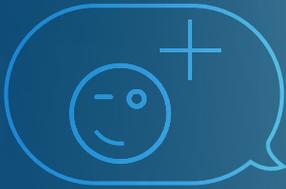


e⁺

rubrik

EBOOK

Selecting a Backup & Recovery Solution for Today and Tomorrow



A Datatude Adjustment with Rubrik & ePlus

Rubrik and ePlus have joined forces to deliver a solid remediation plan that meets the threat of ransomware head-on by arming data-dependent organizations with immutable technology, strategic insight, and unmatched expertise.

This partnership combines Rubrik's simplified and automated data management, instant recovery from ransomware, and secure archive to the cloud with the engineering expertise of the ePlus Managed Services team to support setup, configuration, optimization, and management.

Now organizations can make their data work harder for them by making their backup solution the key to improved business continuity, cloud mobility, multi-cloud management, and regulatory compliance. And the tight integration created by ePlus running their own Cloud Managed Backup service on Rubrik allows a sharper focus on improving customers' business outcomes.

With confident ransomware recovery made possible by the Rubrik/ePlus partnership, organizations will realize a fast track to the cloud and a path to operational excellence that positions them strongly for the future.



SELECTING A BACKUP AND RECOVERY SOLUTION FOR TODAY AND TOMORROW

Changing backup vendors always requires some level of technical or organizational effort. So, if you're considering a change, here are some questions to ask: Is the backup solution something that has been around for years with little change? Is it something created from multiple company acquisitions that have been cobbled together? Does it require multiple systems and interfaces for managing backup and recovery, replication, archival, and compliance? Does it require dedicated employees with specialized skillsets to manage it? What kinds of professional services will this change require? What kind of personnel training?

You will want to know not only how well a new solution will accommodate the complexities of the environment you currently have, but even more importantly, how well it will support the environment you will have in the future. If in that future environment you see a widening array of applications and technologies—from locally attached network-attached storage (NAS) appliances to cloud archives, from SaaS offerings to NoSQL databases—you need to be sure that the vendor you select can provide the support you will need to achieve your vision.

Backup innovation begins with recognizing that a new approach needs to align with the dramatic technology changes and data growth in centers over the past decade. Today, there are new approaches from industry visionaries who understand how to meet business needs in a period of rapid change.



Our team is small, but efficient and effective. We can accomplish great things with the relevant technology, which is why we partner with best-of-breed solutions like Rubrik. Not only does the solution fit nicely into our company initiatives, but also there's immense potential for the future.

Shadrach Kisten

CTO, Sesame Workshop

CLOUD DATA MANAGEMENT

Cloud Data Management services should be designed to orchestrate the management of mission-critical application data regardless of where it resides—whether in on-premises datacenters or within private and public clouds—while unifying backup, instant recovery, replication, search, analytics, archival, compliance, and copy data management in one infinitely scalable, cloud vendor-agnostic software fabric. Any solution built for the cloud generation should be able to take advantage of policy-based automation to manage data programmatically throughout its life cycle. It should be able to use APIs to facilitate data management functions across multiple applications, clouds, and protocols—ensuring the flexibility you need without locking you in to any particular cloud.

COMPREHENSIVE PLATFORM SUPPORT

A modern backup and recovery solution should support, optimize for, and integrate with *all* of the elements in your IT environment. Those might be physical elements, from sandboxed NAS systems to server clusters running SQL Server, MySQL, PostgreSQL, Cassandra, MongoDB, or some other production database. They could be virtual elements built on VMware, Hyper-V, Nutanix, or something else. The elements might not even belong to you but to AWS, Google Cloud Platform, Microsoft Azure, or some other cloud provider.

Your infrastructure needs are ultimately driven by your vision, your customers, and the opportunities that lie before you. Your backup and recovery systems should help you achieve your goals, not constrain or leave vulnerable the infrastructure that will enable you to reach your goals. That calls for solutions built on openness, flexibility, extensibility, and comprehensive platform manageability.



We're growing 33% year over year in server workloads; automation is the only way to maintain that growth.

Brandon Morris

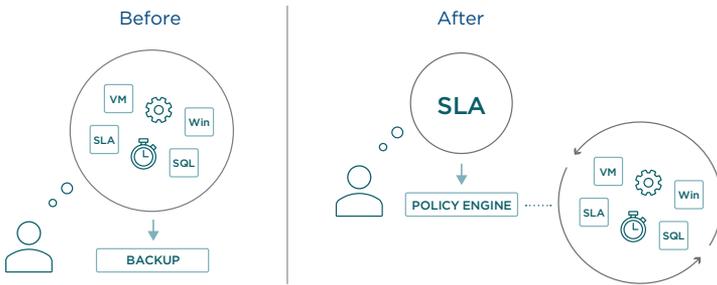
Systems Administrator, City of Sioux Falls

A DECLARATIVE POLICY ENGINE AND AUTOMATION

As IT departments come to rely more heavily on IT generalists, older backup management strategies that relied on imperative scripting techniques have become too complicated to sustain. Backup systems that anyone can manage have become non-negotiable for many organizations.

Modern backup and recovery systems can be managed by generalists when they take advantage of a declarative management model. In a declarative management model, an admin enters the desired state for a workload into a policy engine. After a policy is set, the system automatically and intelligently executes the jobs that need to be performed to achieve that state.

