Enterprise Strategy Group™

The Ransomware Reality: Cyber Resilience, Data Resilience, and Data Protection



Jon Brown | Senior Analyst
ENTERPRISE STRATEGY GROUP



Research Objectives

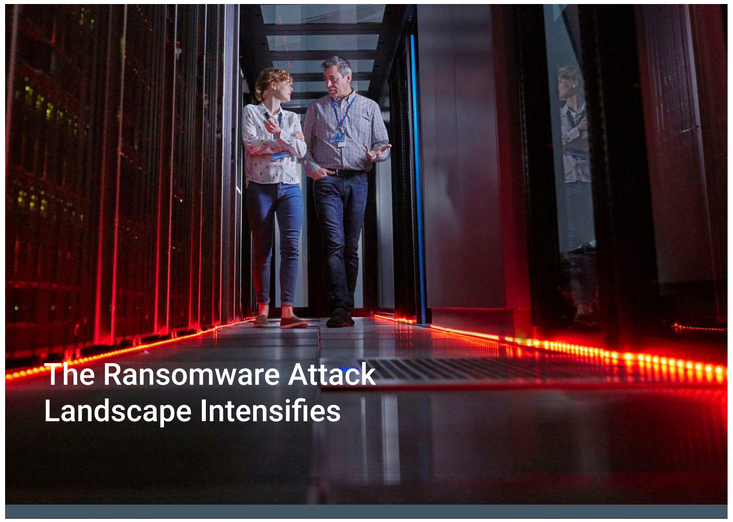
The era of traditional backup is entering its twilight, prompting organizations to shift their approach to data protection. Simultaneously, increased cyberthreats, especially ransomware attacks, and strategic investments in AI and other data-intensive workloads have fundamentally altered how organizations evaluate data protection vendors and offerings. Modern business is built atop data copies, and organizations are working to enhance those copies with higher levels of protection, security, readiness, and recovery. They must also better understand the data to optimize costs and accelerate business initiatives.

In order to gain insights into these trends, Enterprise Strategy Group surveyed 400 IT and data protection professionals in North America (U.S. and Canada) involved with or responsible for evaluating, purchasing, managing, and building data protection and resilience solutions.

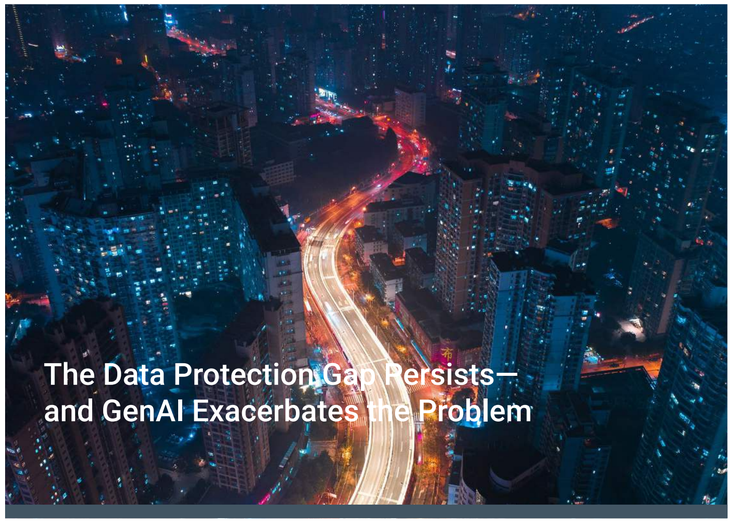
This study sought to:

- **Understand** the current state of data protection and recovery investments.
- **Identify** technology and business drivers that spur adoption of data recovery technologies.
- **Determine** the impact of ransomware attacks and steps organizations take to respond.
- **Monitor** the buying team, including influencers and final decision-makers.

KEY FINDINGS/CONTENTS











"With 88% of organizations ranking ransomware among their top five overall threats, the high relative risk rating suggests **ransomware has likely achieved board-level visibility at most organizations**."



