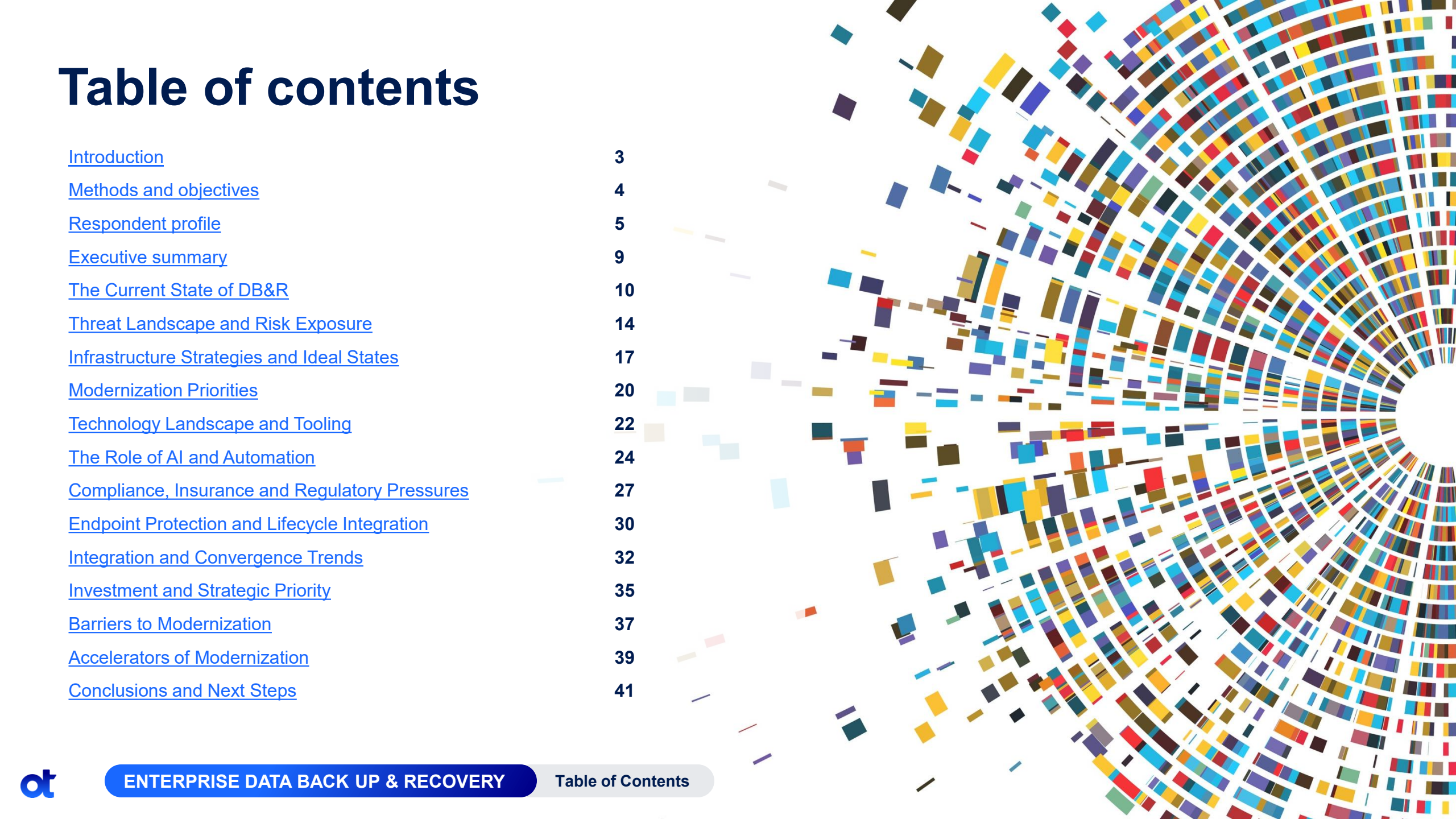
From Backup to Breakthrough: Modernizing Enterprise Data Resilience

What the data tells us

FOUNDRY

opentext™

Table of contents



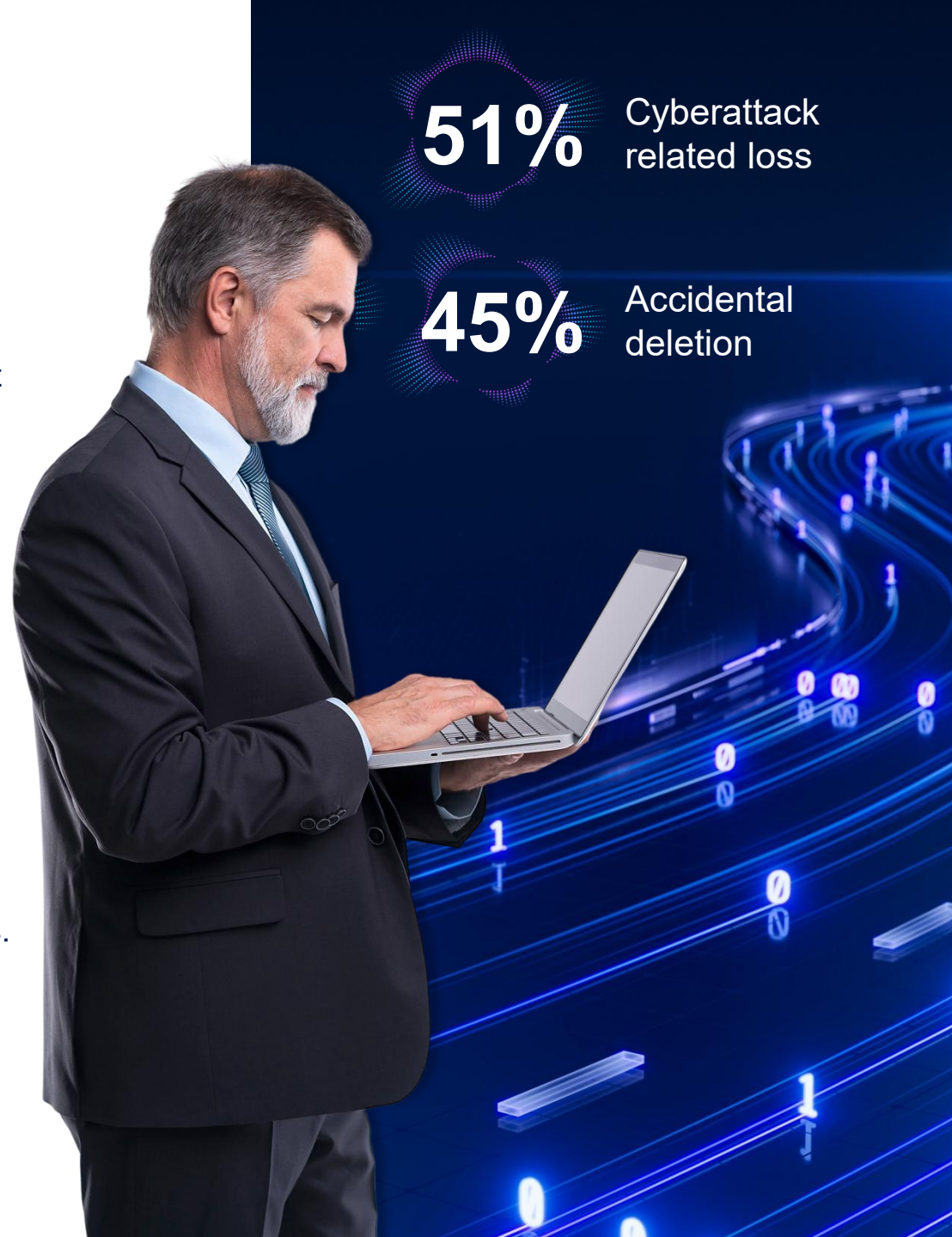
Introduction

Organizations face growing challenges in protecting data across endpoints, on-premises, hybrid, and cloud environments.

While coverage is strong in traditional systems, critical gaps remain for modern workloads like virtual machines and containers. Despite high confidence in current strategies, frequent incidents from ransomware, cyberattacks, and accidental deletion expose vulnerabilities that lead to downtime, data loss, and increased IT strain.

Meeting today's resilience expectations requires more than backup. Average recovery time objectives remain at nine hours, with few organizations achieving rapid sub-three-hour recovery. Compliance mandates, insurance requirements, and the complexity of managing hybrid and multi-cloud environments add additional pressure, making it clear that incremental improvements are no longer enough.

OpenText helps organizations close these gaps by delivering holistic resilience. With AI-driven features such as anomaly detection, predictive analytics, and automated recovery, OpenText strengthens protection for modern workloads, simplifies hybrid and multi-cloud management, and ensures compliance readiness. By moving beyond backup to an integrated approach that unites data protection, security, and threat detection, OpenText empowers enterprises to stay ahead of evolving risks with confidence.

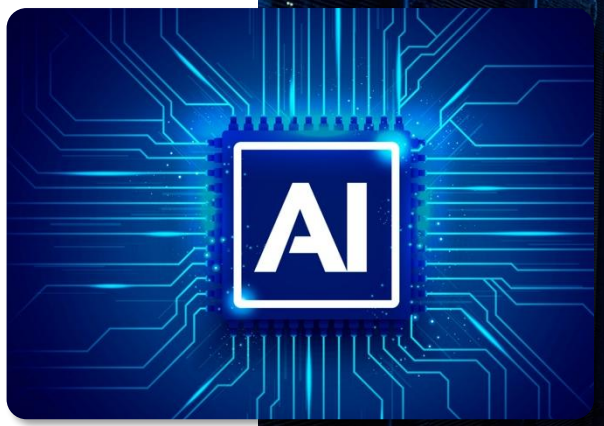


Method and Objectives

Survey goals

- Assess the current state of enterprise Data Backup & Recovery (DB&R) strategies across large organizations (1,000+ employees).
- Identify key coverage areas, confidence levels, and blind spots in backup and recovery environments.
- Understand top threats, pain points, and modernization challenges faced by IT and security leaders.
- Explore the role of AI, automation, compliance, and insurance in shaping DB&R priorities.
- Highlight opportunities for vendors, like OpenText, to address unmet needs in resilience, integration, and multi-cloud complexity.

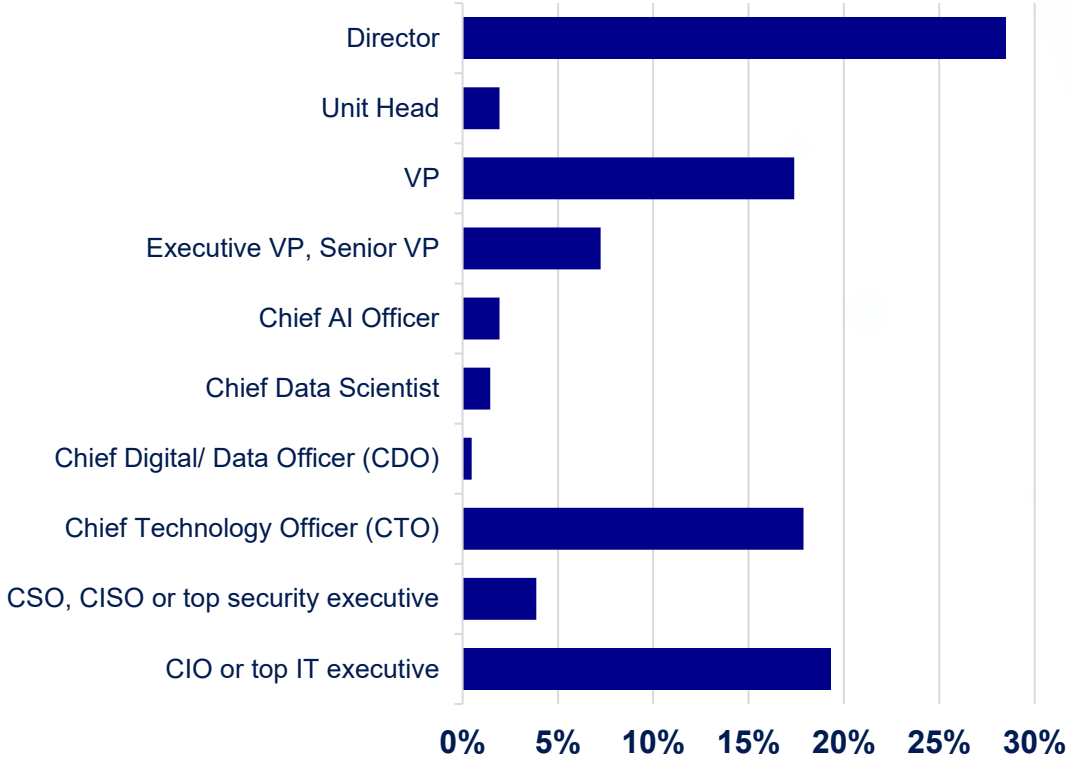
Total respondents	N 207, US 82, UK 61, SG 21, ANZ 21, IN 22
Collection Method	Online questionnaire
Target Company	Companies with 1,000 or more employees
IT Decision makers	Director and above titles in IT / Networking / Security
Number of questions	20 excluding screeners and firmographics
Field dates	August 11 September 14, 2025



