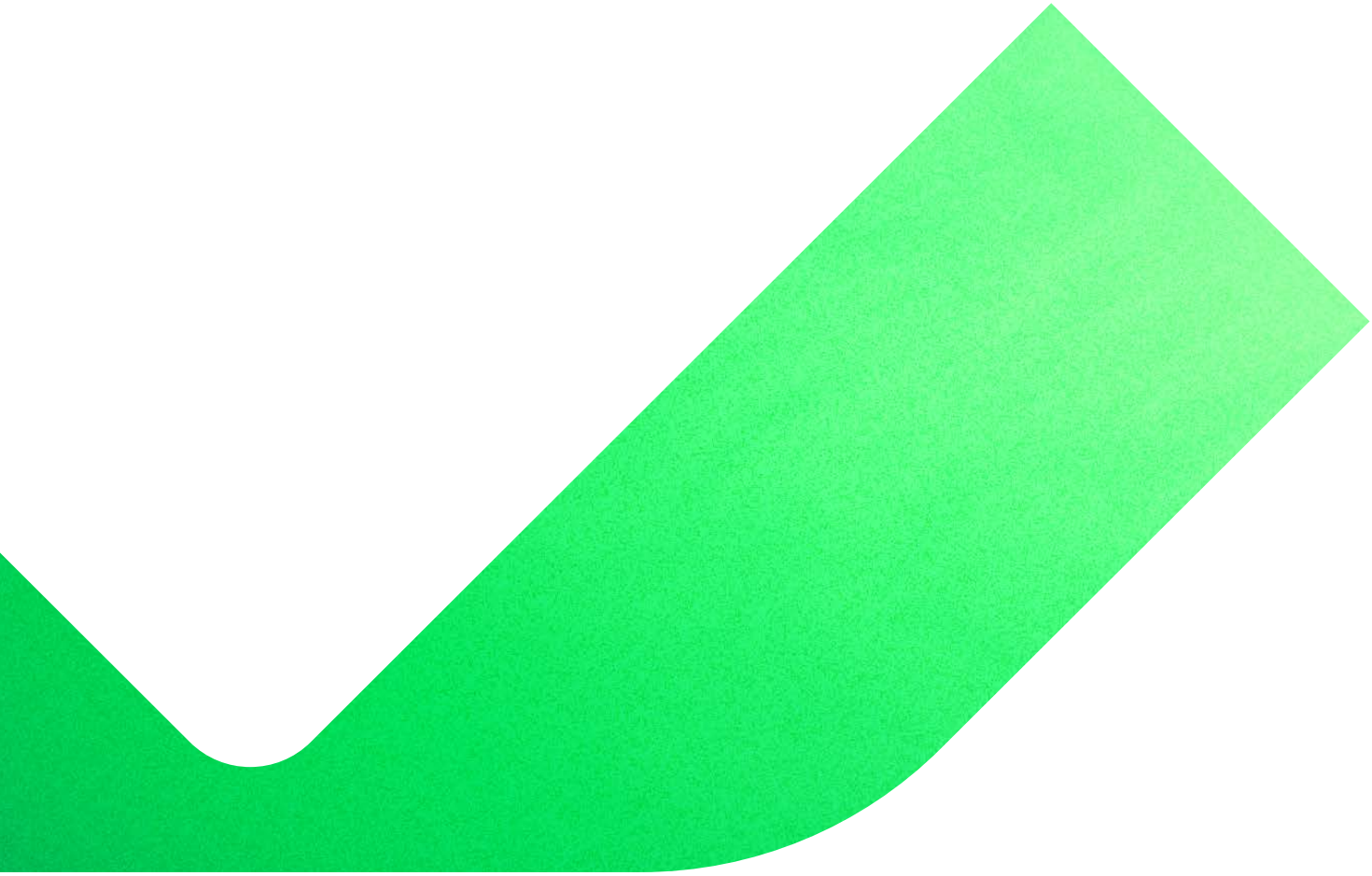
The New Recovery Reality

Emerging Trends and a Checklist for Evaluating Modern Resilience



Introduction

The pace of digitalization, the rise of hybrid and multi-cloud environments, and the growing reliance on SaaS and AI models have reshaped how data is created, stored, and protected. At the same time, cyberthreats have become more targeted, more frequent, and far more disruptive. In this changing world, resilience can't be left to chance. Reliable resilience depends on comprehensive, tested, and secure recovery frameworks so enterprises can adapt as business needs and threat models evolve. These are no longer simply boxes to check; they are essential to keeping your organization running no matter what.

This paper is intentionally structured to cover the following:

Recovery essentials: Five foundational capabilities every enterprise should already have in place to support reliable recovery right now.