Jon Brown | Senior Analyst
ENTERPRISE STRATEGY GROUP

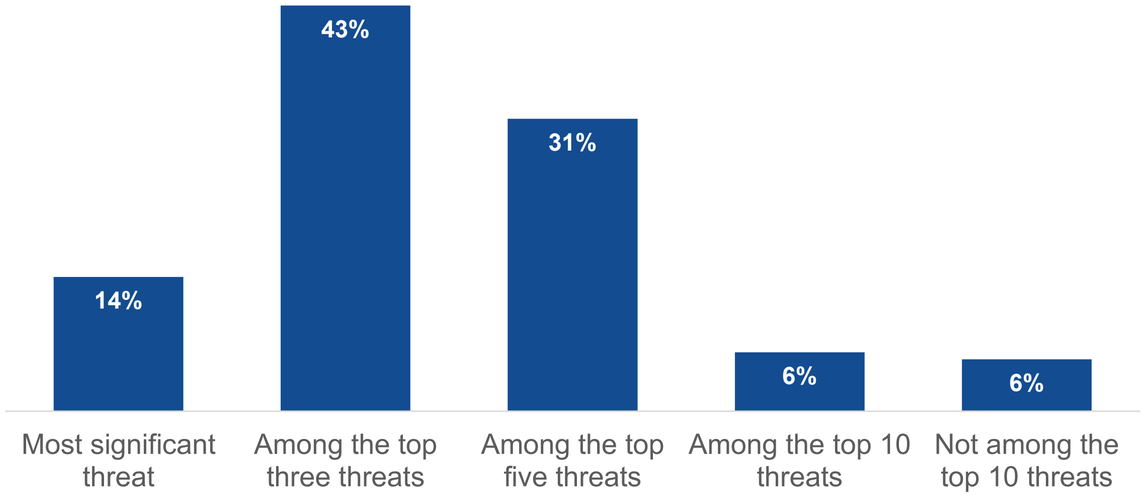


The Ransomware Attack Landscape Intensifies

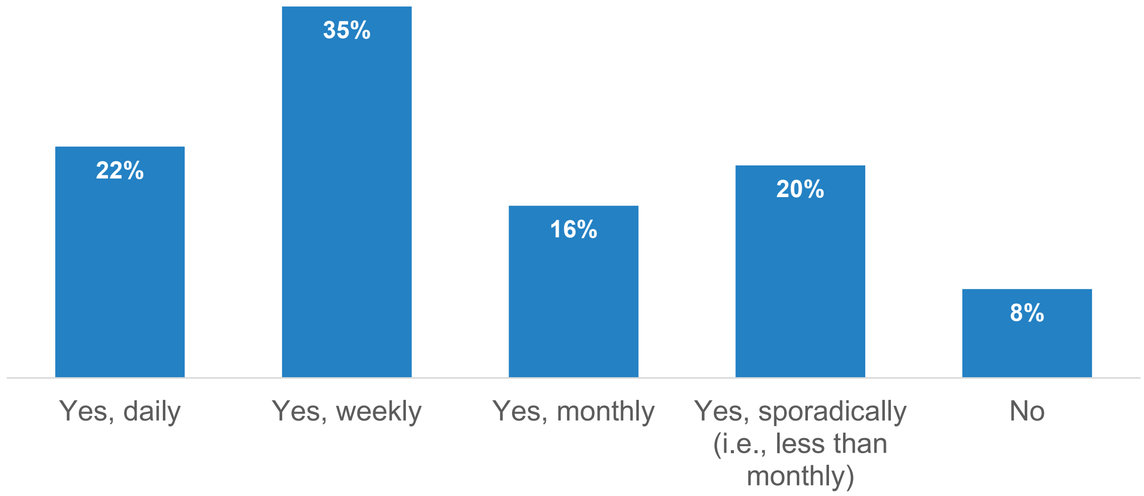
Ransomware Is a Top Threat to Nearly All Organizations, With Most Facing Frequent Attack Attempts

With 88% of organizations ranking ransomware among their top five overall threats, the high relative risk rating suggests ransomware has likely achieved board-level visibility at most organizations, potentially driving increased security investment and executive attention to cyber resilience. Ransomware prevention, recovery, and resilience are undertakings that nearly all organizations worry about. Ransomware attacks are a persistent, universal, normalized threat. The high frequency of attacks (particularly for the 22% facing daily attempts) suggests significant resources must be dedicated to continuous monitoring, threat detection, and response capabilities.

Threat of ransomware to the health of organizations compared with all other potential risks.



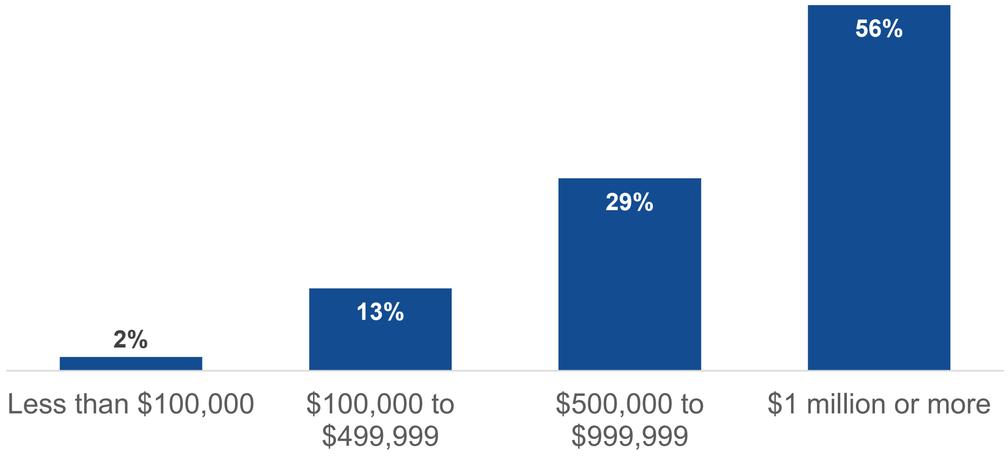
Have organizations experienced attempted ransomware attacks within the last 12 months?



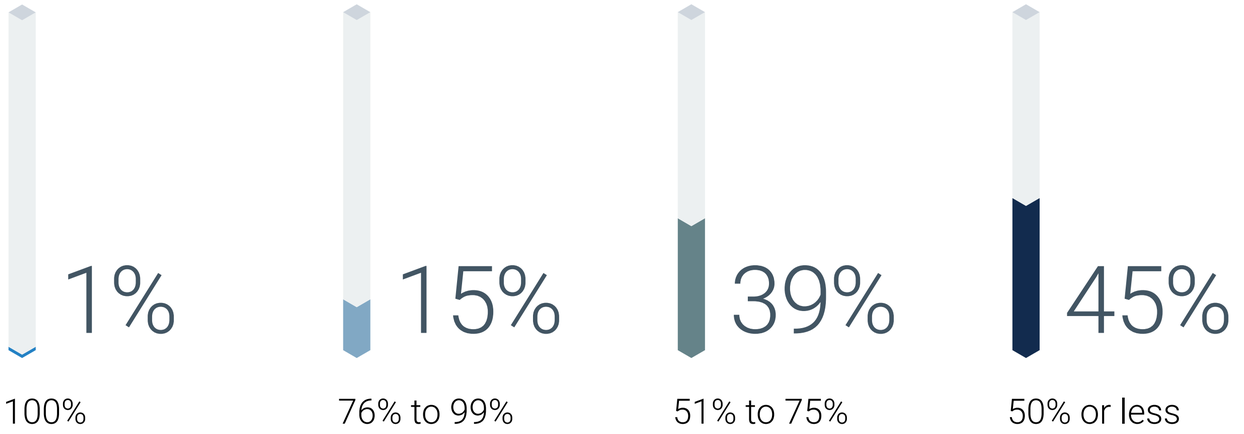
The Impacts of Ransomware Attacks

These outcomes highlight the critical importance of data protection strategies that go beyond prevention to include robust backup and recovery capabilities. There is a clear market need for solutions that can guarantee higher recovery rates and minimize financial impact given that more than half (56%) of organizations estimated the financial impact of recent ransomware attacks to be $1 million or more. The significant percentage (99%) of organizations unable to *fully* recover their data demonstrates significant gaps in current protection approaches. The prevalence of follow-up extortion attempts, whether addressed (63%) or ignored (26%), also indicates the need for security solutions that address the full lifecycle of ransomware incidents, not just the initial attack.

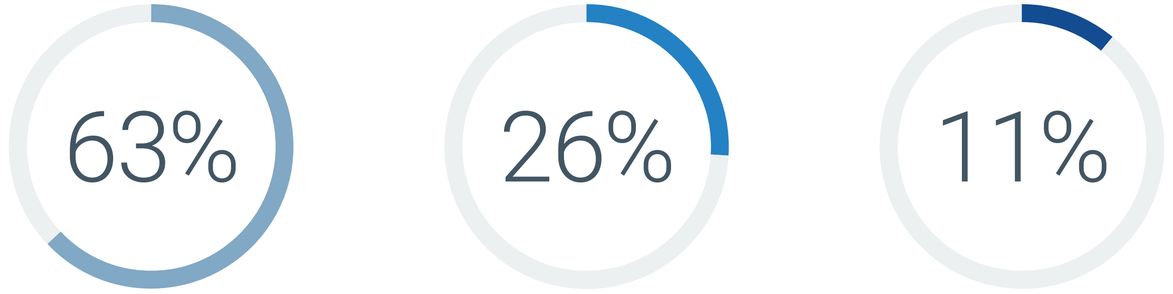
Total estimated financial impact of most recent ransomware attack(s).