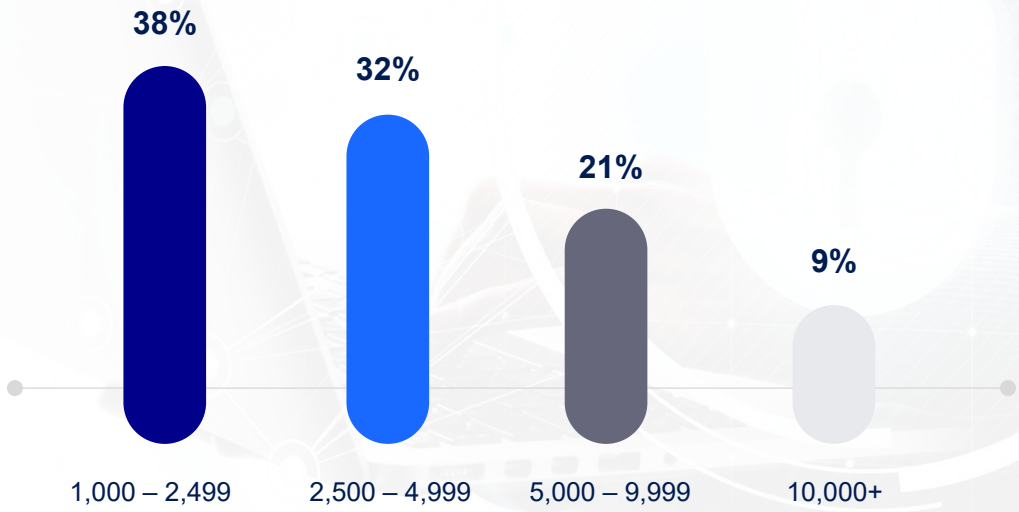
Respondent profile

Role and Company Size

Functional Role



Company Size (Employees)



Top 10 Industries

Manufacturing
ex. Computers and electronics
8%

Software and Internet
8%

Consumer Packaged Goods Manufacturing
7%

Financial Services
ex. Insurance
6%

Banking
Retail, Private or Commercial
5%

Professional Services
5%

Oil and Gas, Other
5%

Retail
5%

Telecommunications
4%

Healthcare
4%

Executive Summary

Summary of Findings

Current State and Gaps

- Organizations report strong DB&R coverage for endpoints and on-prem, but coverage lags for virtual machines (56%) and containers (53%).
- Confidence is high (97% somewhat/very confident), but frequent incidents show gaps: 51% faced cyberattack-related loss, 45% accidental deletion.
- Cyberattacks/ransomware (55%) and cloud data loss (41%) are top concerns; downtime and IT resource constraints are also significant concerns.

Priorities and Future Direction

- Hybrid dominates today (78%) but 32% say current setups aren't "ideal" — organizations want simplified paths to cloud-first or streamlined hybrid.
- AI adoption is mainstream: 93% actively using or piloting, with anomaly detection, incident response, and predictive failure analysis all seen as highly valuable.
- Compliance pressures are strong: insurance mandates (72%) and regulatory requirements (64%) drive DB&R strategies, but 80% find compliance challenging.
- Modernization accelerators include access to AI/automation (43%), compliance guidance (41%), and simplified integration with legacy systems (41%).

***93%** actively using or piloting AI*

The Current State of DB&R

How Enterprises Are Managing Backup and Recovery Today

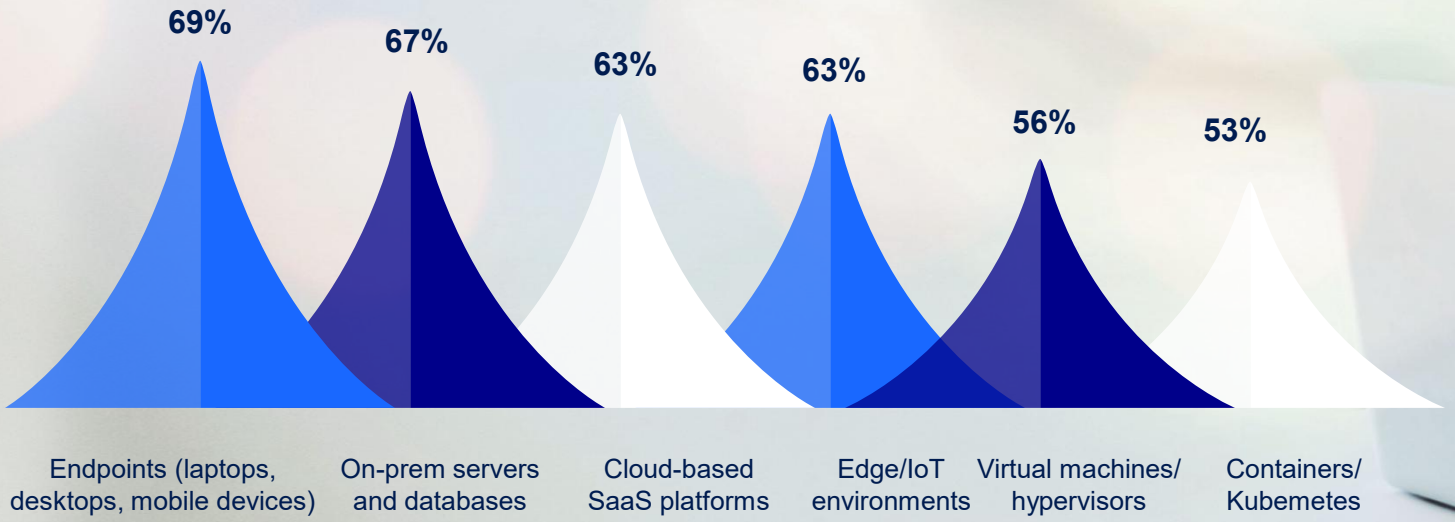
The Current State of DB&R

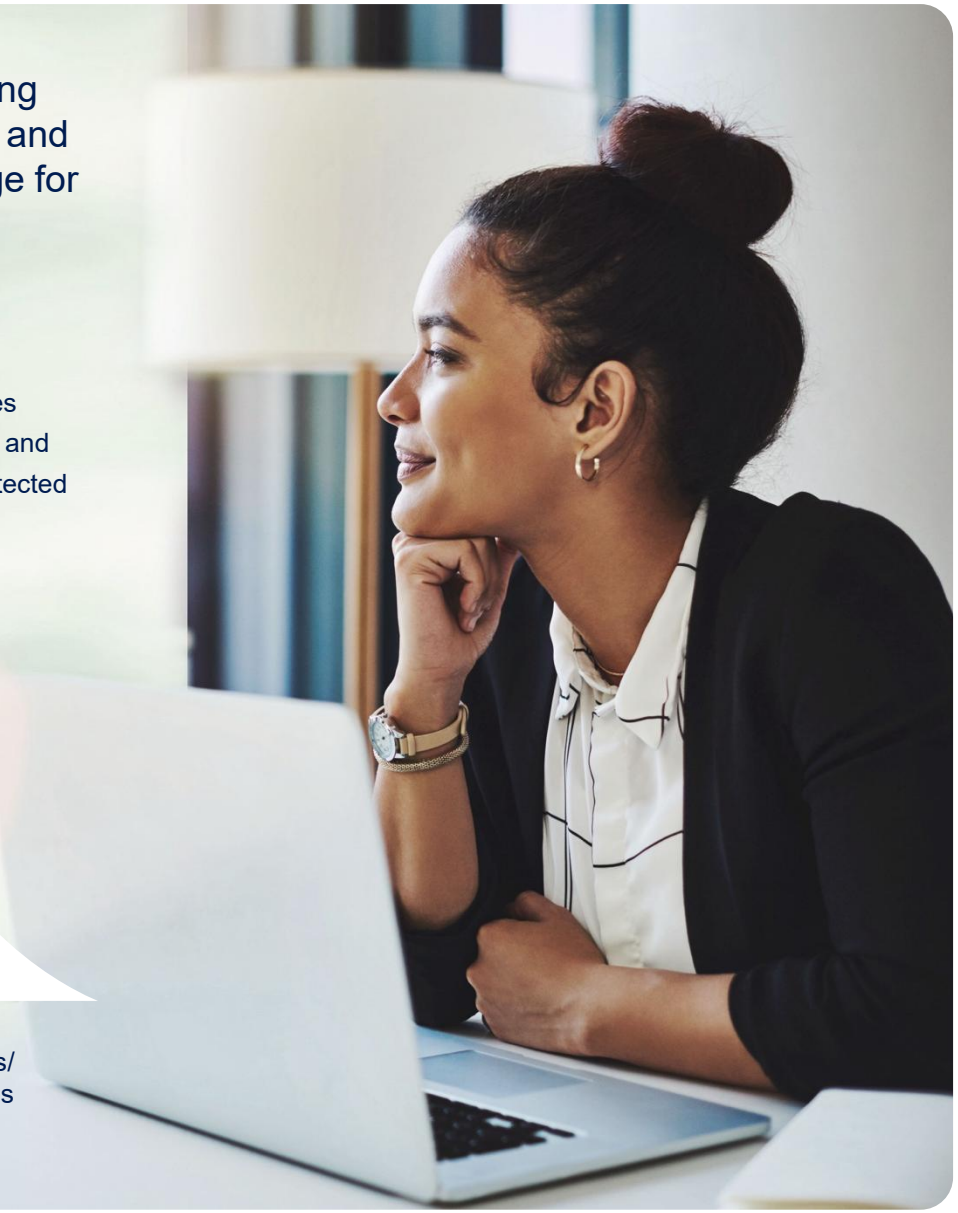
How Enterprises Are Managing Backup and Recovery Today

Most organizations report strong DB&R coverage for endpoints and on-prem systems, but coverage for virtual and containerized environments lags behind.

Current backup and recovery strategy cover the following areas (Fully Covered)

Coverage drops to just over half for virtual machines (56%) and containers/Kubernetes (53%), signaling that modern, cloud-native and containerized workloads remain under protected compared to traditional systems

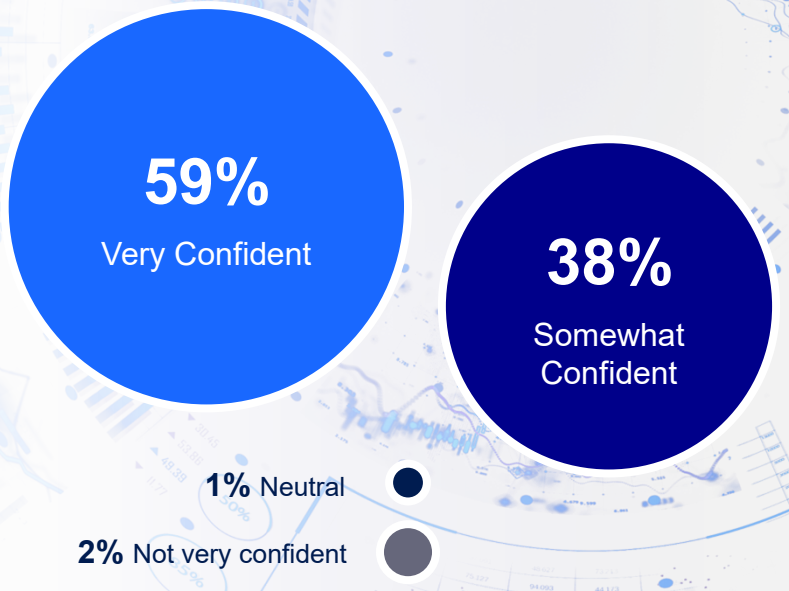




The Current State of DB&R

How Enterprises Are Managing Backup and Recovery Today

Confidence in current backup and recovery strategy



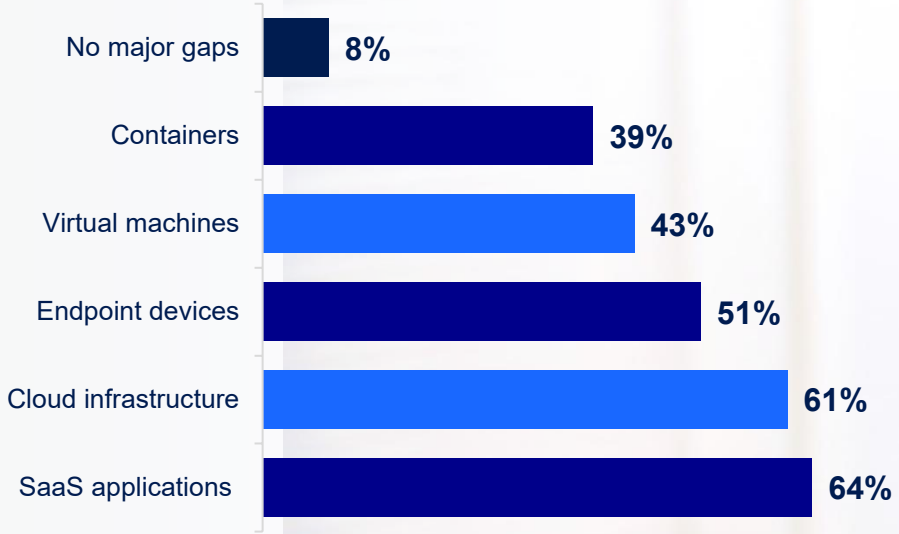
97% of organizations are feeling at least somewhat confident in their current backup, and recovery strategies

