solution, providing high-performance block storage for a range of workloads, including databases, analytics, virtualization, disaster recovery, and data protection.

A key aspect of FlashSystem is that it is built on a resilient architecture, enabling grid-based, zero-downtime data movement, flexible replication and immutable snapshots. However, IBM takes this one step further, as FlashSystem also includes AI-based ransomware detection capabilities that can identify a potential attack.

This is possible because, while FlashSystem supports industry-standard flash drives, it also incorporates IBM's FlashCore Modules (FCM) to deliver advanced protection capabilities. The FCM keeps statistics on every single IOP and summarizes those statistics. The FlashSystem appliance aggregates all the FCMs and passes these summaries to an AI-trained model that is running inside the FlashSystem itself. Every 2 seconds, the model looks at all the data and raises an alert if it discovers a condition that matches patterns for ransomware that it has been trained for. When an alert occurs, these statistics are passed back to IBM Storage Insights where they are then analyzed. Benign statistics are also sent back from each system. By collecting all this data, IBM has been able to retrain models to reduce false positives and test new models. It has been able to reduce the false positive rate to less than 1%, according to IBM.

In this way, the system can detect potential ransomware attacks in less than a minute, at which point the system can automatically trigger an immutable snapshot copy to aid rapid recovery or enable further forensic analysis before restoring operations. Of particular importance is that, as it's being written, this inbound scanning of block data is performed without any impact on performance.

Other notable capabilities of the IBM FlashSystem include the following:

- Immutable and isolated copies ("recovery sets") that cannot be modified or deleted, ensuring rapid and clean recovery.
- Cyber Vault (IBM Power & IBM Z): Advanced methodology combining safeguarded copies with automated analysis and validation for accelerated, trusted recovery.
- Quantum Safe encryption provides a lower risk of data loss along with certified deletion through FCM.
- FlashSystem Policy-based High Availability (PBHA) offers zero RTO and zero RPO for two storage systems in different locations, synchronously replicating data across metro-area distances, allowing concurrent data access for servers in each data center, providing seamless failover, and boosting disaster recovery over greater distances with asynchronous replication across regions.
- Guarantees: Guaranteed detection of potential risks in under a minute, safeguarding the integrity of an organization's data and enabling the recovery of secured copies within 60 seconds.
  - FlashSystem guaranteed detection and alerting on ransomware threats in less than a minute.
  - Reduced downtime with near-immediate access to uncorrupted backups from known good air-gapped snapshots in under a minute.

IBM Storage Defender

IBM Storage Defender is a software solution designed to keep organizations' data safe and workloads continuously available, with robust resilience and compliance capabilities, AI-driven threat detection, and fast, trusted recovery. Built to simplify protection across the storage estate, it provides unified visibility and orchestration for modern hybrid and multicloud environments, helping organizations safeguard critical data against cyberattacks, operational failures, and unforeseen catastrophic events. It enables businesses to detect anomalies early, contain threats, and rapidly restore operations with confidence while maintaining compliance with evolving regulatory requirements.

IBM Storage Defender delivers three core capabilities:

Data Resilience and Compliance

- Always know the location and status of your backups and copies, including the validated ones available for recovery.
- Use robust security features to protect your data and help address data compliance requirements.

- Gain scalability and flexibility to integrate with existing storage infrastructure and multicloud deployments.

Early Threat Detection

- Use advanced AI and ML algorithms to identify data anomalies faster, including zero-day vulnerabilities and other sophisticated attacks.
- Rapidly engage your security operations team when anomalies are detected through integration with SIEM tools such as IBM QRadar and Splunk.
- Synchronize hardware and software detection to identify attacks that may evade a single layer of protection.