Percentage of lost data recovered after ransomware attack(s).



Did organizations receive additional extortion attempts or other fee demands beyond the initial ransomware demand?



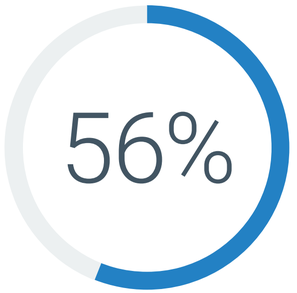
Organizations Worry Their Data Protection Copies Could Be Compromised by Ransomware

More than eight in 10 organizations are either very concerned (25%) or somewhat concerned (56%) that their data protection copies (e.g., backup, snapshot, replication, etc.) could become infected or corrupted by ransomware, indicating broad awareness of backup targeting as a key ransomware tactic.

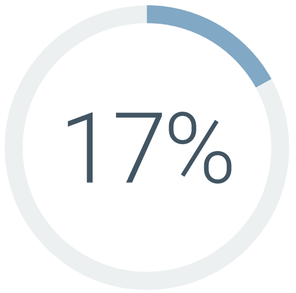
Level of concern that data protection copies could become infected or corrupted by ransomware attacks.



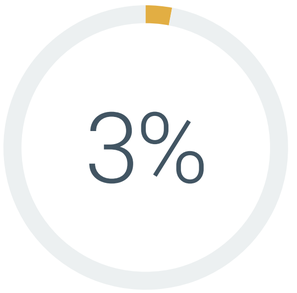
Very concerned



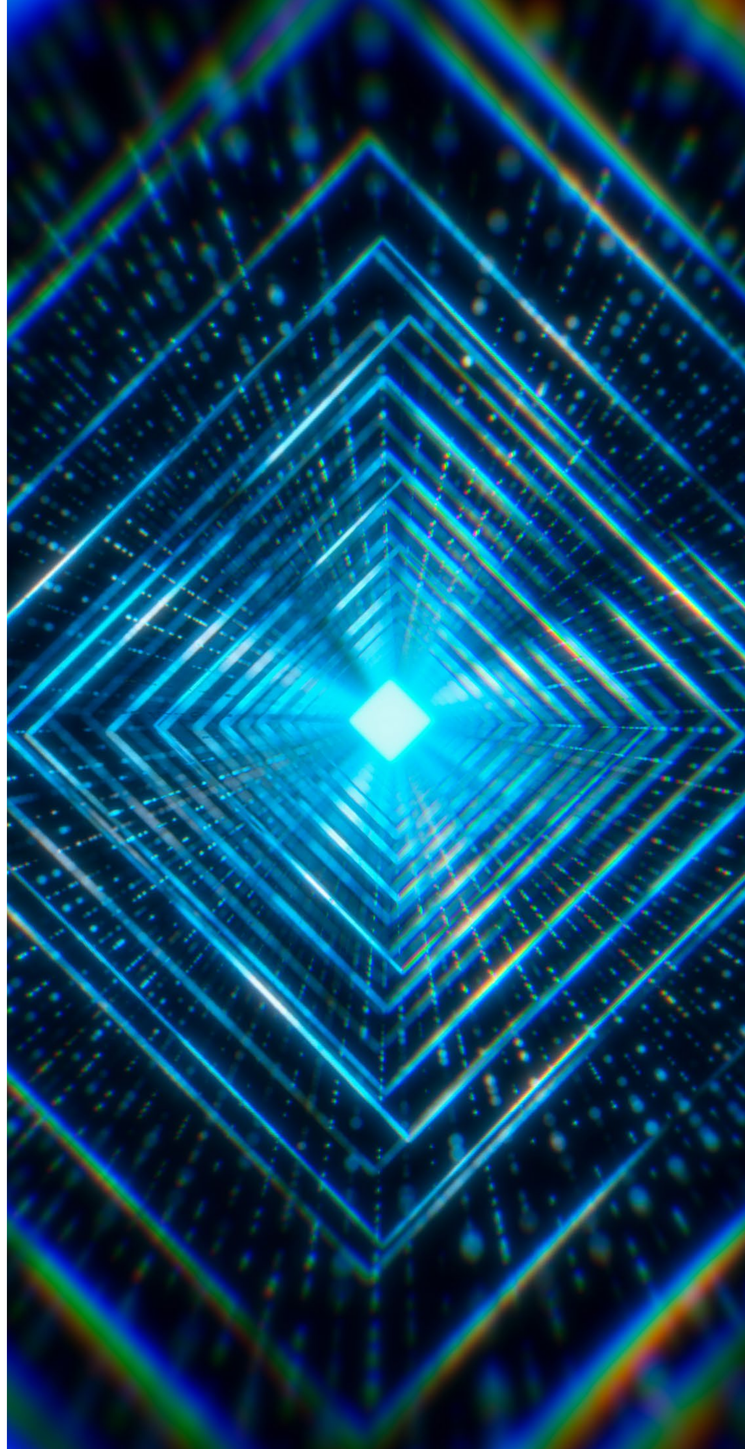
Somewhat concerned



Not very concerned



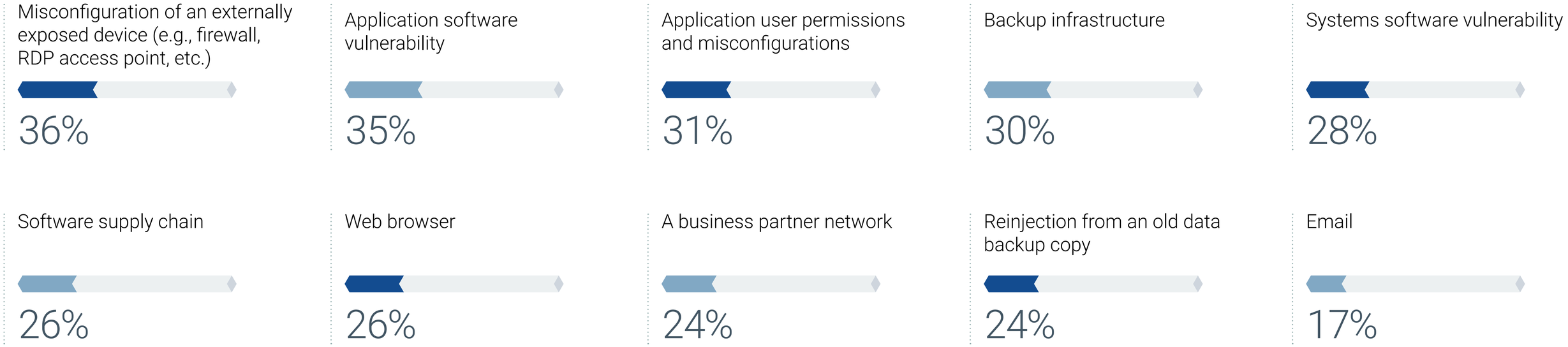
Not at all concerned



Misconfigurations and Vulnerabilities Lead Attack Vectors

The top three vectors all relate to configuration issues: exposed devices, application vulnerabilities, and permission misconfigurations. Attackers are increasingly exploiting technical vulnerabilities rather than relying on social engineering. Ransomware defense has traditionally focused on end-user hardening, but data suggests more focus needs to go to configuration management and hardening and vulnerability management for applications and systems, backup infrastructure security, and third-party and software supply chain risk management.