The two in five who are not highly confident shows an opening for vendors like OpenText to position advanced reliability, automation, and resilience features to eliminate lingering doubts

The Current State of DB&R

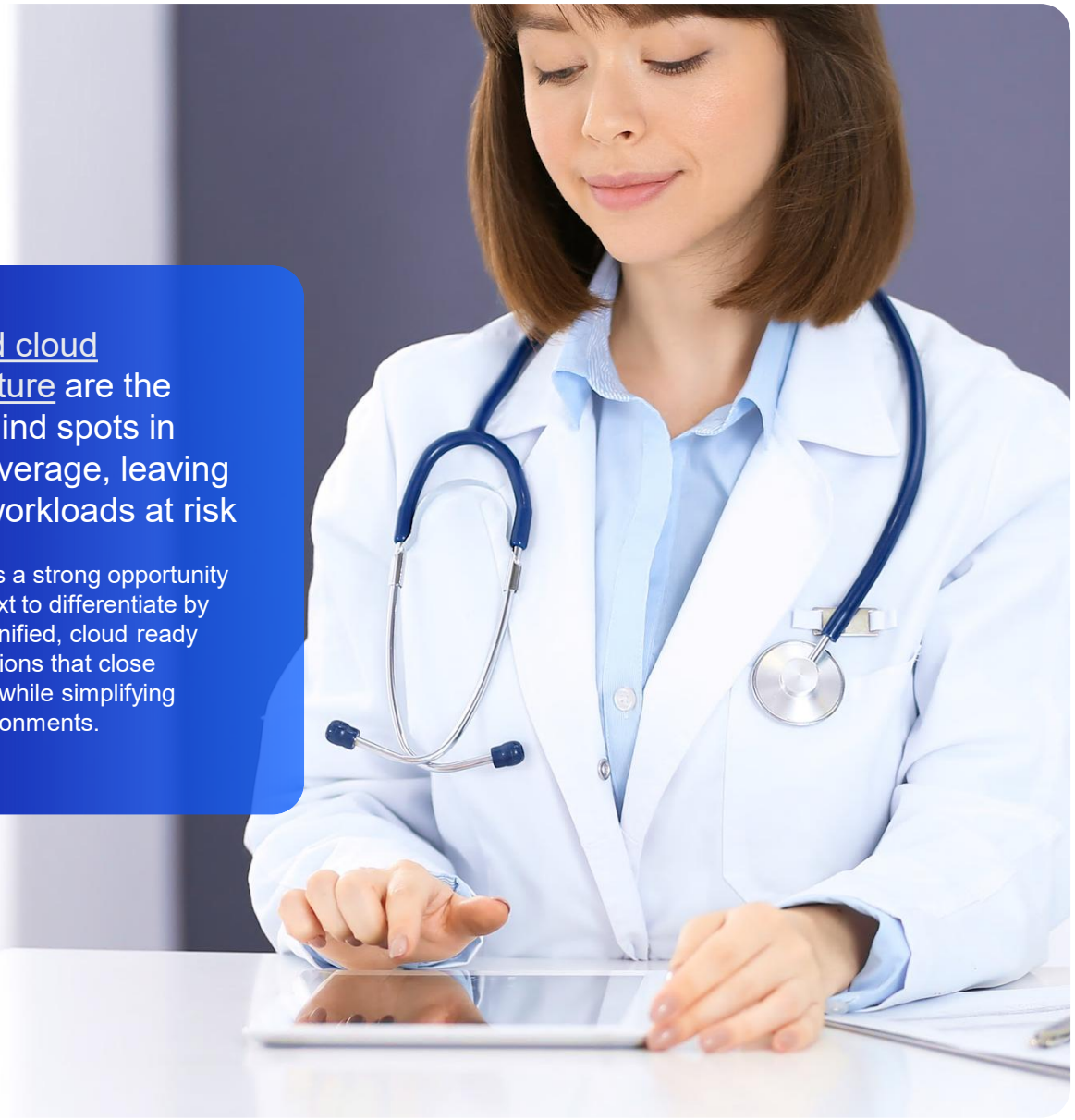
How Enterprises Are Managing Backup and Recovery Today

Gaps or blind spots in current DB&R coverage



SaaS and cloud infrastructure are the biggest blind spots in DB&R coverage, leaving modern workloads at risk

This creates a strong opportunity for OpenText to differentiate by delivering unified, cloud ready DB&R solutions that close these gaps while simplifying hybrid environments.

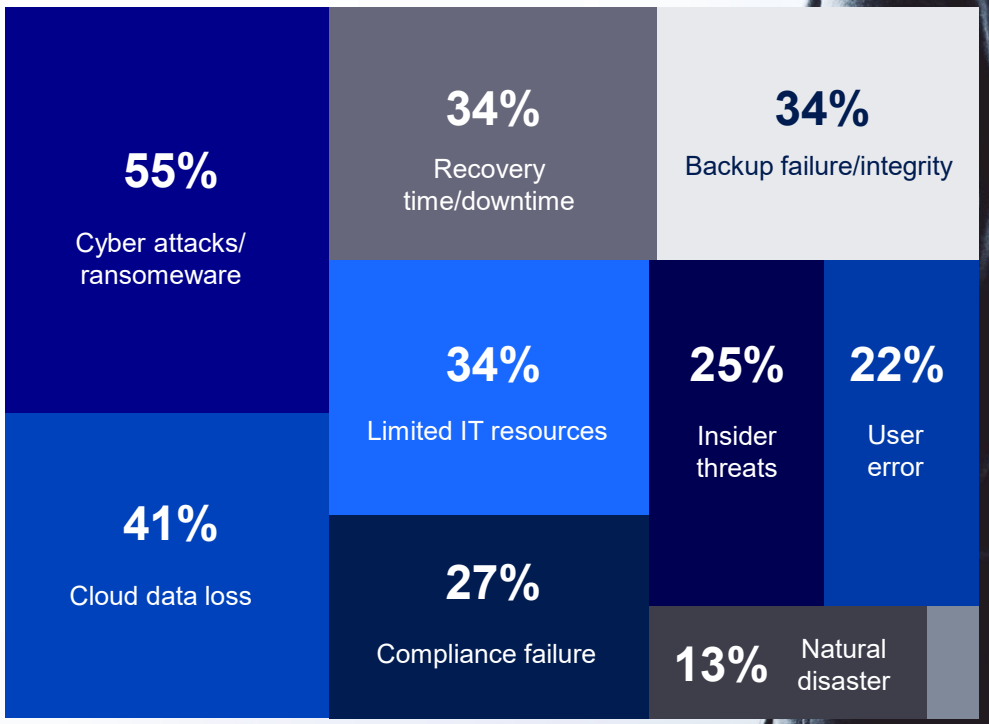


Threat Landscape and Risk Exposure

The Realities of Data Loss and Cyber Threats

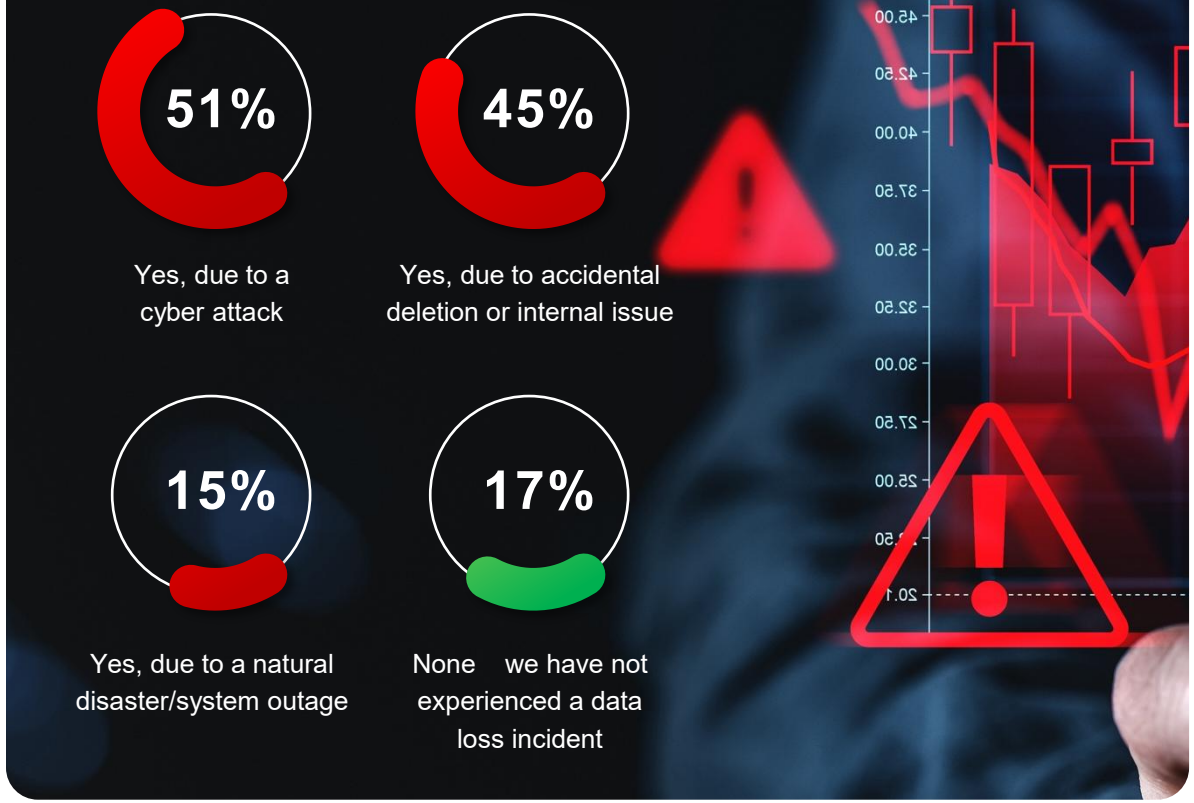
Threat Landscape and Risk Exposure
The Realities of Data Loss and Cyber Threats

Top concerns when it comes to backup and recovery



Has your organization experienced a data loss incident in the past 12 months?

Most organizations faced data loss in the past year, with cyberattacks and accidental deletion driving the majority of incidents.