What's next: Five emerging trends that are reshaping how recovery must evolve to stay effective tomorrow.

The readiness checklist: A practical self-assessment tool to help organizations evaluate their current recovery posture, identify gaps, and prioritize next steps.



Note: While you may use the link above to jump directly to the checklist, doing so skips important context. The **Essentials** and **What's Next** sections explain why each checklist item matters and how the criteria within build on one another.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

The Essentials: Bases You Should Already Have Covered

Before preparing for recovery challenges, ensure the foundational elements of resilience have already been addressed.

1. Take inventory of your backup architecture

A clear, well documented backup architecture is key to resilience and compliance. Before you can strengthen your recovery or meet regulatory standards, you need full visibility into what's protecting your data. Start by mapping every backup system across your environment, from on-premises infrastructure to cloud and hybrid deployments. Document what's in place, who manages it, and how each system contributes to your overall data protection strategy. Don't just stop at a high-level list. Capture the details that matter, including:

- Software versions you currently use.
- Platforms you protect, such as virtual machines (VMs), databases, file systems, and SaaS applications.
- Integration points that tie these systems together.
- Workloads containing data are essential to the business.

The trend: This exercise often reveals overlaps, inconsistencies, or aging components that can slow down recovery or create compliance blind spots. It's also the first step toward understanding where your most valuable data lives and how well it's being protected.

The gotcha: This inventory is the first step to identifying what you will need to get your business back up and running. Replication isn't the same as backup. While replication helps with availability, it can also mirror corrupted or ransomware encrypted data.

2. Define your recovery objectives

Having clear recovery objectives is also particularly important since it helps connect your technical capabilities to your business priorities. This helps ensure your recovery efforts can support what matters most to your business outcomes when disruption strikes.

Start by defining recovery time objectives (RTOs) and recovery point objectives (RPOs) for every critical workload. Then, classify your systems based on business criticality. This includes outlining what absolutely must be restored first, what can wait, and what can operate in a reduced state. This clarity helps align IT decisions with business expectations and budget realities.

The trend: This is not just an exercise in documentation. These targets shape everything that follows, including your technology choices, testing cadence, and overall confidence in recovery performance.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

The gotcha: Keep your goals practical, and back them up with automation and orchestration. Targets that look good on paper won't help if they can't be achieved. Unrealistic RTOs or RPOs can create a false sense of security and leave your recovery at risk when you need it most.

3. Build out regular backup and retention policies

Consistent, well-defined backup and retention practices are what turn your recovery plans from theory into something you can count on when the unexpected happens. Start by setting clear daily backup policies — whether they're full, incremental, or differential — and pair them with long-term retention schedules that support business continuity and regulatory compliance. Regularity and structure also help ensure that no data is left unprotected, and that older backups are available if you ever need to roll back further than expected.

The trend: Equally important is where those backups live. Store them securely offsite or in the cloud, so your data remains safe even if your primary site is compromised. Separation is what protects you from site level outages, hardware failures, or localized cyber incidents.

The gotcha: A scheduled backup that never leaves the primary environment isn't really protection. Without secure offsite or cloud copies, a single disaster could take both your production data and your backups offline, which could leave recovery out of reach.

4. Ensure comprehensive backup coverage

Gaps in coverage are one of the biggest threats to resilience. You can have strong policies and solid recovery plans, but if a single workload isn't protected, that's all it can take to disrupt operations or put compliance at risk.

A complete strategy should span every layer of your environment — from on-premises infrastructure to cloud workloads (e.g., IaaS and PaaS) and SaaS applications like Microsoft 365 and Salesforce. Each layer has unique data ownership and recovery responsibilities, so understanding where those lines are drawn is key.

The trend: Gartner predicts that by 2028, most enterprises will need dedicated SaaS backup strategies to keep pace with growing data volume and shared responsibility models. This is a reminder that coverage can't stop at infrastructure; it must extend to every application that drives your business.

The gotcha: Vendor native protection only goes so far. Built-in tools often focus on availability, not long-term recoverability. Evaluate whether third-party solutions could help you maintain complete control of your data and ensure recovery on your terms.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

5. Place strong security controls on your backup systems

Security isn't just about keeping attackers out. It's about making sure your recovery foundation can't be compromised when you need it most. Backups are often the final safeguard after an incident, so they must be protected with the same rigor as your production data.

Start by reinforcing your backup infrastructure with layered controls, including:

- **Encryption** for data in transit and at rest.
- **Role-based access control (RBAC)** and **multi-factor authentication (MFA)** to limit unauthorized access.
- **WORM storage** to prevent tampering and strengthen ransomware defense.