Initial point of compromise for recent ransomware attacks.



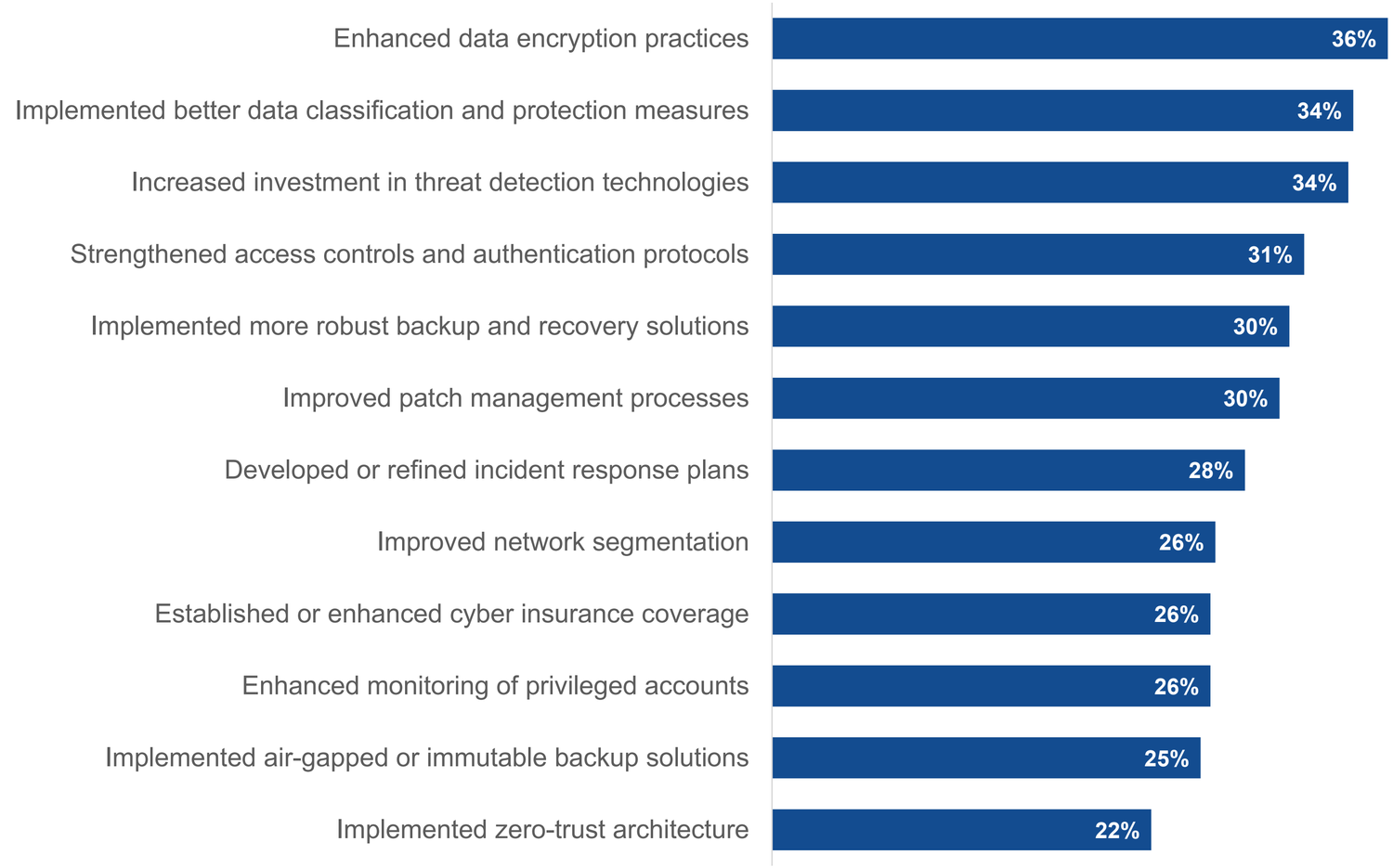


Data Security and Threat Detection Top Improvements

This data on post-attack improvements reveals a discipline in transition, moving from traditional security approaches toward more data-centric, detection-oriented, and recovery-focused strategies.

The somewhat low percentage across categories (all below 40%) suggests that many organizations may still be underinvesting in critical ransomware defenses despite having experienced attacks.

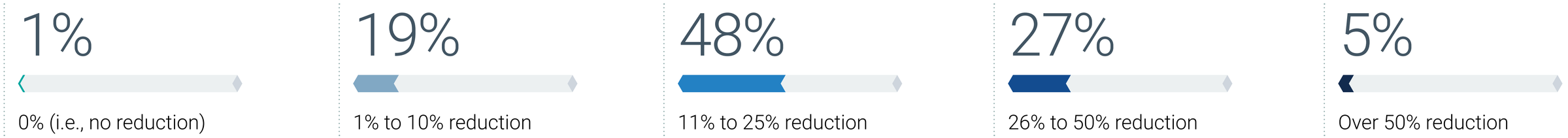
Most valuable lessons learned from or improvements made as a result of recent ransomware attacks.



AI Delivers Significant Recovery Time Improvements, as Most Organizations Achieve at Least a 10% RTO Reduction

Almost all organizations report some level of RTO reduction through AI-powered solutions, with only 1% seeing no improvement. This demonstrates AI's consistent ability to deliver tangible recovery benefits. AI-powered backup and recovery solutions deliver measurable and meaningful RTO improvements for the vast majority of organizations, with typical results falling in the 11% to 25% range, with substantial potential for greater gains with more advanced implementations.

Percentage reduction in RTOs organizations have achieved through AI-powered backup and recovery solutions.