Threat Landscape and Risk Exposure
The Realities of Data Loss and Cyber Threats

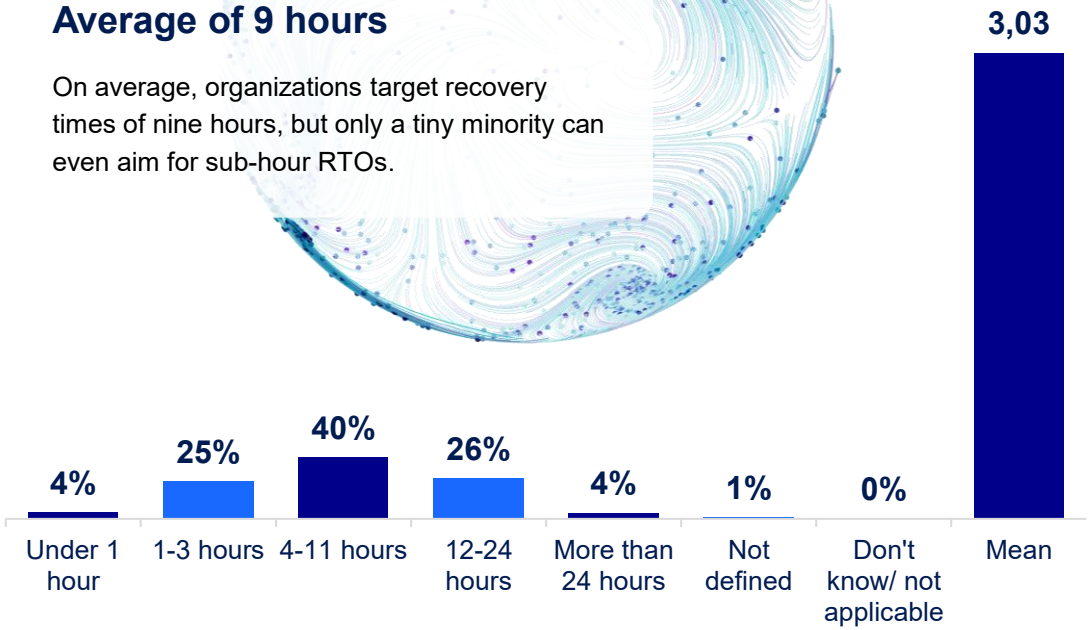
Insight:

The relatively lower concern for accidental deletion (22%) and natural disasters (13%) shows that IT leaders are prioritizing modern digital risks over traditional ones — underscoring a key opportunity for vendors to emphasize ransomware resilience, cloud protection, and faster recovery capabilities

Typical recovery time objective (RTO) for mission-critical data and applications

Average of 9 hours

On average, organizations target recovery times of nine hours, but only a tiny minority can even aim for sub-hour RTOs.



Infrastructure Strategies and Ideal States

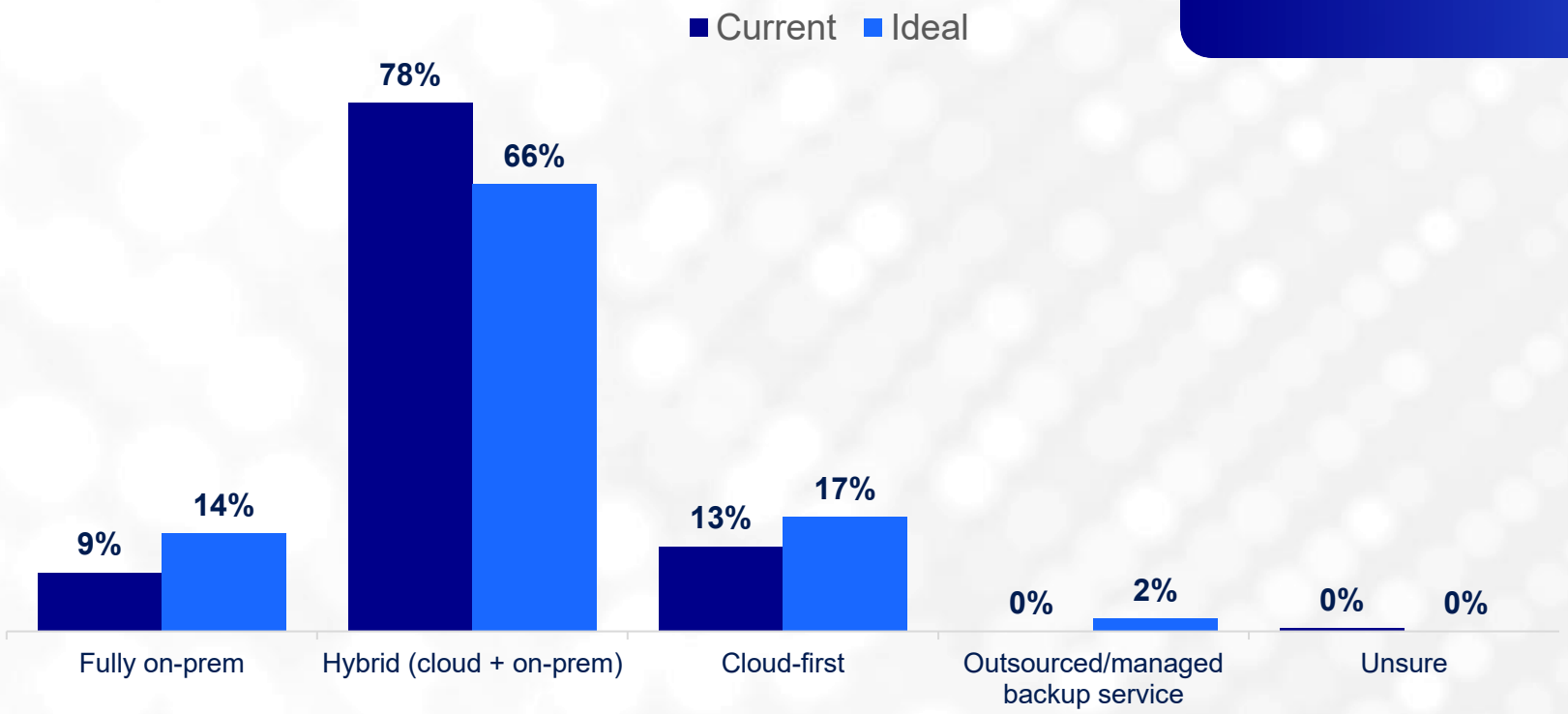
How Organizations Structure — and Want to Evolve — Their Backup Environments

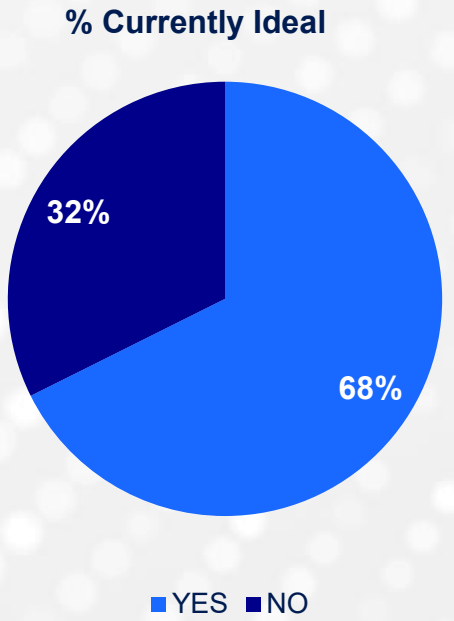
Infrastructure Strategies and Ideal States
How Organizations Structure — and Want to Evolve — Their Backup Environments

Hybrid cloud + on prem remains the dominant backup model, but a third of organizations say their current setup doesn't yet match their ideal.

While 78% currently operate in a hybrid model, only 66% see it as their ideal, suggesting some want to simplify toward cloud first (17%) or fully on prem (14%). With 32% not yet at their currently ideal state, vendors can position offerings that ease hybrid complexity and accelerate cloud first transitions meeting enterprises where they are while guiding them to where they want to be.

Current vs. Ideal backup infrastructure

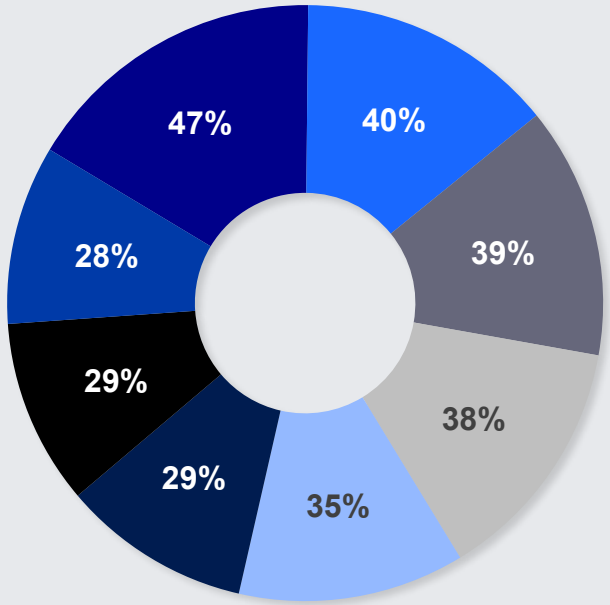




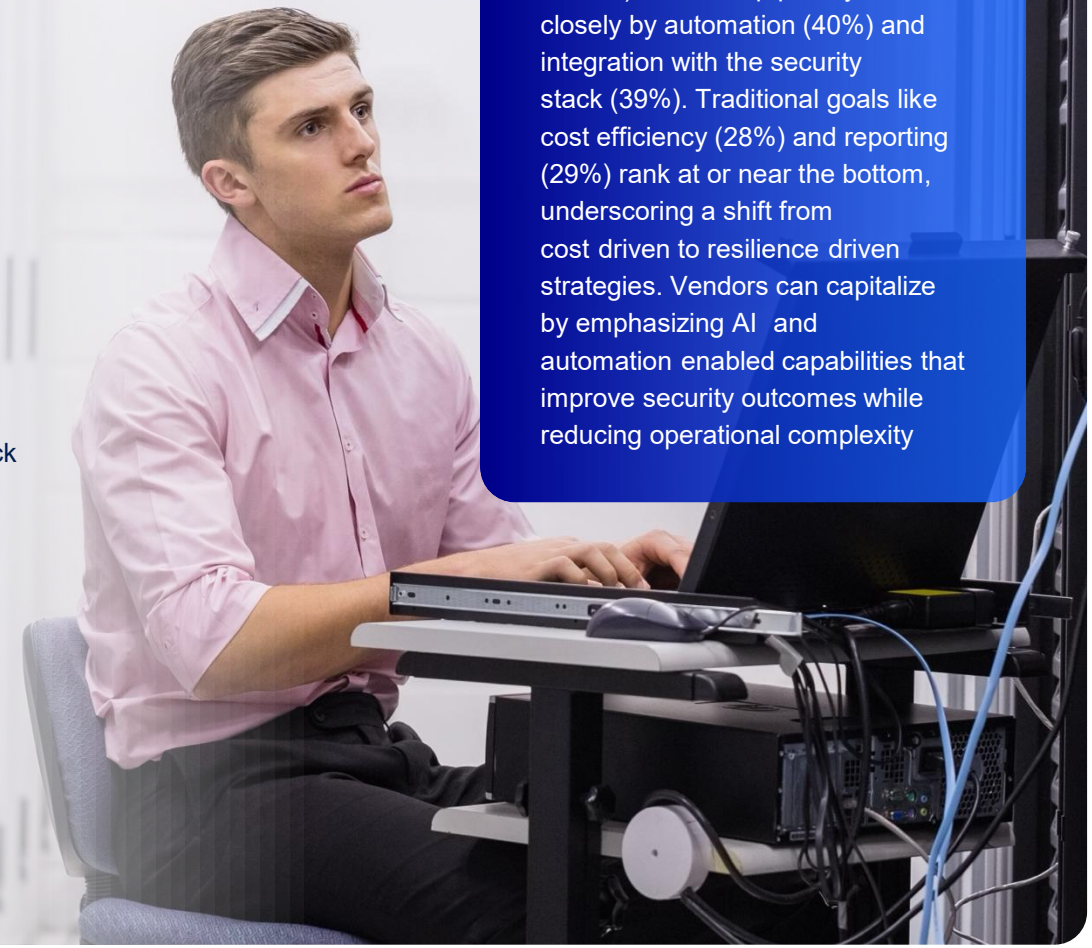
Infrastructure Strategies and Ideal States
How Organizations Structure — and Want to Evolve — Their Backup Environments

Security and automation are the leading priorities for improving DB&R, outweighing cost efficiency and reporting.