Safe and Fast Recovery

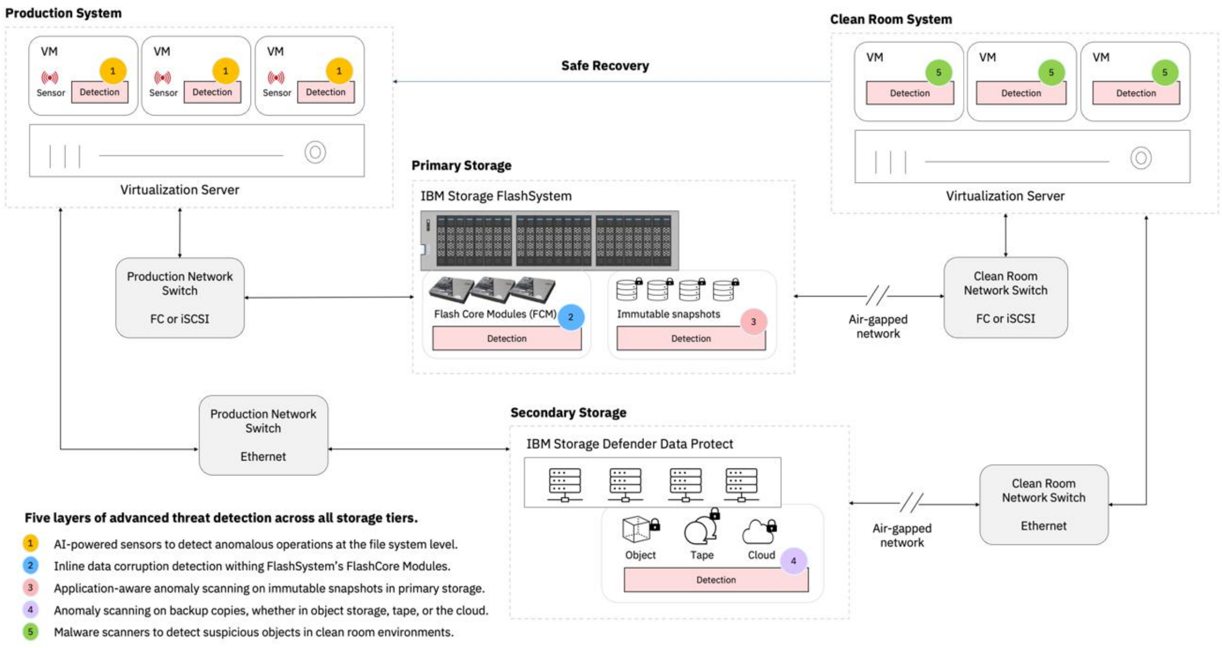
- Leverage validated immutable backups, hardware snapshots, and orchestrated recovery workflows that connect storage and security teams.
- Enable support for a clean room to conduct forensic investigations following an attack before data is restored to production.
- Restore critical business operations with an architecture that enables parallel recovery across nodes to accelerate restoration.

Combining IBM FlashSystem and Storage Defender for End-to-end Cyber-resilience

While both IBM FlashSystem and Storage Defender provide compelling value when deployed standalone, this value can increase further when the two are paired together. FlashSystem arrays can be combined with IBM Storage Defender to create protection groups that include specific volumes, which can then be backed up according to user-defined policies. Data can be restored or recovered to multiple target locations, including new locations, when recovering from a cyberattack. Snapshot copies can also be replicated to another cluster for an additional layer of protection.

This combined approach delivers five layers of advanced threat detection across all storage tiers, delivering a comprehensive defense against ransomware and other sophisticated attacks (see Figure 4).

Figure 4: IBM Storage for Data Resilience


Production System
VM
1
Sensor
Detection
VM
1
Sensor
Detection
VM
1
Sensor
Detection
Virtualization Server
Safe Recovery
Clean Room System
VM
5
Detection
VM
5
Detection
VM
5
Detection
Virtualization Server
Primary Storage
IBM Storage FlashSystem
Flash Core Modules (FCM)
2
Detection
Immutable snapshots
3
Detection
Production Network Switch
FC or iSCSI
Air-gapped network
Clean Room Network Switch
FC or iSCSI
Production Network Switch
Ethernet
Secondary Storage
IBM Storage Defender Data Protect
Object
Tape
Cloud
4
Detection
Air-gapped network
Clean Room Network Switch
Ethernet
Five layers of advanced threat detection across all storage tiers.
1 AI-powered sensors to detect anomalous operations at the file system level.
2 Inline data corruption detection withing FlashSystem's FlashCore Modules.
3 Application-aware anomaly scanning on immutable snapshots in primary storage.
4 Anomaly scanning on backup copies, whether in object storage, tape, or the cloud.
5 Malware scanners to detect suspicious objects in clean room environments.