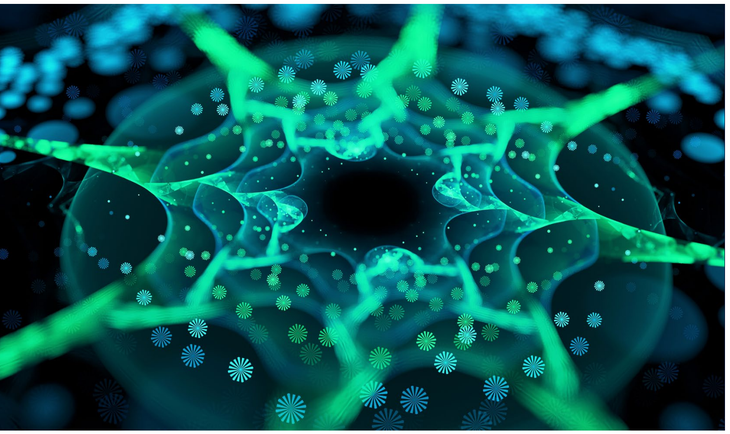




Data Protection Technologies Saturate Enterprise Environments

Nearly Half of Organizations Opt for a Platform Approach

When it comes to strategy, consolidation is the most widespread approach to data protection, with nearly a quarter (24%) opting for full consolidation, and another 22% maintaining a core platform with some exceptions. Organizations recognize the need to balance the efficiency of platform consolidation with the specialized capabilities of purpose-built solutions.



Organizations' current strategic approach to data protection, data management, and data resilience.

24% **Full consolidation** (i.e., one platform or vendor for all data protection, management, and resilience needs)

22% **Primary consolidation** (i.e., one platform with limited specialized solutions for specific use cases)

13% **Strategic diversification** (i.e., multiple specialized solutions to avoid vendor lock-in and reduce risk)

12% **Hybrid cloud approach** (i.e., separate solutions for on-premises and cloud environments)

22% **Balanced approach** (i.e., mix of consolidated platforms and specialized solutions based on workload requirements)

7% **Full diversification** (i.e., separate best-of-breed solutions for different aspects of data protection, management, and resilience)

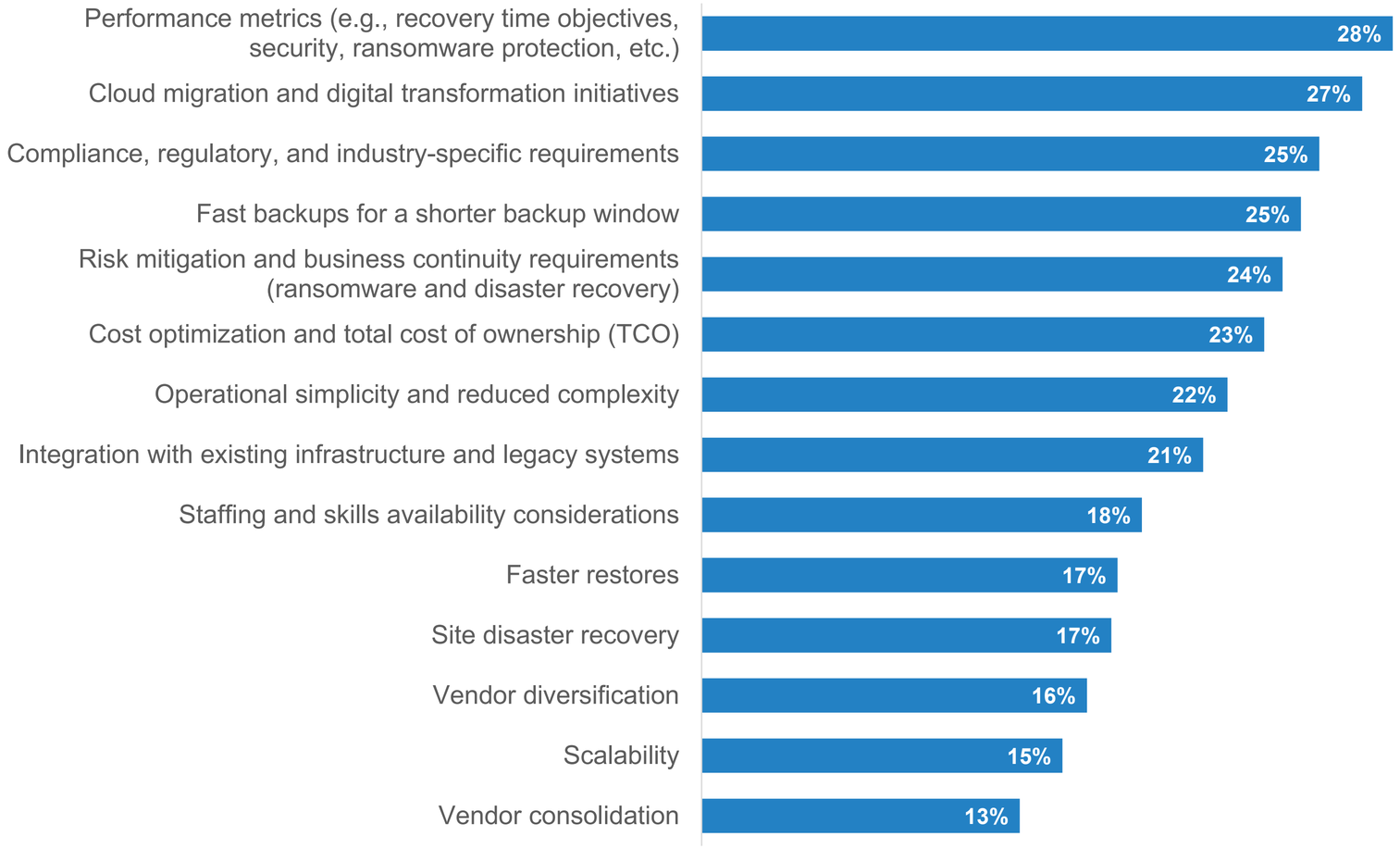
1% In transition from a diversified to a consolidated approach



Performance and DX Lead Data Protection Strategy, While Risk and Compliance Form a Critical Second Tier

When it comes to the drivers shaping data protection and management strategies, organizations are evolving toward more sophisticated, business-aligned approaches that prioritize measurable outcomes and digital transformation support while balancing risk, compliance, and operational considerations.

Primary drivers behind current strategic approach to data protection, data management, and data resilience.

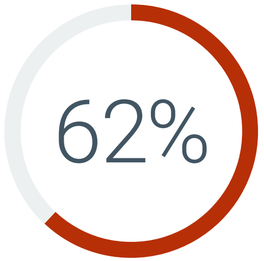


Purpose-built Appliances Are Commonly Tasked With Backup

Purpose-built backup appliances (PBBAs) have achieved majority adoption, establishing specialized backup infrastructure as the preferred approach for most organizations.

Nearly half of organizations now incorporate object storage into their on-premises backup. Despite predictions of its demise, tape remains relevant in nearly a quarter of organizations, likely for long-term retention, air-gapped protection, or specific compliance requirements.

Technologies primarily used for backup data storage in on-premises backup environments.