Top priorities for improving backup and recovery operations



- Automated security (e.g., AI detection, Ransomware checks)
- Back-up and recovery automation
- Better integration with security stack
- Faster recovery times
- More reliable testing
- Simplified management
- Better reporting/auditing
- Cost efficiency



Insight:

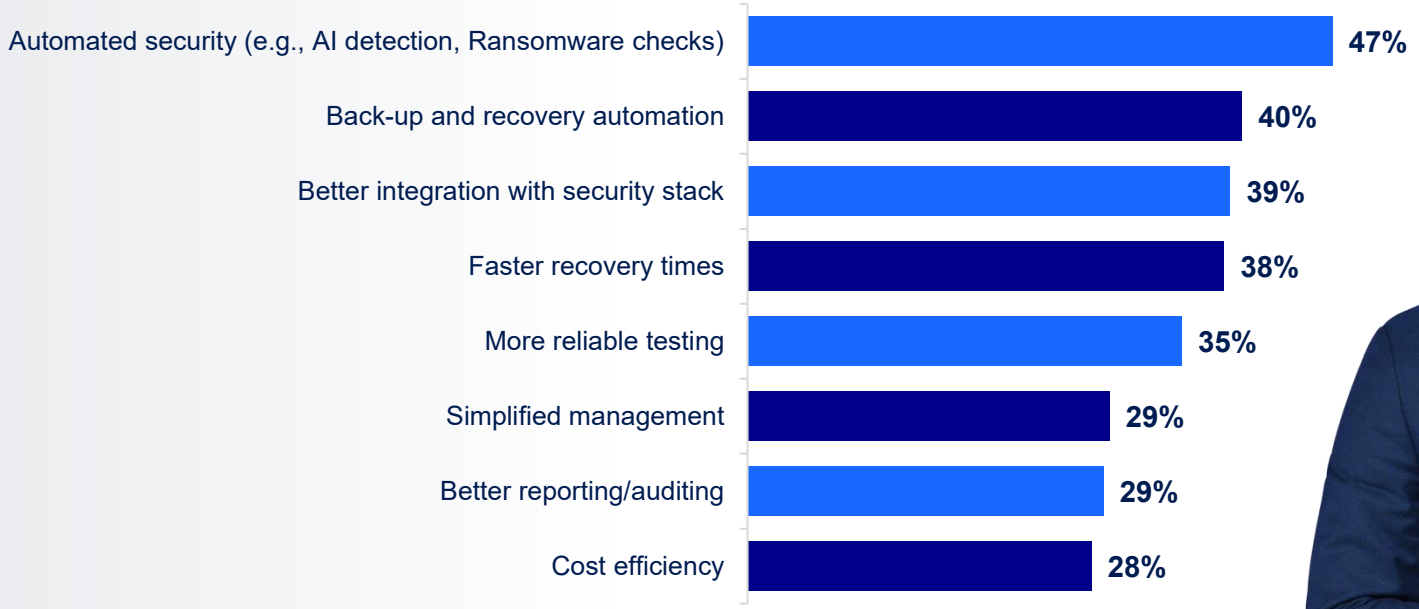
Nearly half (47%) cite automated security (AI detection, ransomware checks) as their top priority, followed closely by automation (40%) and integration with the security stack (39%). Traditional goals like cost efficiency (28%) and reporting (29%) rank at or near the bottom, underscoring a shift from cost driven to resilience driven strategies. Vendors can capitalize by emphasizing AI and automation enabled capabilities that improve security outcomes while reducing operational complexity

Modernization Priorities

What IT Leaders Value Most in the Next Generation of DB&R

Modernization Priorities
What IT Leaders Value Most in the Next Generation of DB&R

Top priorities for improving backup and recovery operations



Security and automation are the leading priorities for improving DB&R, outweighing cost efficiency and reporting.

Nearly half (47%) cite automated security (AI detection, ransomware checks) as their top priority, followed closely by automation (40%) and integration with the security stack (39%). Traditional goals like cost efficiency (28%) and reporting (29%) rank at or near the bottom, underscoring a shift from cost driven to resilience driven strategies.

Vendors can capitalize by emphasizing AI and automation enabled capabilities that improve security outcomes while reducing operational complexity

Technology Landscape and Tooling

Tools, Platforms, and Technologies Powering Today’s DB&R Environments

Technology Landscape and Tooling

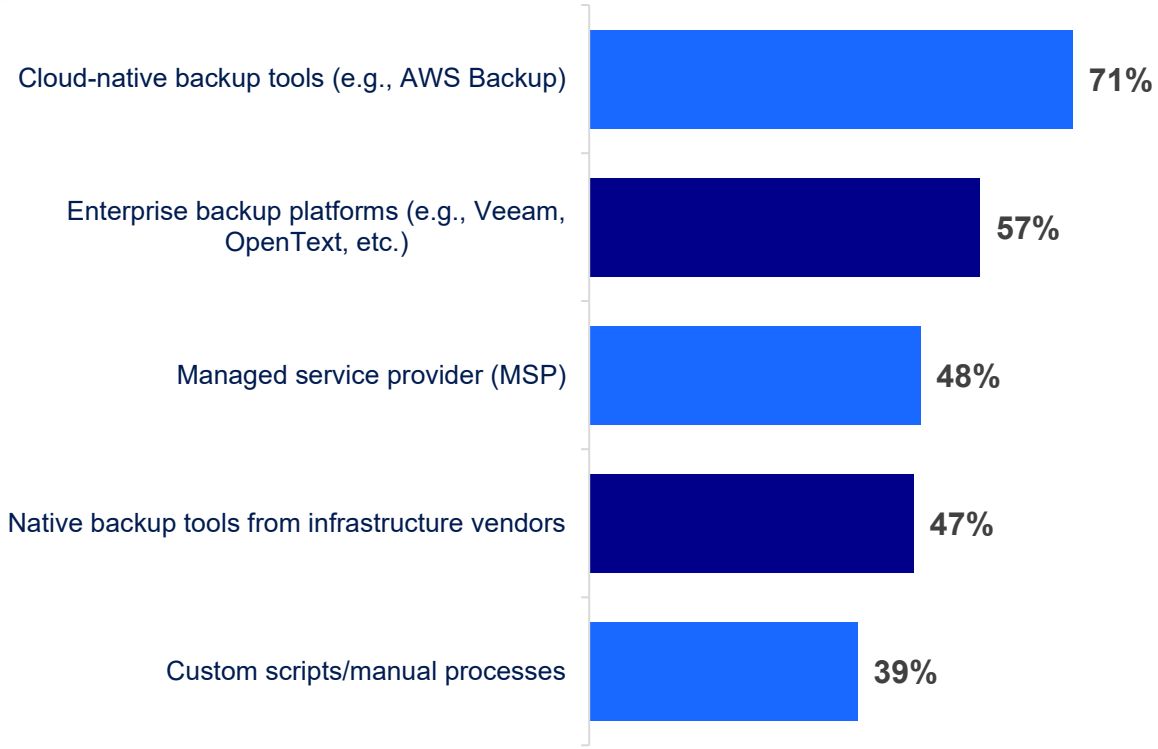
Tools, Platforms, and Technologies Powering Today's DB&R Environments

Insight:

The reliance on cloud-native solutions (71%) underscores the growing shift toward cloud-first IT strategies, yet the continued use of enterprise platforms (57%), managed services (48%), and scripts/manual processes (39%) highlights that backup environments remain complex and fragmented, requiring vendors to address integration and simplification needs

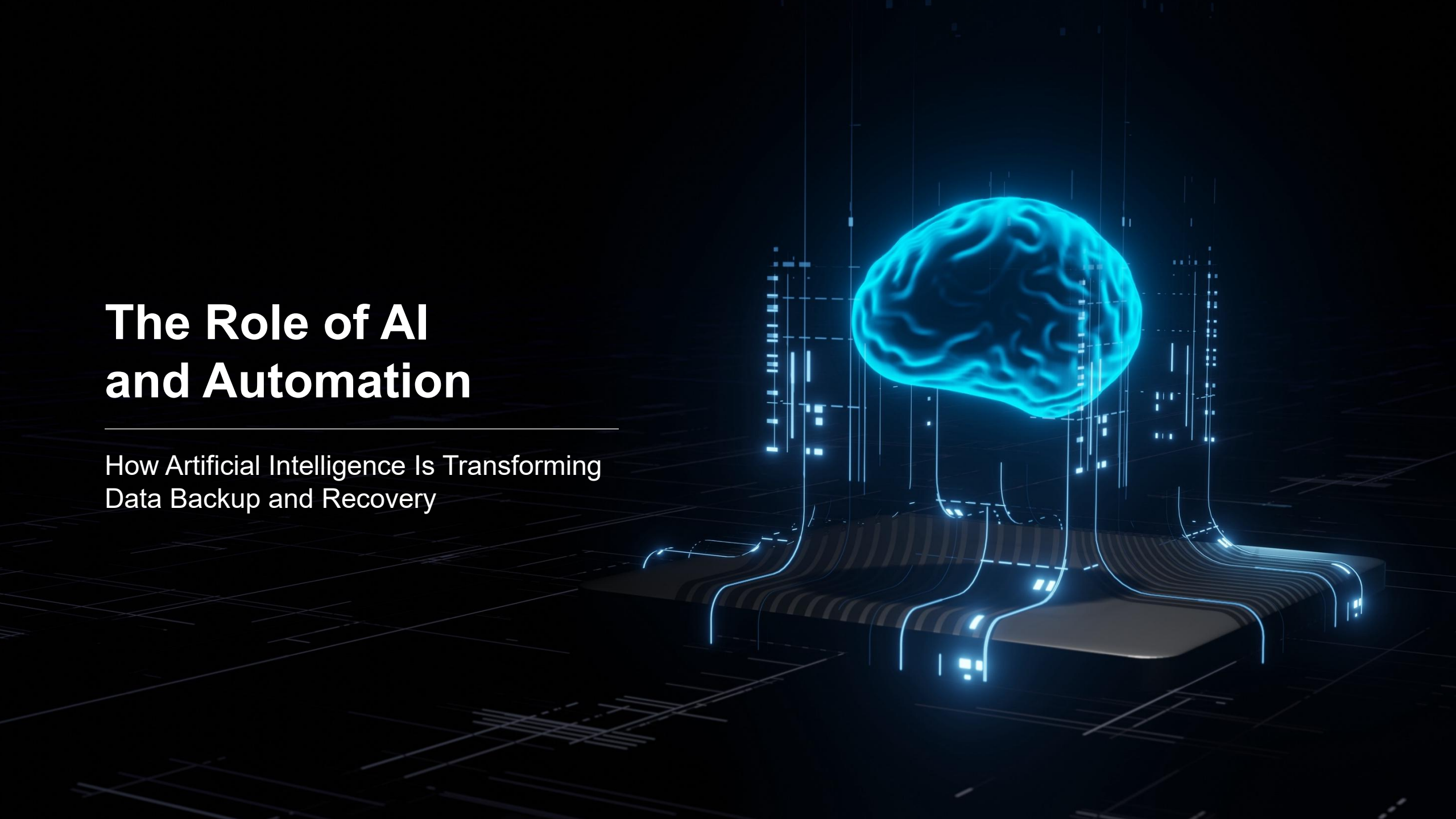
Cloud native backup tools dominate DB&R strategies, but most organizations also rely on a mix of enterprise platforms, MSPs, and even manual processes.