Source: IBM

Additionally, settings enable admins to automate the creation of immutable snapshots, which are cyber-resilient point-in-time volume copies that cannot be changed or deleted through user error or malicious action or a ransomware attack. As part of this ecosystem, IBM Storage Defender Sentinel enhances these capabilities with AI-driven validation and anomaly detection, helping identify and isolate corrupted backups before recovery to ensure trusted, verified recovery points. Such isolation of backup copies from production data can help accelerate data recovery following an attack.

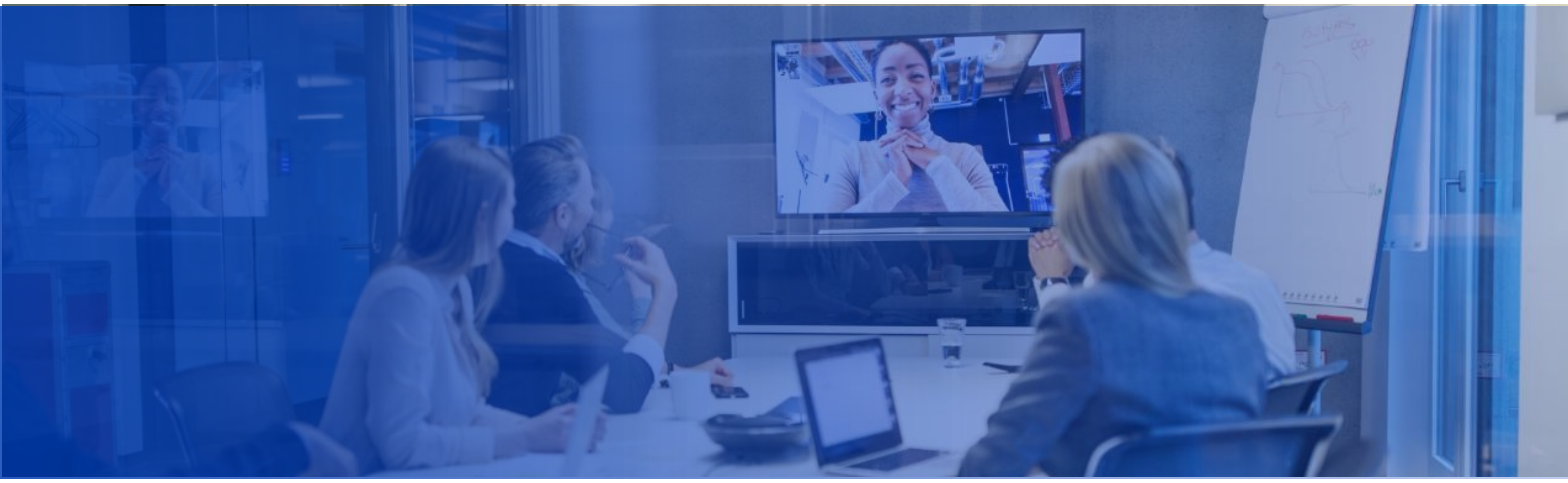
Working in this way, organizations can build a complete solution for data resilience, with FlashSystem providing a smart and resilient foundation and Defender providing the intelligence and orchestration for rapid operational resilience. In this way, IT teams can create a multi-layered and integrated—rather than a piecemeal—resilience approach to boost recovery times and enable the business to return to normal operations as quickly as possible.

Moreover, organizations are able to move to a more proactive stance for resilient, real-time threat detection capabilities, utilizing Defender's software sensors with FlashSystem's inline corruption detection. Recovery times are further enhanced through restoring directly from FlashSystem via SAN, rather than over the network, while the proactive creation of immutable snapshots when potential attacks are detected further supports offline investigation and clean recovery. Crucially, all of these capabilities can be unified under a single platform, achieving consistent recovery capabilities across a wide range of critical applications, including Oracle, SAP HANA, VMware, and Epic.