Purpose-built backup appliances (PBBA) with deduplication (e.g., Dell PowerProtect Data Domain, HPE StoreOnce, and ExaGrid)



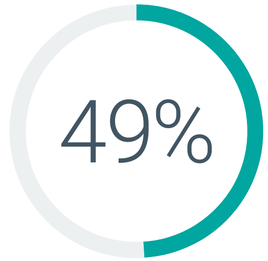
Tiered backup storage (automatic movement between storage tiers)



Hard disk drives (HDDs) in general-purpose storage arrays



Solid-state drives (SSDs) in general-purpose storage arrays



Object storage systems (e.g., Dell ObjectScale and IBM Cloud Object Storage)



Tape libraries (LTO and enterprise)

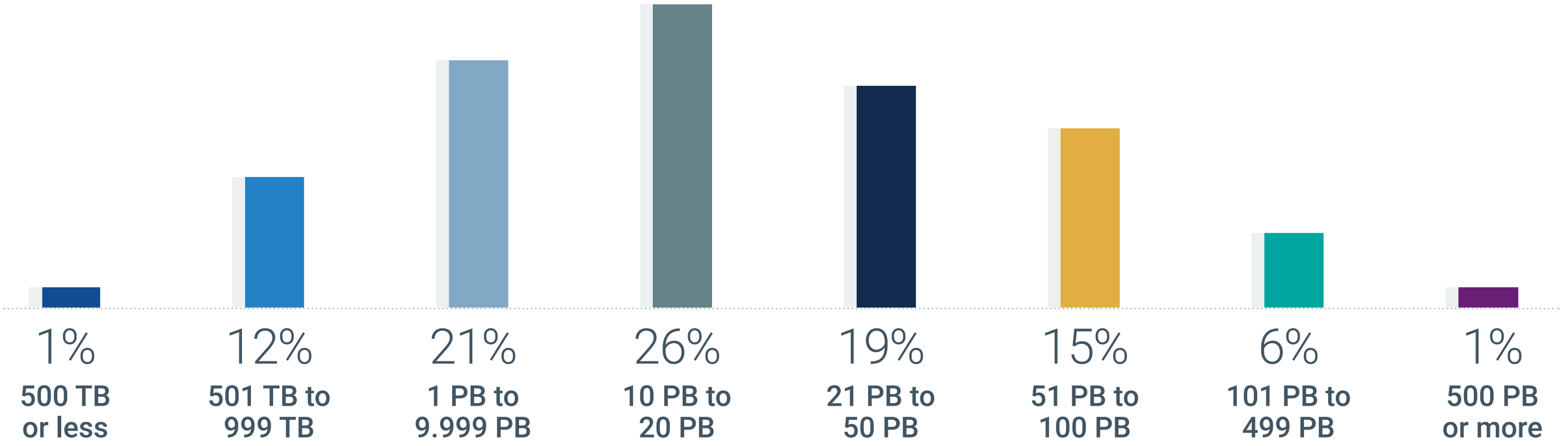


The Data Protection Gap Persists—and GenAI Exacerbates the Problem

Multi-petabyte Data Environments Are Now Standard as Organizations Manage Massive Digital Footprints

Two-thirds of organizations manage at least 10 petabytes of data, demonstrating that multi-petabyte environments have become standard rather than exceptional. On average, organizations manage 49 PB of data spanning all corporate storage resources, including cloud platforms.

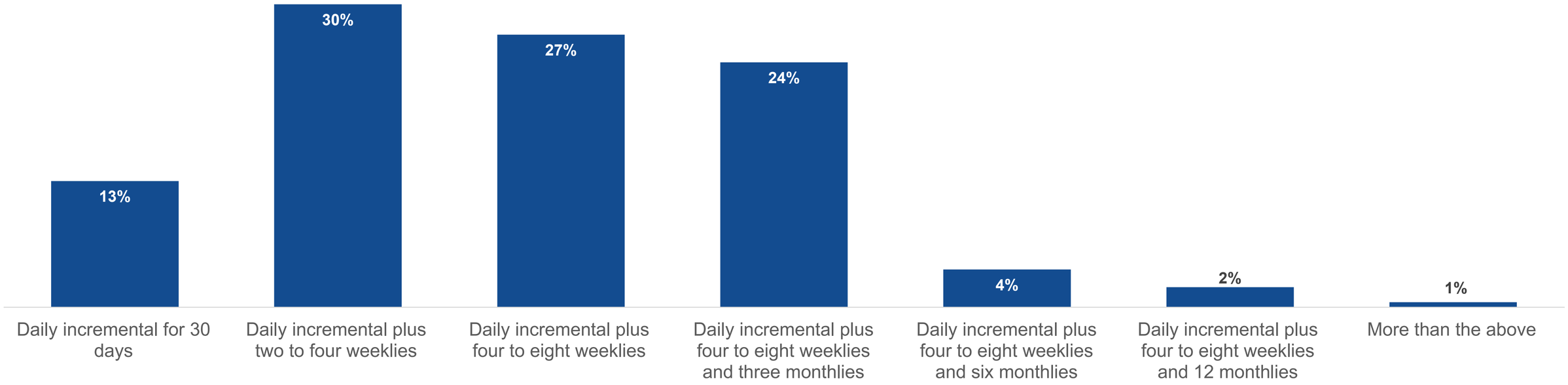
Approximate total volume of data stored on corporate storage resources.



Organizations Favor Moderate Backup Retention Policies With Limited Long-term Archives

Organizations typically implement backup retention policies focused on recovery scenarios, with most maintaining weekly backups and only a quarter extending to quarterly retention. Most organizations balance recovery capabilities against resource constraints rather than implementing extensive retention within their standard backup policies.

Organizations' standard backup retention policy.



Majority of Organizations Do Not Adequately Protect Both Mission-critical Applications and AI-generated Data

In terms of the extent to which mission-critical applications are protected by a solution that can ensure there is always a copy of uncompromised data from which organizations can restore, nearly two-thirds (64%) report protecting no more than 50%. On average, 47% of mission-critical applications are fully protected. More than eight in ten organizations protect 50% or less of their AI-generated data, indicating most AI outputs lack comprehensive backup coverage. The substantial percentage of unprotected AI-generated data suggests organizations may be underestimating the long-term value and compliance implications of these assets.

Approximate percentage of mission-critical applications protected by a solution that can ensure there is always a copy of uncompromised data.



Approximate percentage of organizations' total volume of AI-generated data that is regularly backed up.