Tools or technologies currently used to manage DB&R process



The Role of AI and Automation

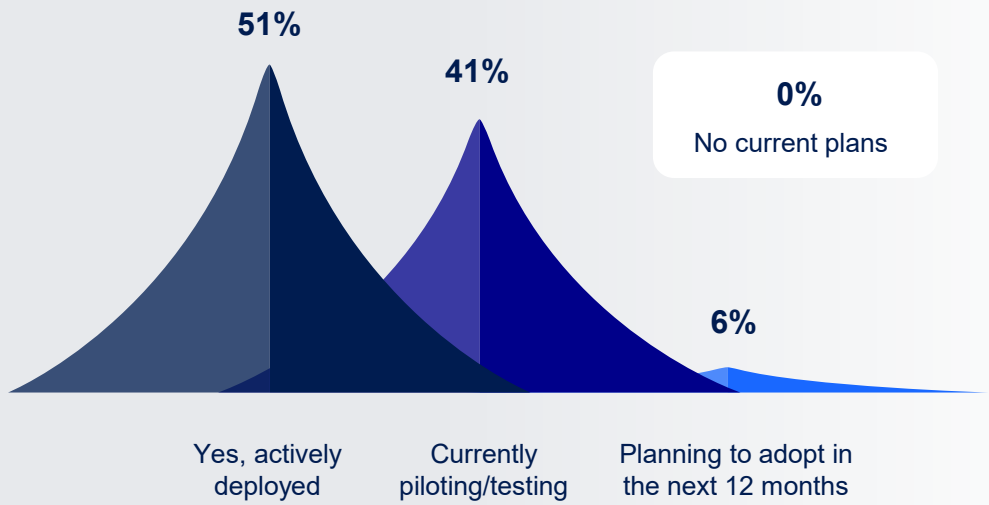
How Artificial Intelligence Is Transforming Data Backup and Recovery



The Role of AI and Automation

How Artificial Intelligence Is Transforming Data Backup and Recovery

Organizations using AI or machine learning in any part of its backup and recovery process



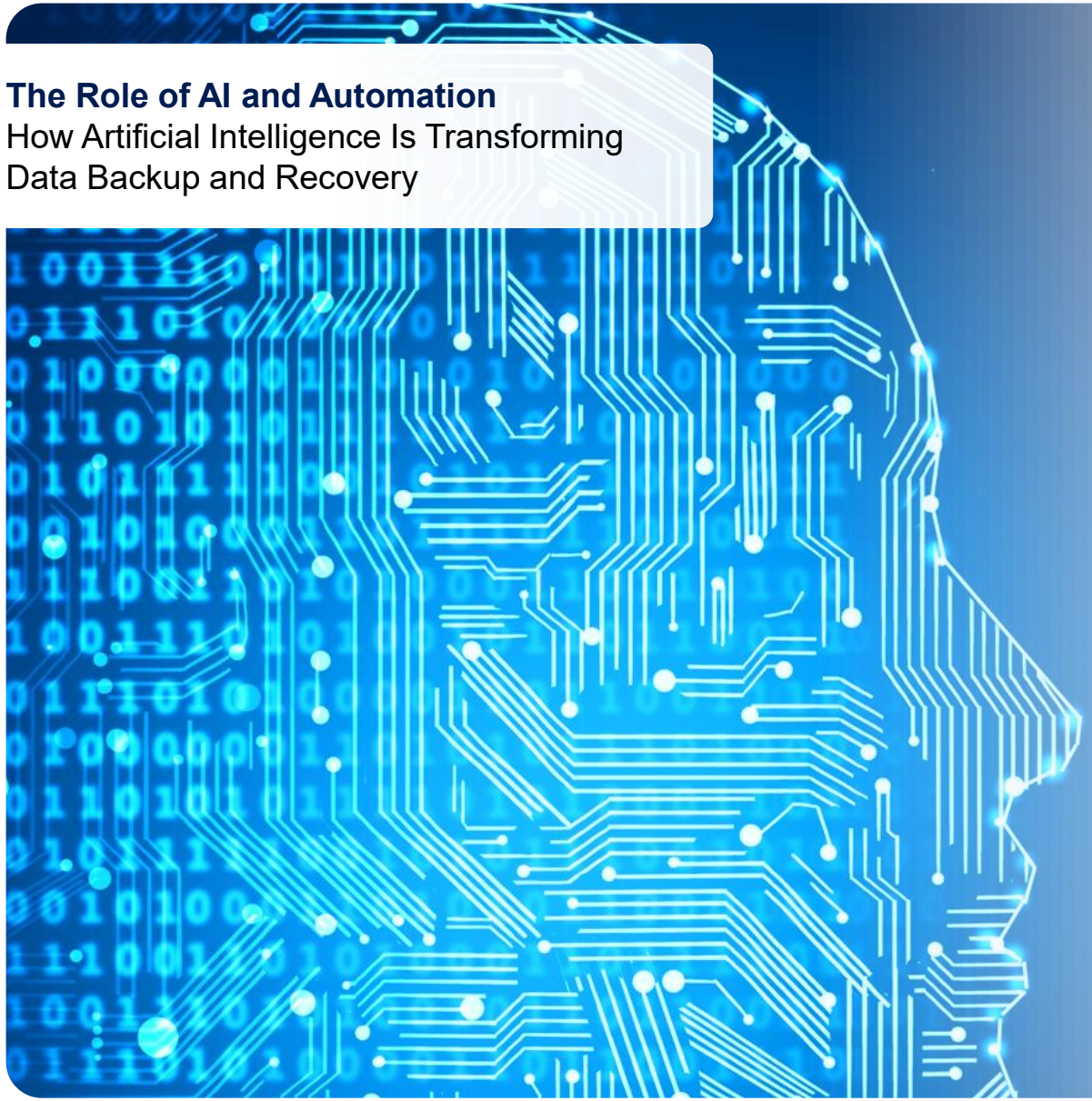
0%
No current plans

AI adoption in backup and recovery is already mainstream, with over half of organizations actively deploying it and most of the rest piloting.

A combined 93% are either actively using AI (51%) or piloting/testing it (42%), leaving almost no organizations without AI on their roadmap. This rapid adoption underscores a market shift toward intelligent, automated DB&R. This creates a prime opportunity for vendors to differentiate through advanced AI use cases like anomaly detection, predictive failure analysis, and automated policy enforcement.

The Role of AI and Automation

How Artificial Intelligence Is Transforming Data Backup and Recovery



Although recovery guidance and incident response top the list by a small margin, AI is highly valued across all of our DB&R use cases.

Vendors that can deliver across this full spectrum from anomaly detection to automated recovery action can position themselves as indispensable partners in resilient, AI driven DB&R.

Value to organization of use cases for AI in DB&R

- **87%** AI powered recommendations for recovery
- **87%** AI for incident response
- **84%** Anomaly detection in backups
- **81%** Predictive failure analysis (e.g., GenAI)
- **81%** Automated policy enforcement

Compliance, Insurance and Regulatory Pressures

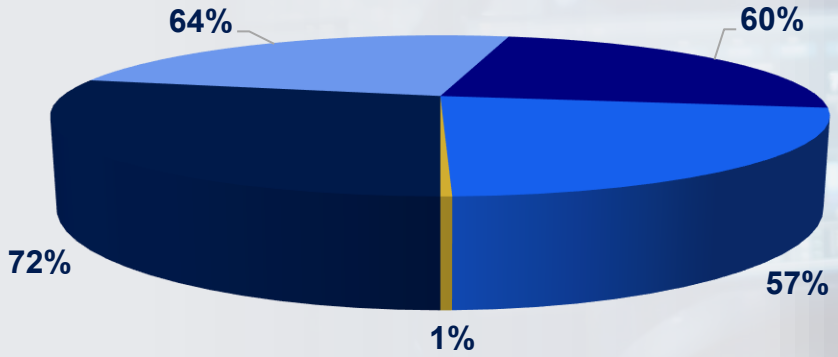
How Governance and Risk Mandates Shape DB&R Strategy

Compliance, Insurance and Regulatory Pressures

How Governance and Risk Mandates Shape DB&R Strategy

Requirements that influence backup and recovery strategy

- Cybersecurity insurance mandates
- Regulatory compliance (e.g., GDPR, HIPAA, SOX)
- Industry standards (e.g., NIST, ISO 27001)
- Internal risk/audit requirements
- No specific compliance drives

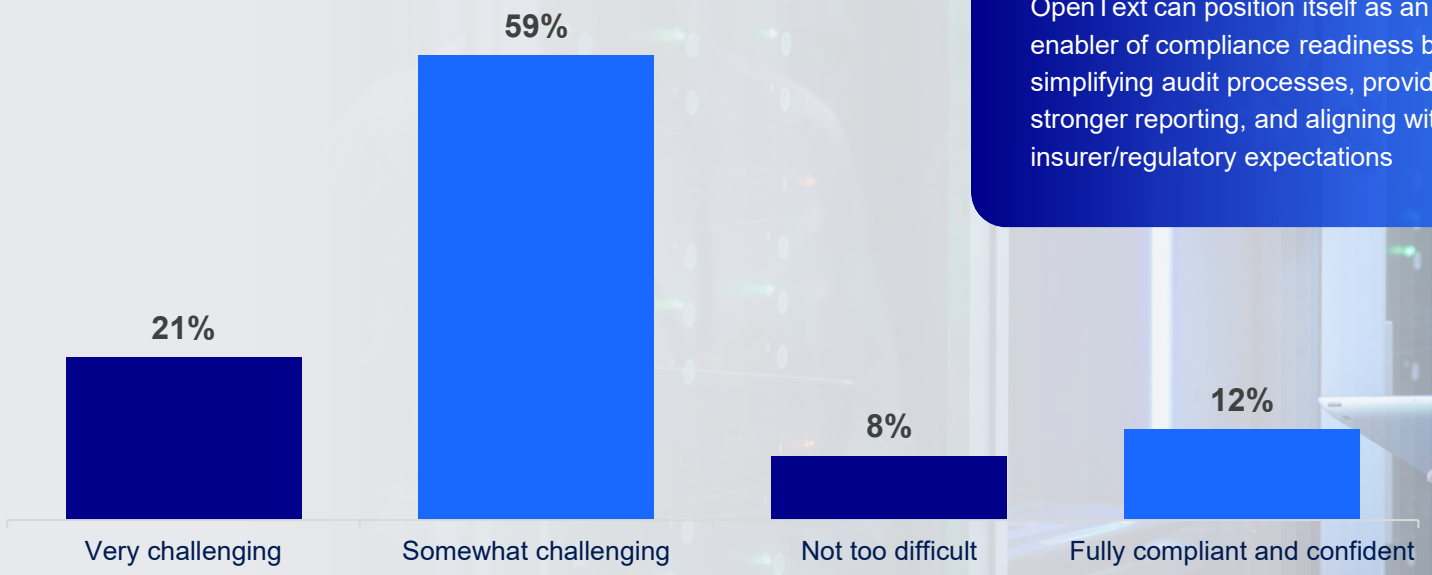


Cybersecurity insurance mandates and regulatory compliance are the strongest forces shaping DB&R strategy

This is an opportunity for OpenText to position DB&R not only as a resilience solution but also as a compliance and insurance enabler (i.e., helping enterprises streamline audits and meet insurer expectations).

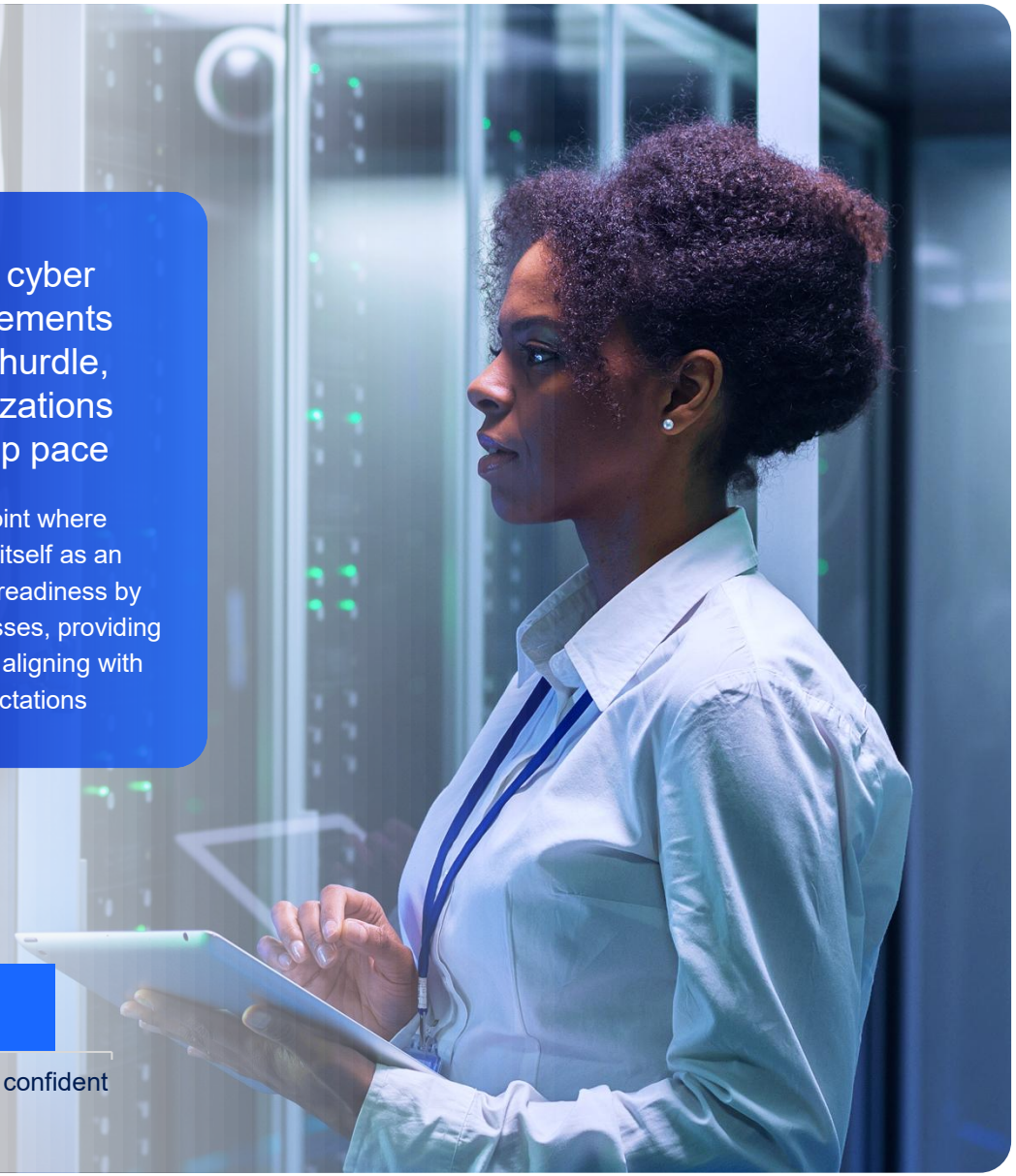
Compliance, Insurance and Regulatory Pressures
How Governance and Risk Mandates Shape DB&R Strategy

