SHOWCASE

Omdia by informa techtarget

MARCH 2026

Achieving Cyber Resilience With Actionable Data Intelligence

Todd Thiemann, Principal Analyst

Abstract: As enterprises accelerate AI adoption, securing and governing distributed data across on-premises and cloud environments has become mission-critical. IT and security leaders must stay resilient against cyberattacks like ransomware and meet compliance requirements. However, they often can't assess risk quickly or accurately because they lack visibility into where sensitive data lives and what it contains. CIOs, CISOs, CDOs, and CROs (Chief Risk Officers) need to come together to address these AI adoption-related risks and the subsequent security risks that emerge. The combination of Cohesity Data Cloud for data protection and Cyera's Data and AI Security Platform enables organizations to leverage best-in-class platforms to gain the data intelligence and risk context needed for streamlined, automated, and comprehensive cyber resilience for the AI era.

Scaling Cyber Resilience – The Data Visibility Quandary

Sensitive data lives across the enterprise, and IT and security teams need to understand where their sensitive data lives in order to secure it and maintain compliance with external regulatory regimes and internal data governance requirements.

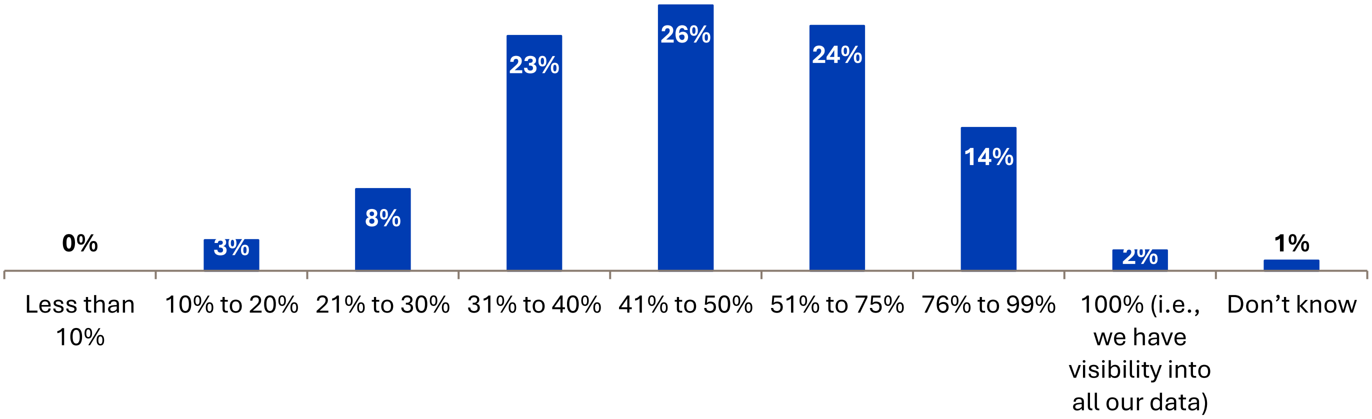
The challenge for most organizations is that the entirety of an organization's data estate is often unknown and poorly governed. IT teams, in particular, have to make backup decisions without adequate context around the data and often operate in a silo separate from their security counterparts. This creates dangerous gaps that attackers are eager to exploit. This risk grows rapidly as enterprises rush to adopt AI, which can act on sensitive data, raising the stakes for both data security and cyber resilience initiatives.

Enterprise Strategy Group (now Omdia) research found that 60% of enterprises lack visibility into at least half of their data estate (see Figure 1).[1] Visibility, delivered through data discovery and classification, is a prerequisite to avoid sensitive data loss, and prove cyber resilience to regulators and boardrooms.

[1] Source: Enterprise Strategy Group (now Omdia) Research Report, *Reinventing Data Loss Prevention: Adapting Data Security to the Generative AI Era*, May 2025.

Figure 1. Enterprises Lack Visibility Into Their Data Estates

Approximately what percentage of your organization's data do you believe your organization has visibility into (i.e., it has been both discovered and classified)? (Percent of respondents, N=370)



Source: Omdia

Cyber resilience initiatives typically involve IT and security teams that share common goals in identifying and protecting sensitive data. Enterprise Strategy Group (now Omdia) research found that the top four business drivers behind these initiatives were improving cyber resilience efforts (37%), improving data security posture (37%), reducing business risk (34%), and complying with data privacy and data protection laws (31%).[2] Those drivers affect critical business outcomes and stakeholders across the entire enterprise.

Cyber resilience is now everyone's responsibility—from executives to frontline practitioners. Security and IT teams have a shared interest in optimizing data security and cyber resilience, but often come from slightly different vantage points, and the two often act in silos. IT teams want to better protect sensitive data, recover it faster, and meet compliance requirements—while doing so cost-effectively. Security teams share these goals, but they also need the visibility and context to assess and reduce risk and to respond proactively to incidents.

Collaboration between the teams is imperative for optimal cyber resilience and data security posture that provides for the most efficient use of resources during recovery operations.

Streamlining Data Security and Protection

Security and IT operations teams struggle to answer critical questions, such as:

- What assets contain sensitive data that require priority protection?
- What mission critical data should be recovered first during incident response?
- Where is regulated and proprietary data located? How is it being protected?

