DATAPRISE

Disaster Recovery in the Age of Ransomware:

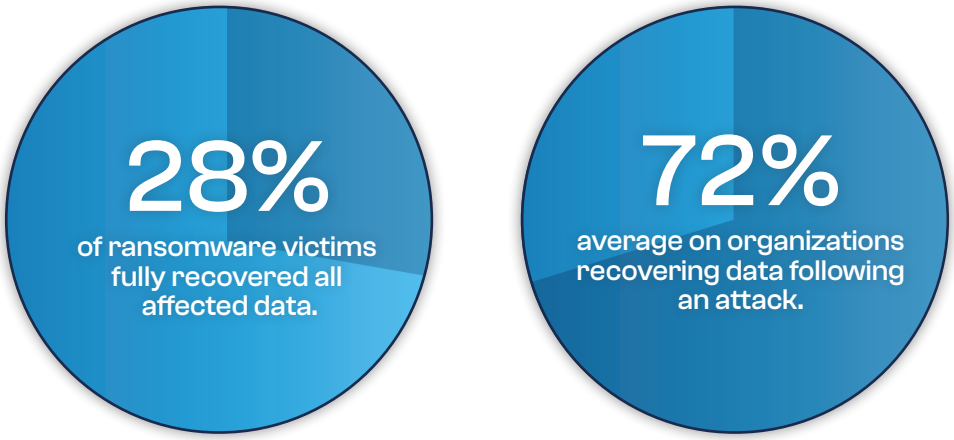
Why Traditional Backup Strategies Fail

DATAPRISE

INTRODUCTION

In today's interconnected world, downtime is no longer an IT inconvenience - it is a business risk with operational, financial, reputational, and regulatory consequences. It is a business risk with operational, financial, reputational, and regulatory consequences. As ransomware attacks grow more sophisticated and businesses accelerate AI adoption, traditional backup strategies are proving insufficient for modern resilience requirements.

Recent industry research reveals a widening gap between perceived preparedness and actual recovery capability. According to the 2026 Veeam Data Trust and Resilience Report, 90% of organizations believe they can recover from a cyber incident quickly, yet only 28% of ransomware victims fully recovered all affected data. On average, organizations recovered just 72% of impacted data following an attack.



Source: 2026 Veeam Data Trust and Resilience Report

Organizations that increased their BCDR budgets and strategy saw better outcomes. Only 33% paid a ransom, compared to 52% of those that did not increase their budgets. They also recovered more data, with 40% fully restoring their data versus just 16% of organizations without budget growth.

This disconnect highlights a critical reality: backup alone is no longer enough. In today's technology landscape, organizations requir a resilient, tested, and strategically aligned business continuity and and disaster recovery (BCDR) solution capable of supporting business continuity in increasingly complex environments.

At Dataprise, we believe resilience must move beyond recovery confidence and evolve into proven operational readiness. Businesses need solutions that not only protect data, but also ensure rapid restoration, secure recovery, and continuity of operations when disruption occurs.

The Modern Threat Landscape Has Changed

While these risks still exist and pose great harm to organizations that are under-prepared, today's most significant threats are cyber-drive.