The trend: These measures prove resilience in action. Robust security controls help ensure that even if a cyberattack penetrates primary systems, your backups remain intact, trustworthy, and ready to restore.

The gotcha: Ransomware now targets backups directly. Immutability isn't optional anymore — it's the baseline for modern protection and recovery confidence.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

The New Reality: Getting Ready for What's Next

Now that we have covered recovery essentials, let's look at emerging trends that we need to plan for.

1. SaaS and cloud-native protection

As organizations lean further into cloud adoption, the boundaries of data protection are changing. Resilience and compliance must extend to every SaaS and cloud-native application that keeps business running. Start by formalizing a backup strategy for all SaaS and cloud-native workloads. Define how APIs, export and restore workflows, and service level agreements (SLAs) fit into your recovery objectives. Having clarity with this ensures that data stored across multiple platforms can be recovered consistently, no matter where it lives. Define how APIs, export and restore workflows, and SLAs fit into your recovery objectives.

The trend: More critical workloads than ever now operate in the cloud. That shift demands consistent protection and recoverability across every environment, not just for operational continuity, but to sustain confidence in compliance and governance.

The gotcha: Not all SaaS and cloud-native platforms offer the same depth of backup or recovery capabilities. API limitations, vendor-managed retention policies, or incomplete restore options can create blind spots that only appear during an incident. Validating restore paths and understanding provider responsibilities upfront is critical to avoiding false assumptions about recoverability.

2. Hybrid and multi-cloud support

As more organizations distribute workloads across multiple cloud providers, unified protection has become essential for both resilience and compliance. The complexity of hybrid environments means that visibility, governance, and recovery must work together — not in silos.

Your data protection strategy should deliver consistent oversight and recoverability across every environment you operate in. A unified control plane can help manage backup policies across clouds, while regular cross cloud restore confirms that data remains portable and recoverable wherever it's stored.

Aligning policies and workflows between platforms like Azure, AWS, and others eliminates coverage gaps and ensures recovery can run smoothly when it matters most. With multi-cloud adoption accelerating, flexibility and control are now equally critical to long-term resilience.

The trend: Multi-cloud backup is gaining traction because it gives organizations the flexibility to scale and adapt as their business needs evolve.

The gotcha: Inconsistent cloud policies can silently create protection gaps that only surface during recovery. Regular audits and standardized governance help close those gaps before they become real risks.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

3. Automated recovery workflows

As IT environments become more distributed and dynamic, automation emerges as a cornerstone of resilience and compliance. Manual recovery processes can slow response times and introduce human error, but automation enables consistency, accuracy, and speed when every minute counts.

Start by implementing automated failover and failback procedures and integrating runbooks with orchestration or automation tools. These workflows help standardize recovery operations, so systems respond predictably (not reactively) under pressure.

Automation should never be a "set it and forget it" approach, however. Regular testing is essential to confirm that automated actions perform as intended. Proper configuration and validation make automation a strength, not a risk.

The trend: Automation reduces reliance on manual intervention, saving time, and minimizing the potential for human mistakes.

The gotcha: Automation can fail too. Misconfigured scripts or overlooked dependencies can trigger the very outages they're meant to prevent. Regular testing and documentation keep automation reliable and ready when it's needed most.

4. Predictive and AI assisted backup

Traditional monitoring reacts after something goes wrong, but AI and ML-driven analytics can provide a proactive edge by spotting anomalies in backup performance and triggering alerts before failures occur.

The trend: By learning from patterns across backup jobs, storage systems, and recovery operations, predictive tools can highlight risks early and recommend preventive action. This means fewer surprises, faster remediation, and stronger assurance that your data is protected long before issues surface.

The gotcha: AI insights are only as good as the data and configurations behind them. Incomplete telemetry, poor data quality, or overreliance on automated recommendations can lead to missed risks or unnecessary alerts. Human oversight and clear thresholds remain essential to ensure predictive tools enhance — rather than replace — sound backup governance.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

5. Immutable and air-gapped backup

Protecting backup data is every bit as important as protecting your production systems. Resilience and compliance both hinge on preserving secure, isolated copies that can't be compromised by ransomware or accidental corruption.

Establish offsite, air-gapped backups and vault snapshots with immutability to ensure data cannot be modified or deleted. These layers of separation create a trusted recovery source; one that maintains data integrity, satisfies retention requirements, and keeps your organization ready to recover at any moment.

True resilience means planning for worst-case scenarios. When your backups are immutable and isolated, you can recover with confidence knowing that your last line of defense is beyond the reach of attackers or system failures.