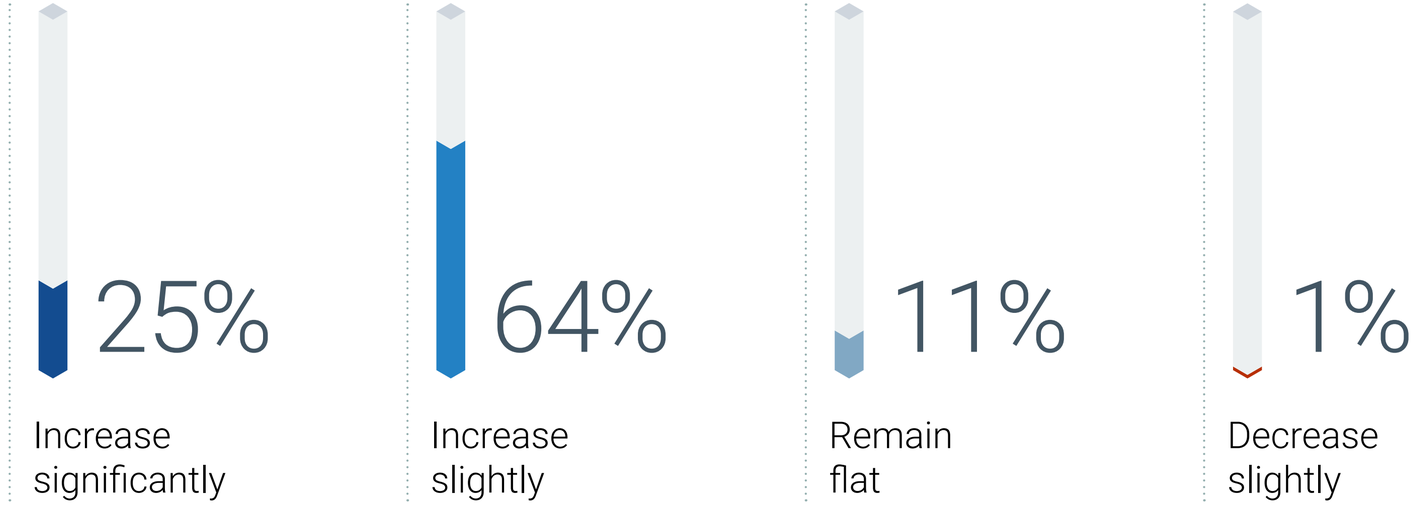


Most Organizations Plan to Ramp Up Data Protection Spending

Most Organizations Are Increasing Backup and Recovery Spending

Nearly nine in ten organizations expect to increase spending on their data backup and recovery solutions over the next 12 months. However, the majority (64%) plan modest spending increases rather than dramatic budget expansions, suggesting organizations are taking an evolutionary rather than revolutionary approach to strengthening their data protection capabilities.

Expected spending change for data backup and recovery solutions over the next 12 months.

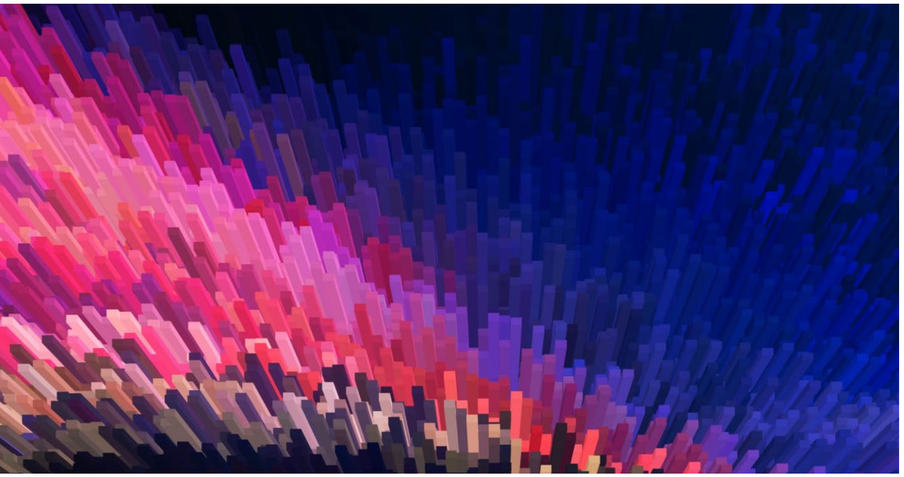




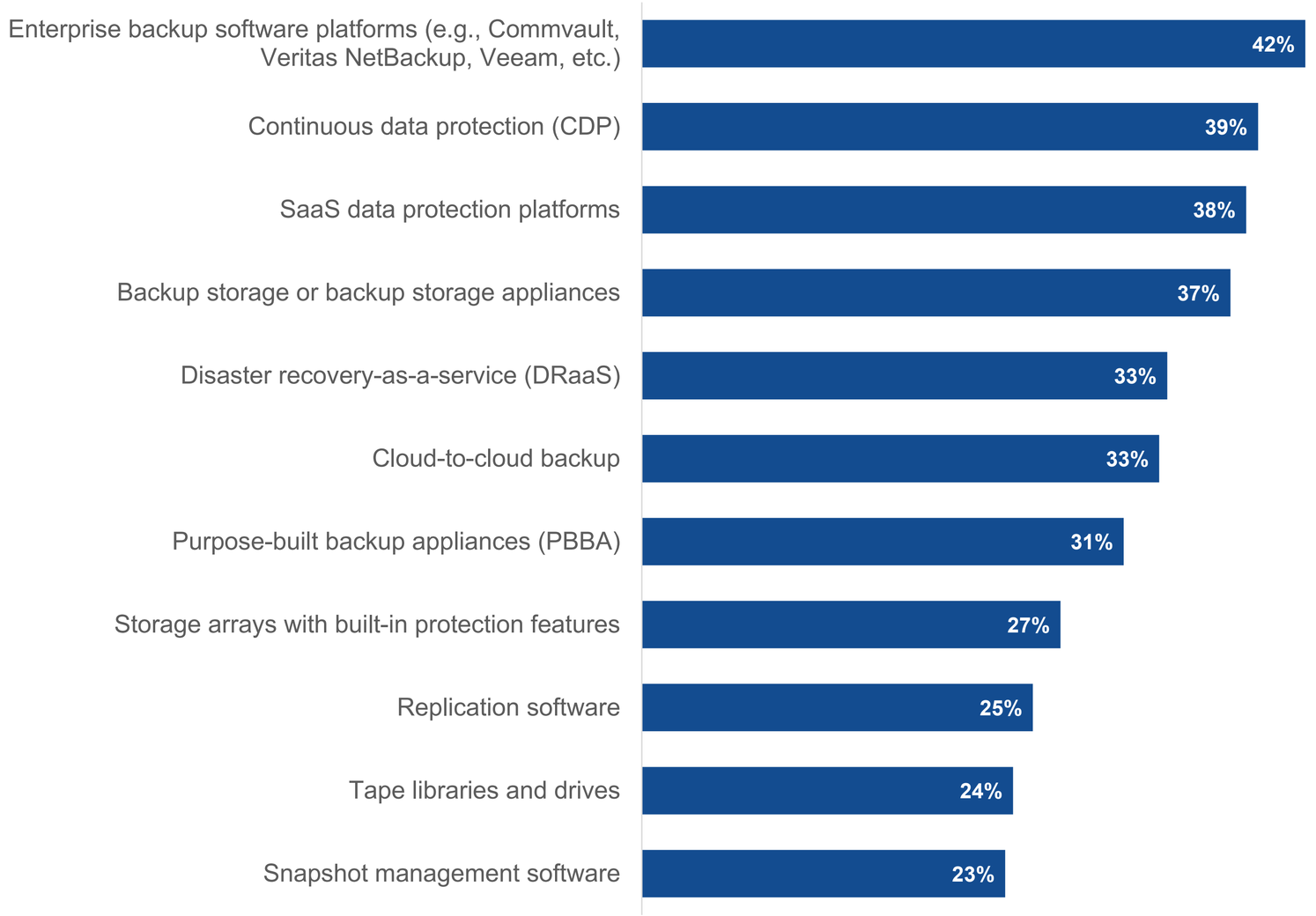
Enterprise Backup Platforms Lead Investment Priorities as Organizations Modernize Their Data Protection Portfolios