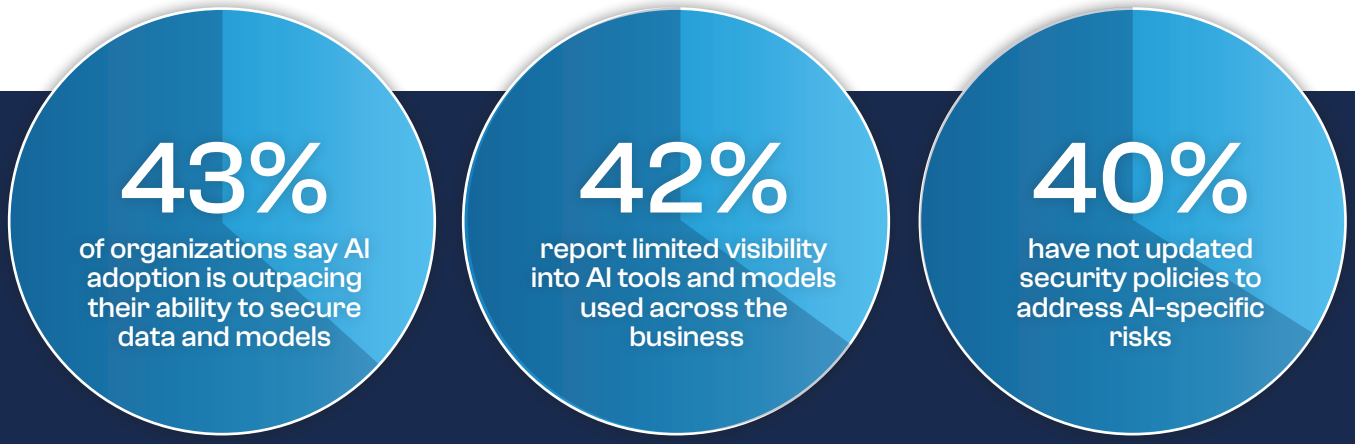
Ransomware attacks now routinely target backup infrastructure itself. Modern attackers spend days or weeks inside networks disabling recovery tools, corrupting restore points, and identifying critical systems before launching encryption attacks. Discussions among cybersecurity professionals increasingly emphasize that attackers intentionally compromise backup environments before triggering ransomware events.

The consequences are severe.

Organizations impacted by cyber incidents report:

- Extended downtime of critical systems
- Customer disruption
- Regulatory exposure
- Financial and revenue loss
- Operational paralysis

Even organizations with backup systems in place are discovering that incomplete testing, inconsistent policies, and outdated architectures prevent successful recovery during actual incidents.



As businesses integrate AI tools, cloud platforms, SaaS applications, and distributed workforces, the attack surface expands significantly. Data is now spread across hybrid environments, cloud platforms, endpoints, collaboration tools, and third-party applications. Without a resilient recovery strategy, organizations risk losing visibility, control, and recoverability.

veeam

Why Traditional Backup Approaches Fail

Many organizations still approach backup as a compliance checkbox rather than a strategic resilience function. Having backup jobs running does not guarantee recoverability.

Common weaknesses include:

Infrequent Recovery Testing
Many businesses rarely validate whether backups can actually be restored successfully. Backup success notifications may create false confidence, while corrupted or incomplete recovery points go unnoticed.

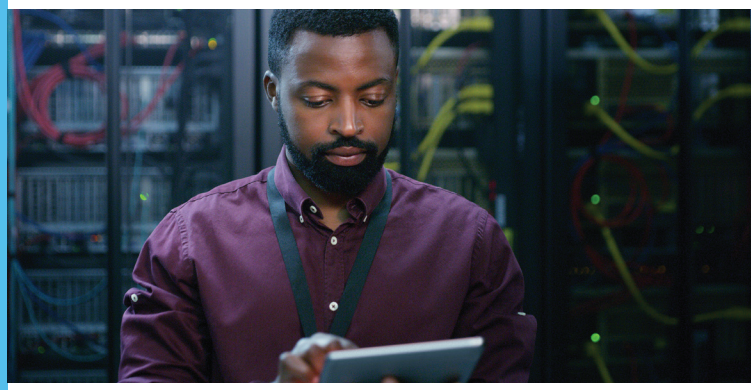
Lack of Immutable Storage
Without immutable backup protection, ransomware attackers may encrypt or delete backup repositories alongside production data.

Poor Recovery Prioritization
Organizations often lack clear recovery runbooks identifying:

- Critical applications
- Recovery dependencies
- Recovery time objectives (RTOs)
- Recovery point objectives (RPOs)
- Operational sequencing

SaaS Data Protection Gaps
Many organizations incorrectly assume Microsoft 365, Google Workspace, and other SaaS providers fully protect customer data. In reality, SaaS providers typically operate under shared responsibility models, meaning organizations remain responsible for backup and recovery of their own data.

Misalignment Between IT and Business Objectives
The Veeam report found that while 90% of organizations believe they can recover within RTO expectations, only 69% say those RTOs are fully aligned with actual business continuity goals. This gap often means IT teams restore systems successfully, but the business still experiences prolonged operational disruption.



Resilience Requires More Than Backup
Modern resilience requires a comprehensive strategy that combines these 6 items.