[2] Source: Enterprise Strategy Group (now Omdia) Research Report, *Achieving Cyber and Data Resilience: The Intersection of Data Security Posture Management With Data Protection and Governance*, September 2024.

- Does protected data comply with data sovereignty requirements? Which data is subject to compliance policies and shouldn't be recovered to certain locations?
- How can we optimize costs by eliminating or vaulting redundant, obsolete, and trivial (ROT) data?

It is no surprise that 34% of research respondents reported that one of the most valuable lessons their organization learned or improvements it made following a recent ransomware attack was implementing better data classification and protection measures.[3]

The lack of context around sensitive data is a major component for achieving cyber resilience. A recovery without the correct visibility and understanding of protected data can prevent organizations from confidently and quickly bouncing back. For example, backup admins can see storage assets but do not know the criticality of the data or cannot align protection policies with data sensitivity. Existing "one-size-fits-all" service-level agreements can waste resources on low-value data and prevent the recovery of mission-critical data for minimum viability.

Compounding the low-value data dynamic is redundant, obsolete, and trivial (ROT) data protection. Identifying ROT data and excluding it from a data protection plan can avoid unnecessary overhead and costs, lowering total cost of operations and ensuring high-value data is protected.

Compliance and data sovereignty risk pose challenges for organizations with the current tools they have in place. GDPR and regional regulations frequently require data location awareness. The risk of backing up or sending recovered data to a non-compliant region may violate regulatory obligations. For example, storing EU data outside of Europe can invite regulatory scrutiny and costly fines.

In the event of a security incident, data needs to be recovered as quickly as possible. Inefficient recovery without a good understanding of what is the most critical data for your organization to be operational can delay that recovery. If the team lacks this visibility, the organization can end up wasting time and resources, instead of getting the "minimum viable company" operational.

Enterprises also face security and exfiltration risks within their backup environments. Adversaries know backup platforms hold an organization's crown-jewel data and may be the last line of defense against paying a ransom. As a result, they target these platforms for encryption and data exfiltration. Unencrypted sensitive data and excessive ROT data in backups can create unnecessary exposure, and accidental recovery of sensitive data into the wrong environment can result in a data breach, regulatory scrutiny and fines.

Cohesity and Cyera Unify Data Intelligence, Security, and Recovery

The Cyera and Cohesity partnership delivers end-to-end governance across data security and cyber resilience workflows. Cyera's Data and AI Security Platform autonomously discovers, classifies, and provides context around sensitive and critical data with real-time policy enforcement and proactive remediation, including data accessed by AI tools and agents. This actionable data intelligence flows seamlessly into Cohesity Data Cloud and enables IT teams to ensure secure, immutable, recoverable secondary data. Cyera's data context and access risk scores inform Cohesity's protection policies. On the flip side, Cohesity's

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

cyber recovery capabilities integrate with Cyera's data intelligence, enabling customers to validate data integrity, detect anomalies post-recovery, and provide recovery evidence to maintain compliance.

Combining Cyera's Data Security Posture Management (DSPM) and the Cohesity Data Cloud enables enterprises to confidently address data security and cyber resilience in the face of cyberthreats and growing AI adoption.

- **Speed:** In terms of speed of deployment, Cyera AI-native DSPM can be deployed to scan and classify large volumes with 95% precision, showing results and driving value in just a few hours or days, rather than weeks or months. Cohesity's hyperconverged architecture and file system means protected data can be backed up and recovered at a speed that is unmatched.
- **Scale:** Both Cyera and Cohesity are built to handle the largest enterprise environments, whether in the form of scanning petabytes of data or migrating thousands of virtual machines.
- **Secure:** Cyera's classification engine identifies all sensitive and proprietary data and prioritizes the highest risk by automatically correlating data sensitivity with identities, access, exposure conditions, and business associations. Cohesity's built-in security capabilities mean protected data is immutable and durable, ensuring clean recoveries. AI-powered threat scanning and ransomware anomaly detection combined with air-gapped cyber vaulting means that organizations can be confident that a secure recovery is always in reach.
- **Savings:** The combination of Cyera and Cohesity helps CIOs and CISOs optimize and justify their spending and ensure they are extracting maximum value. Organizations can seamlessly combine the two platforms to eliminate the cost of ROT data while also helping teams achieve cost risk avoidance by understanding where their crown jewel data is located and efficiently protect it.

Combining Cohesity data protection with Cyera's DSPM enables comprehensive cyber resilience from data discovery to data protection to rapid recovery.

A Future-ready Approach to Securing Data for Cyber Resilience

Data context is a core requirement for effective cyber resilience. Valuable and sensitive data remaining neglected or unknown should set off alarm bells with CIOs, CDOs, CROs, and CISOs alike, especially as AI and agents expand the attack surface for cyberthreats and increase data exposure risks. Optimizing for cyber resilience requires having end-to-end data security posture management and cyber resilience to protect the entire data estate.

Organizations can't secure what they don't know they have, and they cannot optimize data security and cyber resilience if they don't understand the nature of their data. Cyera delivers visibility and rich context across all the places your data lives, while Cohesity provides optimal data protection and clean, reliable recovery. This partnership and joint solution enables teams to streamline data security and data protection operations efficiently and cost-effectively in the face of daunting cyberthreats and the increasing pressure to rapidly adopt AI.

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.

Get in touch: www.omdia.com askananalyst@omdia.com