The trend: It's now essential to defend your backups as thoroughly as you defend your data. Immutable and air-gapped protection have become standard practices for maintaining trust and continuity in a threat-filled landscape.

The gotcha: Immutability and air gaps don't automatically guarantee recoverability. Misconfigured retention policies, inaccessible vaults, or untested restore procedures can turn secure backups into unusable ones. Regular validation, access reviews, and recovery testing ensure your last line of defense is both protected and usable when it matters most.

A Checklist for the New Recovery Reality

Insights are only valuable when they lead to action. Having reviewed recovery essentials and emerging trends, it's time to evaluate your current recovery status.

The following checklist is designed to help you prioritize enhancements across your backup and recovery strategy so you can close critical gaps, strengthen recovery confidence, and build resilience against expected outages and unforeseen disruptions.

This is meant to be used as a guide to help you access where your organization stands today and where you should focus your attention next. Each area represents a building block of operational strength, from architecture and automation to governance and testing.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Criteria Checklist: Evaluate Your Current Recovery Status

Your final total score will measure how far along the maturity road your organization is.

In the categories below, each answer is worth a possible 4 maximum points. (Yes = 4, Partial = 2, No = 0)

Total /100 → Percentage

- ≥ 80%: Good baseline
- 50–79%: Needs improvement
- < 50%: At risk; prioritize remediation

1. Backup Coverage

Item	Yes	Partial	No
Points	**4**	**2**	**0**
On-premises servers are backed up			
Cloud IaaS workloads are backed up			
SaaS apps are protected separately			
VM workloads are protected			
Cloud-native workloads are protected			
AI workloads are protected			
Total points per column			
Total points for this category (Max. 24 possible)			

Key takeaway: Missing any critical workload means potential business interruption.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

2. Restore and Recovery Testing

Item	Yes	Partial	No
Points	**4**	**2**	**0**
File-level restore has been tested			
VM image restore has been tested			
Full disaster simulation has been completed			
SaaS data restore has been tested			
Container and VM restore has been tested			
Total points per column			
Total points for this category (Max. 20 possible)			

Key takeaway: Backups that never get restored are worthless. Restore testing finds corruption and misconfigurations early.

3. Security and Compliance

Item	Yes	Partial	No
Points	**4**	**2**	**0**
Backup encryption is implemented			
Role-based access control (RBAC) is enforced			
Immutable storage in place			
Backup data meets compliance (GDPR, HIPAA, etc.)			
Total points per column			
Total points for this category (Max. 16 possible)			

Key takeaway: Security controls on your primary environment do not automatically extend to backup stores.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

4. Architecture and Performance

Item	Yes	Partial	No
Points	**4**	**2**	**0**
RTOs and RPOs documented			
Instant Recovery capabilities are accounted for			
Deduplication/compression is enabled			
Total points per column			
Total points for this category (Max. 12 possible)			

Key takeaway: Deduplication helps costs but can complicate recovery if not configured correctly.

5. Operational Practices

Item	Yes	Partial	No
Points	**4**	**2**	**0**
Do you complete monthly restore drills?			
Step-by-step recovery runbooks have been written and released to stakeholders			
Identity, access, and dependency readiness validation during recovery			
Contact lists and escalation paths have been planned out			
SLAs with BaaS/DRaaS providers have been confirmed			

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Item	Yes	Partial	No
Points	**4**	**2**	**0**
Escalation terms and support coverage have been reviewed			
Daily backup and restore success rate and MTTR (meant time to restore) are measured and acted on			
Total points per column			
Total points for this category **(Max. 28 possible)**			

Key takeaway: Without consistent measurement, the enterprise does not have clear pictures of overall recovery health. Many organizations schedule backups but never test restoration, which still leaves them vulnerable.

Final readiness scorecard (0-100), 5 Key Areas

Category	Your Score	Max
Backup Coverage		24
Restore and Recovery Testing		20
Security and Compliance		16
Architecture and Performance		12
Operational Practices		28
Total		**100** %

Total /100 → Percentage

- ≥ 80%: Good baseline
- 50–79%: Needs improvement
- < 50%: At risk; prioritize remediation

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.

Conclusion

As enterprises continue to contend with growing data volumes, distributed infrastructures, and an increasingly complex threat environment, the effectiveness of backup and recovery capabilities directly influences operational continuity and business competitiveness.

The new recovery reality demands not only robust backup coverage and rapid restoration, but also proactive security, automation, and regular validation of recovery plans to meet aggressive business continuity objectives.

Ultimately, strong backup and recovery operations are not just IT functions — they are foundational enablers of organizational stability, customer trust, and long-term growth.

© 2026 Veeam Software. Confidential information. All rights reserved. All trademarks are the property of their respective owners.