Additional Data and Storage Resiliency Capabilities

With its extensive experience in cybersecurity and risk management, IBM is a recognized leader in cyber resilience and offers a comprehensive suite of advanced storage and data protection solutions across a broad range of infrastructure architectures, platforms, and technologies. Some of these include the following:

- **IBM Storage DS8000:** Mission-critical protection and resilience across mainframe environments.
- **IBM Tape:** Air-gapped, immutable data protection for bulk offline storage and archives.
- **IBM Fusion:** Extends IBM's resilience approach to hyperconverged infrastructure environments, including virtual machines and cloud-native applications.



Conclusion

The relentless rise in cyberattacks is precipitating some foundational shifts in the way IT and business leaders think about protecting their organizations, particularly from malicious actors. There's a growing realization that merely focusing on keeping the bad guys out is insufficient and, just as with more traditional forms of disaster recovery, the need to quickly and efficiently recover the business when a bad actor eventually gets lucky is increasingly critical.

With data being the primary target for many attacks, especially ransomware, an organization's cyber-resiliency strategy must include a comprehensive, data-centric approach that ensures early detection, minimizes damage, and enables rapid restoration of operations. In this regard, IBM's broad storage and resilience portfolio, **FlashSystem** and **Storage Defender** solutions in particular, are purpose-built to address these challenges, offering a robust foundation for resilience. Together, these solutions empower businesses to not only withstand attacks but also recover rapidly, minimizing downtime and financial losses.

For both IT and business leaders, resilience is no longer optional; it's a business imperative. IBM's integrated approach ensures organizations can detect threats early, isolate compromised data, and restore operations quickly, safeguarding both their reputation and bottom line. By prioritizing resilience and leveraging IBM's AI-enabled advanced technologies, businesses can confidently navigate the evolving threat landscape, ensuring continuity and stability in the face of even the most sophisticated cyberattacks.

For more information about IBM's storage resiliency capabilities, including Storage Defender and IBM FlashSystem, please visit https://www.ibm.com/products/flashsystem.

Appendix

Methodology

A combination of Omdia and Enterprise Strategy Group (now Omdia) research, vendor-provided material, and public and industry knowledge was used to develop this paper and come to its conclusions. The research included in this paper consisted of multiple online surveys of IT leaders and decision-makers.

Simon Robinson, Principal Analyst, Storage and Converged Infrastructure
askananalyst@omdia.com

Omdia consulting

Omdia is a market-leading data, research, and consulting business focused on helping digital service providers, technology companies, and enterprise decision makers thrive in the connected digital economy. Through our global base of analysts, we offer expert analysis and strategic insight across the IT, telecoms, and media industries.

We create business advantage for our customers by providing actionable insight to support business planning, product development, and go-to-market initiatives.

Our unique combination of authoritative data, market analysis, and vertical industry expertise is designed to empower decision-making, helping our clients profit from new technologies and capitalize on evolving business models.

Omdia is part of Informa TechTarget, a B2B information services business serving the technology, media, and telecoms sector. The Informa group is listed on the London Stock Exchange.

We hope that this analysis will help you make informed and imaginative business decisions. If you have further requirements, Omdia's consulting team may be able to help your company identify future trends and opportunities.

Get in touch

www.omdia.com
askananalyst@omdia.com

Copyright notice and disclaimer

The Omdia research, data, and information referenced herein (the "Omdia Materials") are the copyrighted property of TechTarget, Inc. and its subsidiaries or affiliates (together "Informa TechTarget") or its third-party data providers and represent data, research, opinions, or viewpoints published by Informa TechTarget and are not representations of fact.

The Omdia Materials reflect information and opinions from the original publication date and not from the date of this document. The information and opinions expressed in the Omdia Materials are subject to change without notice, and Informa TechTarget does not have any duty or responsibility to update the Omdia Materials or this publication as a result.

Omdia Materials are delivered on an "as-is" and "as-available" basis. No representation or warranty, express or implied, is made as to the fairness, accuracy, completeness, or correctness of the information, opinions, and conclusions contained in Omdia Materials.

To the maximum extent permitted by law, Informa TechTarget and its affiliates, officers, directors, employees, agents, and third-party data providers disclaim any liability (including, without limitation, any liability arising from fault or negligence) as to the accuracy or completeness or use of the Omdia Materials. Informa TechTarget will not, under any circumstance whatsoever, be liable for any trading, investment, commercial, or other decisions based on or made in reliance of the Omdia Materials.