rubrik

SELF-ASSESSMENT

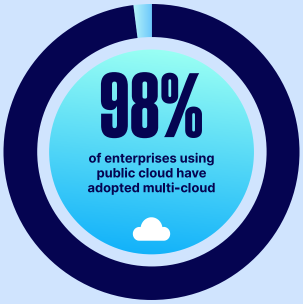
When “Good Enough” Cloud Backup Isn’t Good Enough

Is your cloud data protection strategy truly keeping pace with your evolving business needs—or leaving you vulnerable? While native cloud tools like AWS Backup, Azure Backup, and Google Backup and DR Service offer straightforward deployment and baseline protection, the gap between ‘good enough’ and ‘truly protected’ widens as your footprint expands and cyber threats to your data escalate.

This brief assessment helps you determine whether your current approach aligns with your organization’s security and compliance demands—or if it’s time for a more robust solution.

Q1 Do you manage workloads across multiple or hybrid cloud environments?

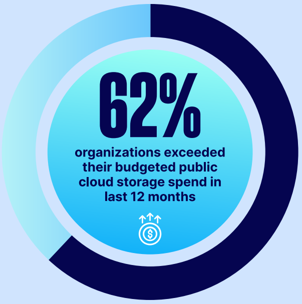
YES **Why it matters:** Native cloud backup tools are built for protecting their own environments but weren’t designed for multi-cloud or on-premises environments. This creates management silos requiring separate expertise, policies, and monitoring across different platforms. And during critical recoveries, you’re forced to juggle multiple interfaces and inconsistent processes—precisely when you need seamless, unified operations most.



Source: 451 Research, S&P Global Market Intelligence

Q2 Do you find it challenging to track and optimize your organization’s backup and data storage costs?

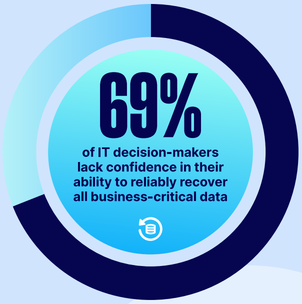
YES **Why it matters:** Native cloud backup tools often fall short in two key cost areas: they don’t allow immediate archiving to lower-cost tiers, and they bury backup expenses in complex billing statements. As a result, you could be overpaying for storage without a clear view of your true costs leading to dramatic cost increases overtime—a blind spot that purpose-built solutions eliminate with transparent reporting and intelligent tiering.



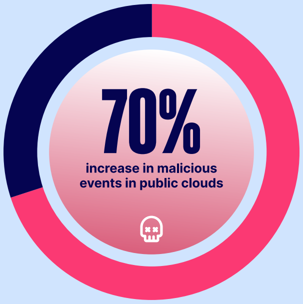
Source: 2025 Cloud Storage Index Report, Wasabi

Q3 Are you still unsure whether your team can meet your organization’s recovery time objectives in real-world scenarios?

YES **Why it matters:** Meeting RTOs isn’t just about system capabilities—it’s about proven processes. Native tools often require multi-step recoveries and full container restores that can add critical hours to recovery time. When every minute of downtime costs your organization, these limitations transform from technical concerns to business risks.



Source: 2024 VMware Cloud Disaster Recovery report



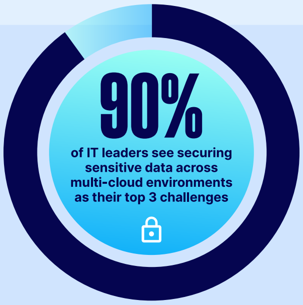
Source: The State of Data Security: Measuring Your Data's Risk (Rubrik Zero Labs)

Q4 Are you uncertain about your ability to identify a clean recovery point and restore operations if hit by ransomware today?

YES **Why it matters:** In the critical moments following an attack, native cloud backup tools may leave you searching for answers: Which backups are unaffected? When did the infection begin? Without advanced detection capabilities and clear visibility into data integrity, you face uncertainty precisely when decisive action matters most.

Q5 Do your compliance requirements mandate knowing exactly where sensitive data resides in your cloud environments?

YES **Why it matters:** Regulations such as DORA, PCI, HIPAA, SOC2 etc. increasingly require organizations to maintain complete visibility into protected data categories. Native tools typically focus on storing data, not classifying or tracking it—creating potential blind spots that can lead to compliance failures, data breaches, and significant financial penalties.



Source: The State of Data Security: A Distributed Crisis (Rubrik Zero Labs)

Native Cloud Backup Tools	Third Party Backup Tools
☒ Cloud-Specific	✓ Multi & Hybrid Cloud
☒ Limited Cost-Optimization	✓ Cost-Optimized Tiering and Retention
☒ Complex and Inconsistent Recovery	✓ Complete and Rapid Recovery
☒ Lack Ransomware Recovery Support	✓ Advanced Ransomware Detection & Response
☒ Lack Visibility into Sensitive Data	✓ End-to-End Sensitive Data Visibility & Classification

CONCLUSION

As your environment evolves, 'good enough' may no longer keep your data truly secure. Each question reveals where native cloud backup tools can fall short—be it complexity, cost, security, or compliance. The table above summarizes how advanced solutions can bridge these gaps. If any of these questions resulted in a 'yes,' you need a third-party solution like Rubrik to protect your business-critical cloud workloads. We invite you to learn more and discover how you can strengthen your cyber resilience against today's most sophisticated threats.

Learn More ›

Watch Demo ›

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

Rubrik (NYSE: RBRK) is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit www.rubrik.com and follow @rubrikInc on X (formerly Twitter) and Rubrik on LinkedIn.