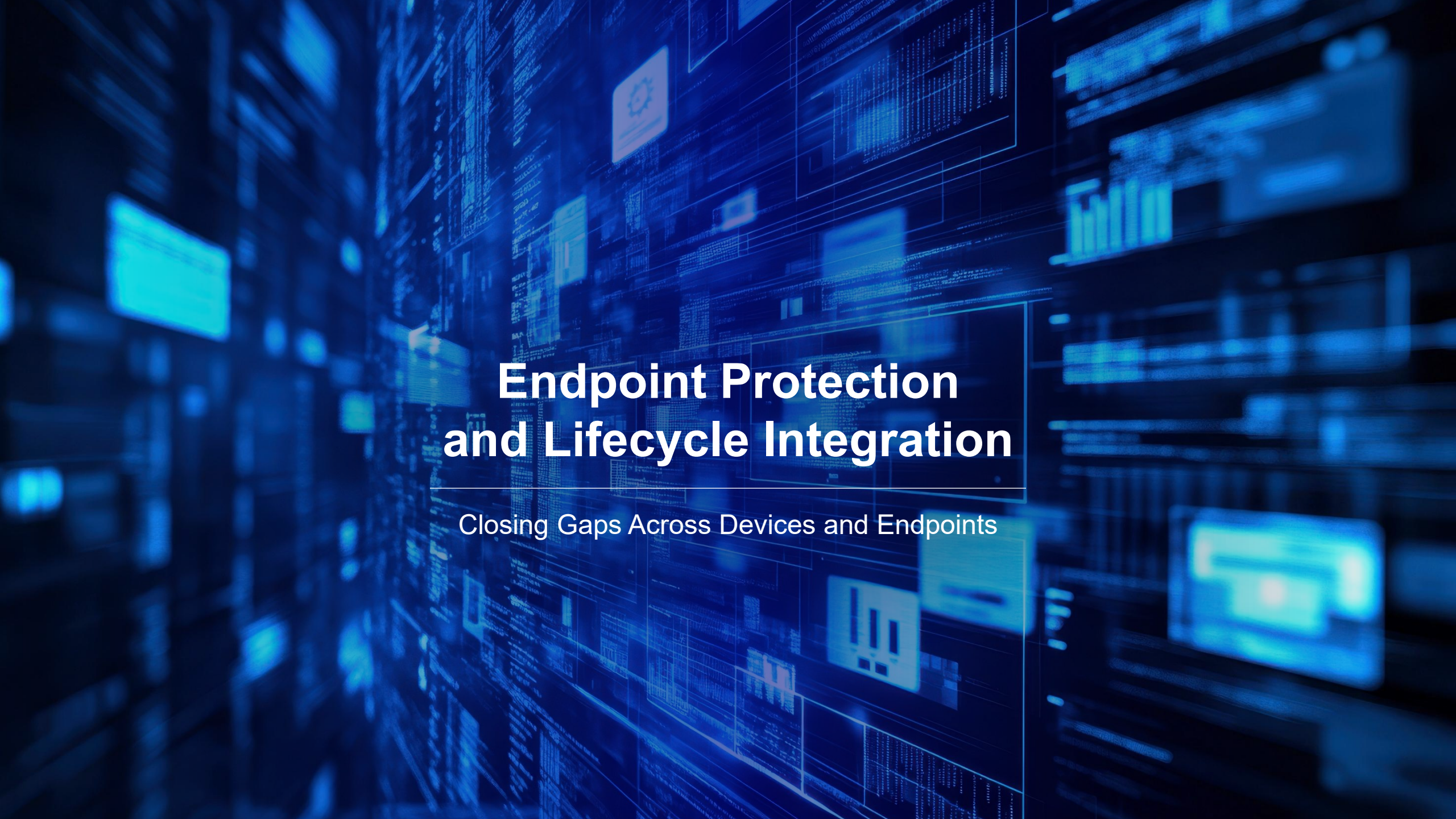
Challenging to meet DB&R-related compliance or cyber insurance requirements



Compliance and cyber insurance requirements are a significant hurdle, with most organizations struggling to keep pace

This is a critical pain point where OpenText can position itself as an enabler of compliance readiness by simplifying audit processes, providing stronger reporting, and aligning with insurer/regulatory expectations





Endpoint Protection and Lifecycle Integration

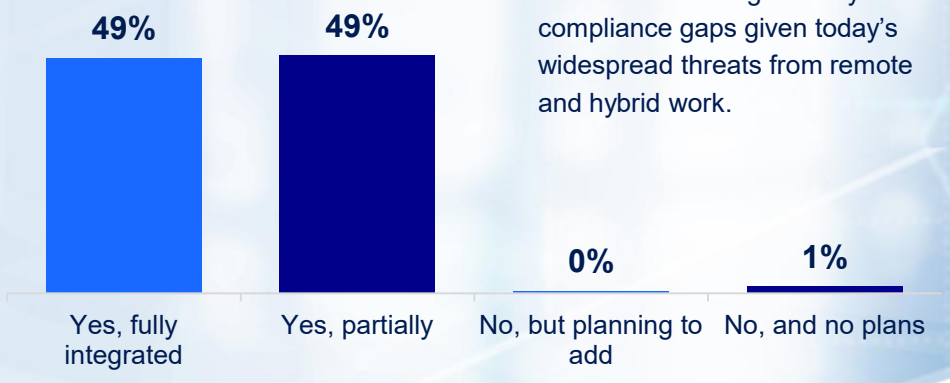
Closing Gaps Across Devices and Endpoints

Endpoint Protection and Lifecycle Integration
Closing Gaps Across Devices and Endpoints

Is endpoint device backup in the core DB&R strategy?

Endpoint device backup is still nowhere close to universal, with half of organizations only partially integrating it into their DB&R strategy

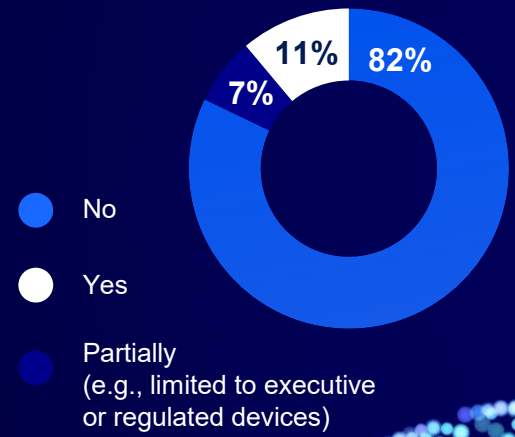
This partial coverage represents a clear opportunity for vendors to position endpoint backup as essential to closing security and compliance gaps given today's widespread threats from remote and hybrid work.



Are backup considerations included in your device lifecycle/recycling process?

Most organizations include backup in their device lifecycle processes, but partial or absent coverage still leaves risk.

While lifecycle integration is becoming a best practice, gaps persist, which is an opportunity for OpenText to stress universal endpoint coverage as a safeguard against compliance failures and inadvertent data exposure during device turnover.



Integration and Convergence Trends

The Push Toward Unified IT, Security, and Backup Management

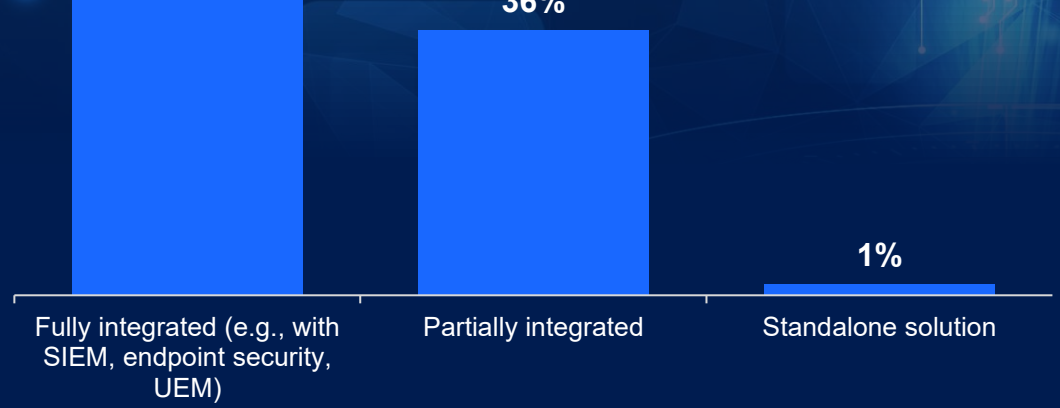
Integration and Convergence Trends

The Push Toward Unified IT, Security, and Backup Management

Most enterprises now integrate DB&R with broader security and IT tools, though more than one third still operate in partial silos

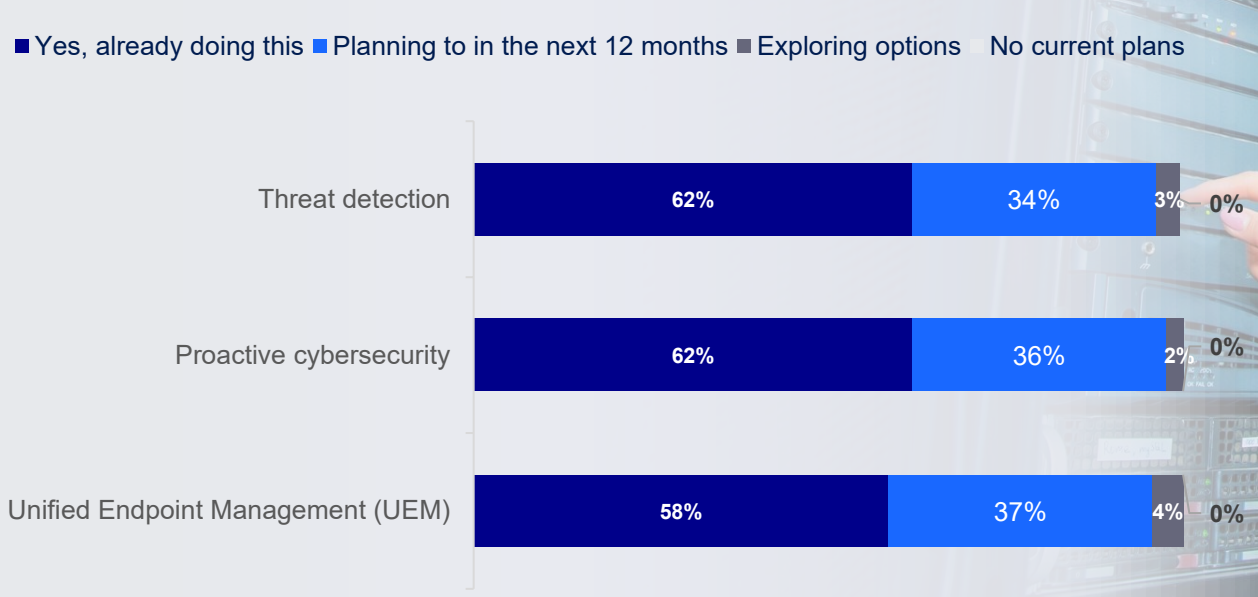
This shows a strong trend toward convergence but also leaves a sizable group struggling with fragmentation. This is an opportunity for OpenText to emphasize unified platforms that seamlessly connect DB&R with the wider security ecosystem.

How is your DB&R solution integrated with broader security and IT management tools?



Integration and Convergence Trends
The Push Toward Unified IT, Security, and Backup Management

Is your organization expanding its security scope beyond its current DB&R strategy?