The strong interest in purpose-built backup appliances (31%) and backup storage appliances (37%) suggests organizations are investing in dedicated, hardened storage infrastructure specifically designed for ransomware resilience.

Despite being a legacy technology, tape libraries (24%) continue to see significant investment, likely due to their inherent air-gap properties that provide effective ransomware protection when properly implemented.



Data protection solutions organizations are likely to purchase in the next 12 months.



COHESITY

Cohesity is the leader in AI-powered data security. Over 13,600 enterprise customers, including nearly 70% of the Global 500, rely on Cohesity to strengthen their resilience while providing Gen AI insights into their vast amounts of data. Formed from the combination of Cohesity with Veritas' enterprise data protection business, the company's solutions secure and protect data on-premises, in the cloud, and at the edge.

LEARN MORE

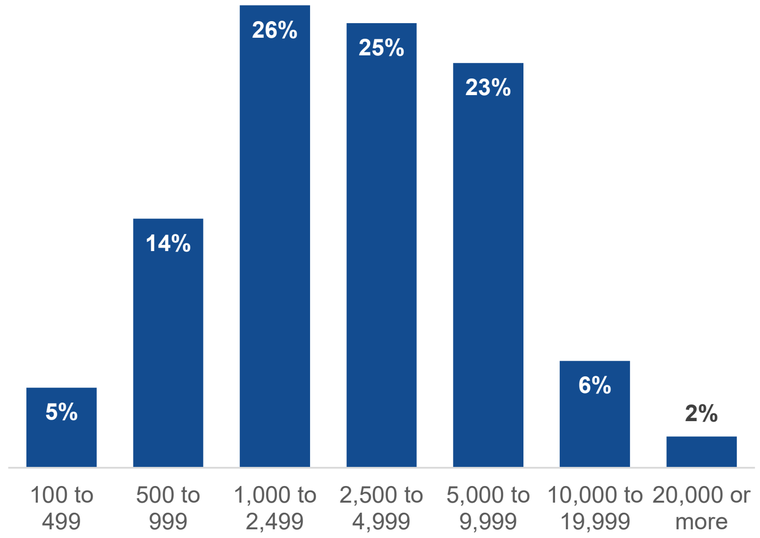


RESEARCH METHODOLOGY AND DEMOGRAPHICS

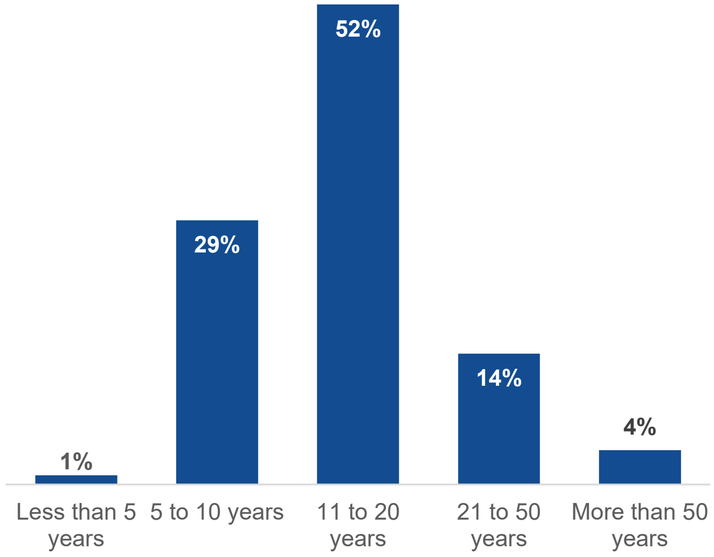
To gather data for this report, Enterprise Strategy Group conducted a comprehensive online survey of IT and data protection professionals from private- and public-sector organizations in North America between June 25, 2025, and July 2, 2025. To qualify for this survey, respondents were required to be involved with or responsible for evaluating, purchasing, managing, and building data protection and resilience solutions. All respondents were provided an incentive to complete the survey in the form of cash awards and/or cash equivalents.

After filtering out unqualified respondents, removing duplicate responses, and screening the remaining completed responses (on a number of criteria) for data integrity, we were left with a final total sample of 400 IT and data protection professionals.

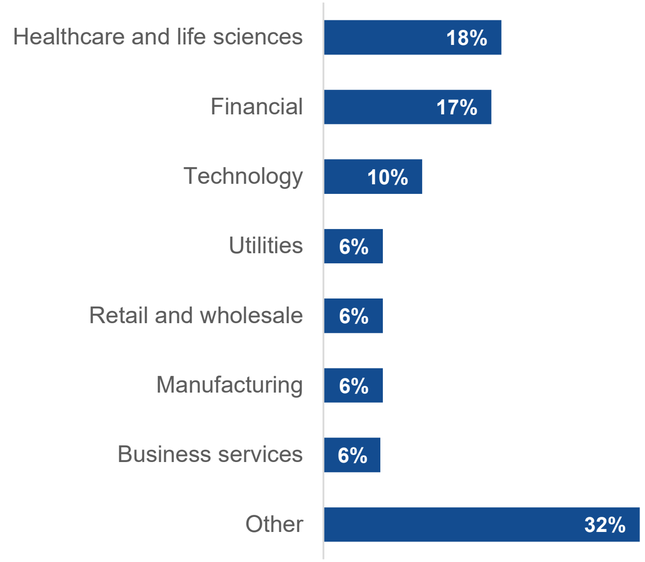
Respondents' organizations by number of employees.



Respondents' organizations by years in operation.



Respondents' organizations by industry.





Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

© 2025 TechTarget, Inc. All Rights Reserved.