1. Secure backup architecture
2. Cybersecurity integration
3. Disaster recovery planning
4. Continuous testing
5. Governance and compliance
6. Operational continuity

A resilient backup and disaster recovery solution should include these 6 critical capabilities.

1. Immutable Backup Protection
Immutable storage prevents backup data from being modified or deleted, even by attackers with administrative access. This creates a secure recovery point organizations can trust during ransomware incidents.

2. Air-Gapped and Isolated Recovery Environments
Organizations increasingly use isolated recovery environments or clean-room recovery solutions to restore systems safely without reintroducing malware into production environments.

3. Automated Recovery Testing
Recovery validation should be continuous and automated wherever possible. Organizations need confidence that backups are recoverable before an incident occurs, not during one.

4. Hybrid and Multi-Cloud Protection

Modern environments require protection across:

- On-premises infrastructure
- Public cloud workloads
- SaaS applications
- Remote endpoints
- Hybrid environments

5. Cybersecurity and Backup Integration
Backup and cybersecurity can no longer operate independently. Effective resilience strategies integrate:

- Threat detection
- Identity protection
- Backup monitoring
- Incident response
- Security operations

6. Business-Centric Recovery Planning
Recovery planning must prioritize business operations, not just infrastructure restoration. Organizations should clearly define:

- Mission-critical applications
- Acceptable downtime
- Operational dependencies
- Communication workflows
- Executive accountability

The Cost of Inadequate Recovery

Organizations often underestimate the true financial impact of downtime.

Beyond direct operational disruption, businesses face:

- Lost productivity
- Revenue interruption
- Customer attrition
- Regulatory penalties
- Legal exposure
- Brand damage
- Recovery consulting costs
- Cyber insurance complications

Industry reporting notes that outages may cost organizations hundreds of thousands — and in some cases millions — of dollars per hour depending on the industry and operational dependency on technology. For mid-market organizations especially, prolonged downtime can become existential. Unlike large enterprises with extensive recovery resources, midsize businesses frequently lack redundant infrastructure, dedicated recovery teams, or in-house cybersecurity expertise.

> **This is why resilience planning has become a board-level business priority rather than solely an IT initiative.**

DATAPRISE

What Resilient Organizations Do Differently

The organizations achieving stronger recovery outcomes share several characteristics.

According to Veeam's industry accredited reports, stronger performers consistently demonstrate:

1. Clear visibility into enterprise data and AI risk
2. Enforced security controls
3. Proven recovery through realistic testing
4. Executive alignment on ownership and recovery expectations

Additionally, organizations increasing cybersecurity and resilience investments reported significantly stronger recovery results. Companies with increased budgets achieved full recovery at much higher rates than those without additional investment.

High-performing organizations also treat resilience as an ongoing operational discipline rather than a one-time project. They continuously:

- Test backups
- Update runbooks
- Validate recovery processes
- Audit access controls
- Monitor backup environments
- Train staff
- Simulate incident scenarios

The Dataprise Approach to Resilience

At Dataprise, we help organizations modernize backup and disaster recovery strategies to support today's evolving threat landscape and operational demands.

Our approach focuses on:

- Business continuity alignment
- Secure and immutable backup architecture
- Hybrid cloud protection
- Disaster recovery readiness
- Recovery testing and validation
- Cyber resilience integration
- Strategic advisory and governance

We recognize that recovery success is not measured by whether backups exist. It is measured by how quickly and effectively organizations can restore operations, protect customers, and maintain business continuity under pressure.

As AI adoption accelerates and cyber threats continue evolving, resilience must become proactive, operational, and measurable.

The modern business environment demands a new approach to backup and disaster recovery. Organizations can no longer rely on assumptions, outdated recovery plans, or untested backup systems.

The reality is clear:

- Cyber threats are growing more sophisticated
- AI is expanding operational complexity
- Downtime costs continue rising
- Regulatory scrutiny is increasing
- Traditional backup strategies are failing to deliver complete recovery

The organizations best positioned for the future will be those that move beyond recovery confidence and invest in proven resilience.

A resilient backup and disaster recovery strategy is no longer optional. It is a foundational business requirement for operational continuity, cybersecurity readiness, and long-term business success.