Organizations are extending DB&R into broader security domains, with most already advancing threat detection, proactive cybersecurity, and UEM

This is a positioning opportunity for OpenText: solutions that unify backup, endpoint, and threat defense can align with customer roadmaps for holistic resilience.

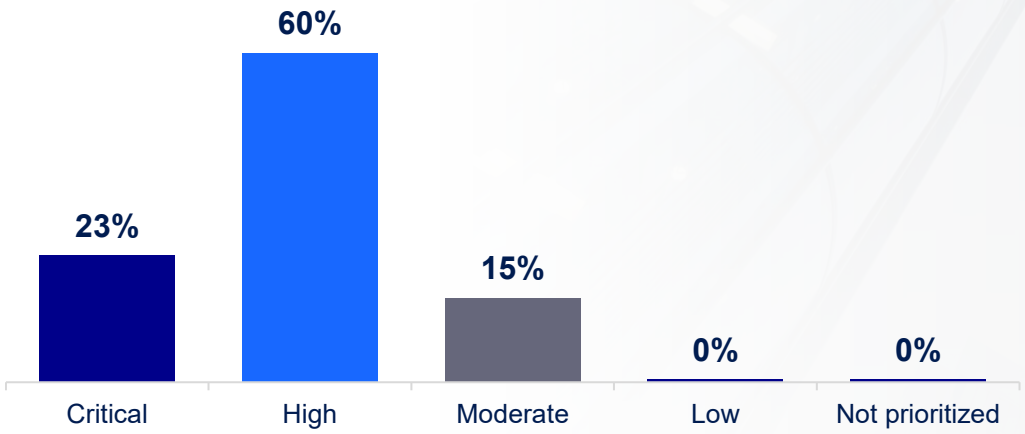
Investment and Strategic Priority

Why Backup & Recovery Is Now Central to Cyber Resilience

Investment and Strategic Priority

Why Backup & Recovery Is Now Central to Cyber Resilience

Perceived priority of DB&R in your broader IT and cybersecurity roadmap based on the level of investment it receives



DB&R is a clear investment priority, with more than 8 in 10 organizations rating it as high or critical in their IT and cybersecurity roadmaps

Backup and recovery is now a strategic pillar of cyber resilience. This is an opportunity to justify investment in advanced, modernized DB&R capabilities that align with top-level IT and security agendas.

Barriers to Modernization

What’s Holding Organizations Back from Evolving DB&R

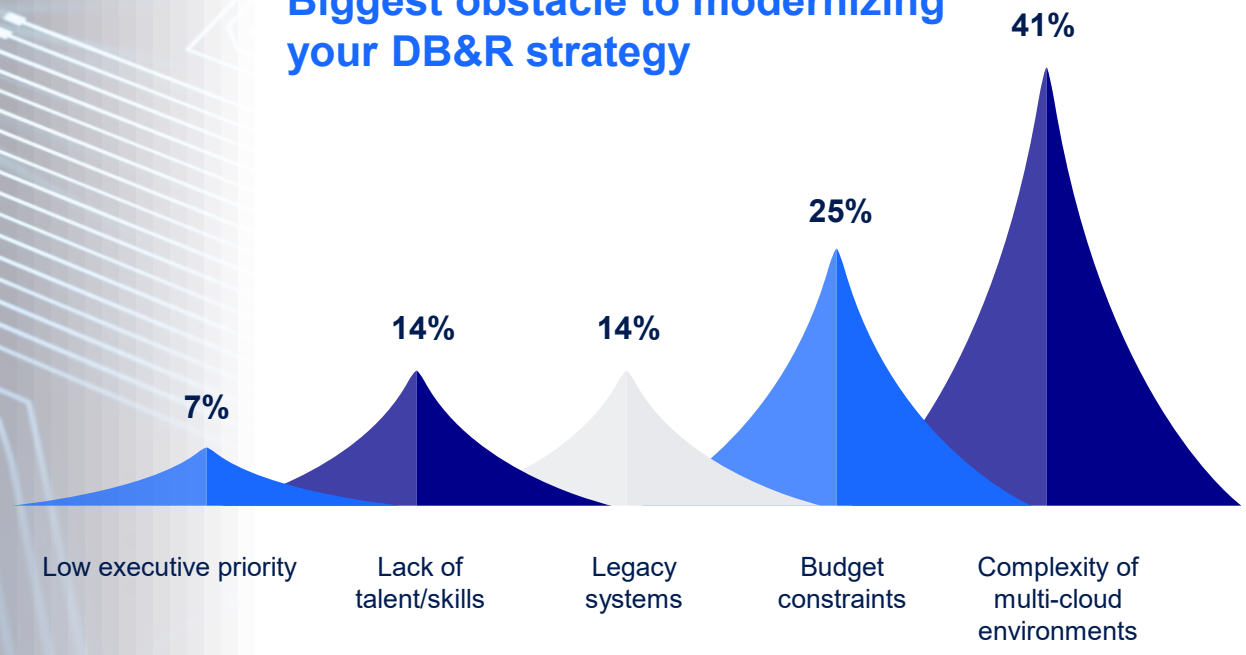
Barriers to Modernization

What's Holding Organizations Back from Evolving DB&R

Multi cloud complexity is the single biggest barrier to modernizing DB&R strategies, far outweighing other challenges

Modernization isn't stalled by lack of will, but by the operational challenges of managing diverse, fragmented environments. This is a prime opportunity to show how OpenText can simplify multi cloud integration and deliver unified management.

Biggest obstacle to modernizing your DB&R strategy

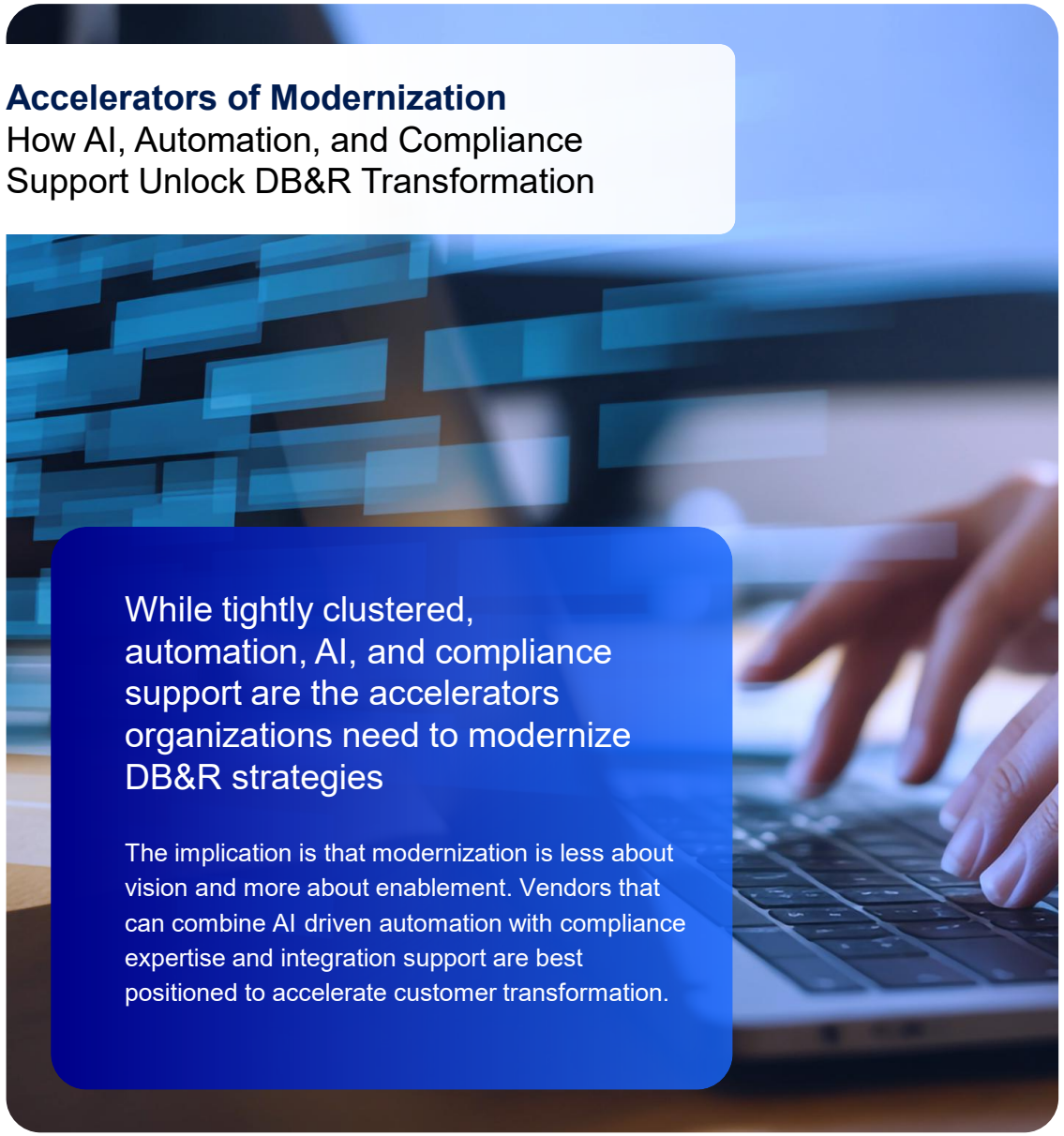


Accelerators of Modernization

How AI, Automation, and Compliance Support Unlock DB&R Transformation

Accelerators of Modernization

How AI, Automation, and Compliance Support Unlock DB&R Transformation

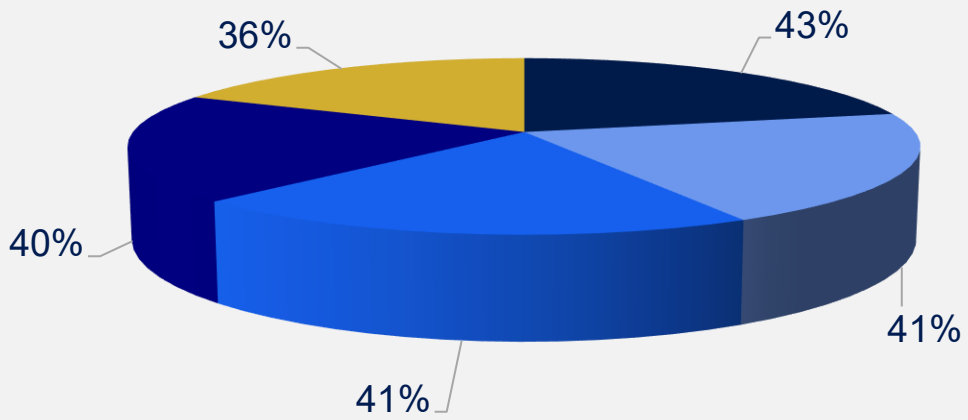


While tightly clustered, automation, AI, and compliance support are the accelerators organizations need to modernize DB&R strategies

The implication is that modernization is less about vision and more about enablement. Vendors that can combine AI driven automation with compliance expertise and integration support are best positioned to accelerate customer transformation.

What would most accelerate your organization's ability to modernize DB&R?

- Access to automation and AI tools
- Guidance on compliance and cyber insurance
- Simplified integration with legacy systems
- Skilled staff or managed services
- Better executive alignment



Conclusion and Next Steps

Turning Insights into Action with OpenText

Key Benefits for OpenText Customers

Close Modern Workload Gaps

Powerful container and hypervisor backup for under protected modern workloads.

Comprehensive Cyber Resilience

Cyber-threat protection, recovery automation, and user-error mitigation to prevent any kind of data loss.

Leading in AI and Automation

AI driven anomaly detection for fast threat response and automated recovery including High Availability (HA) for most important systems.

Simplify Hybrid and Multi-Cloud

Strong backup and recovery options for on-premises (datacenter) and cloud including support for a multitude of SaaS and on-prem solutions.

Enable Compliance and Insurance Alignment

Obtain strong reporting, audit support, and compliance readiness to ease struggles with compliance mandates and insurer requirements.

Expand Beyond Backup

OpenText can provide a comprehensive cyber-security solution from advanced AI threat prevention, to threat mitigation and complete recovery response.

Taking charge:
Building a smarter, more resilient data strategy

Discover how OpenText can help you…..

Protect modern workloads, simplify hybrid cloud, and go beyond backup with AI-driven automation, cyber-threat prevention, and compliance-ready recovery. Your data, always secure and available.

Contact us

Get a free trial

to begin your journey toward smarter data management.

opentext™

opentext.com · twitter.com/opentext · linkedin.com/company/opentext

11.25 | 248-000141-001