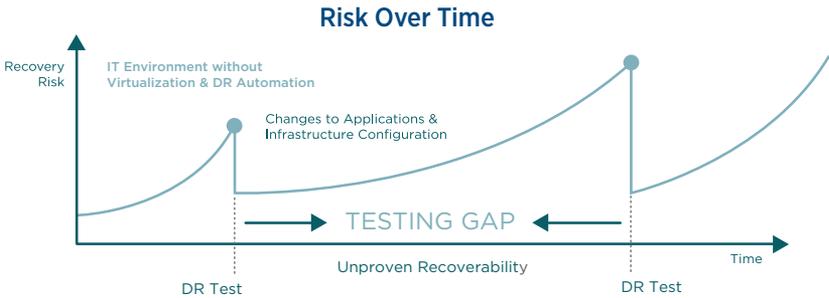
Let Your Policy Engine Do the Thinking



SLA policies allow you to collapse multiple manually implemented settings into a single easy-to-configure and zero-maintenance policy.

A strong policy engine can facilitate other aspects of service automation as well, reducing the number of manual steps that a generalist IT admin might otherwise be required to undertake to accomplish a task. If the backup and recovery solution has an API-first architecture, the organization gains even greater benefits. An admin could use these capabilities to integrate backup and recovery into an IT service catalog (e.g., ServiceNow, VMware vRealize Automation, or vCloud Director), simplify management of large, distributed environments via configuration management or IaC tools (e.g., Puppet, Chef, SaltStack, and Ansible), automate lifecycle data-management workflows, and centralize monitoring and reporting (e.g., Splunk or custom monitoring dashboard).

Additionally, automation enables regular backup validation—a requirement to mitigate the “testing gap” risk, as shown in the illustration that follows. If backups aren’t tested regularly, IT cannot guarantee their validity to the business.



Without regular testing, guaranteeing reliable restores is impossible.

SECURITY AND COMPLIANCE

In the area of security and compliance, today’s IT teams need to do much more than use OS tools to monitor system events and manage access control lists (ACLs). Data security today involves encryption both at-rest and in-transit, key management, and the ability to instantly recover from events ranging from system failure to data breaches and ransomware attacks. Depending on the industry in which you are operating (as well as the countries in which you are operating), you might be subject to regulations ranging from the Health Insurance Portability and Accountability Act (HIPAA) to the EU’s General Data Protection Regulation (GDPR). You might be building payment systems that rely on the Payment Card Industry Data Security Standard (PCI DSS) or conducting financial transactions that are subject to scrutiny under the terms of the Sarbanes-Oxley Act of 2002.

Each regulation places distinct demands on an organization—for data protection and privacy, for data retention, and more. Some require distinct levels of encryption; others stipulate what data you may and may not retain as well as where you must and must not retain it. Your backup and recovery systems are as subject to regulatory compliance as your production systems, which means that you need to be sure that your backup and recovery system can provide the security and compliance support that your business requires.

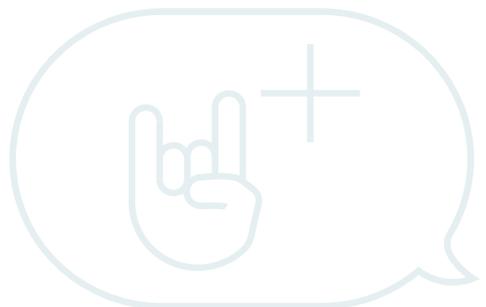
EASY SCALABILITY

Like the modern operational environments they support, backup and recovery solutions need to scale—quickly and easily—or they risk being the bottleneck to growth. Thus, a modern solution should be built to run on any hardware with scale-out software and simple cluster management. This solution should be able to scale from terabytes of data to petabytes of data with consistent performance and usability.

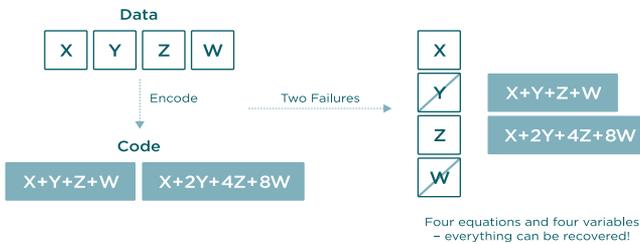
When selecting a backup vendor, it's important to know how easily the solution scales and the maximum size to which it can scale. Metadata and data should be distributed across all nodes within the cluster and support global deduplication. No single management node should be a point of failure, and the system should have self-healing capabilities. When the system has a node failure, find out if system restores are as efficient as when the system is fully functional.

Typically, backup solutions also have a specified amount of data that can be backed up. When this limit is reached, a separate system is required. A truly scalable solution should allow you to add backup nodes that take advantage of current technology and scale to your entire environment. This allows you to find data from a single source and to take advantage of global deduplication. Adding nodes should be an easy process that does not require days of data rebalancing or professional services to manage.

Storage efficiency is another important component of a scalable solution. Modern backup solutions use techniques such as *erasure coding* to make optimal use of storage while simultaneously ensuring fault tolerance and high performance.



Data Efficiency via Erasure Coding



Modern protection methods enable faster rebuilds
with lower storage space overhead.

COST VERSUS VALUE

Understanding the true cost of backups is extremely difficult. You need to know how much data you have, the type of data (structured or unstructured), the amount of granularity required for RPOs, and how long the backups will be stored. From an OPEX perspective, the calculable cost of backups includes the software and hardware, the cost of the WAN for replication and backup, colocation costs, and so on.

But there are other costs associated with backup and recovery that are far more difficult to calculate. What is the cost of business revenue loss and productivity if recovery is delayed—or worse, unavailable because the backup was compromised by ransomware? What is the cost to your organization's reputation if you are unable to recover in a manner commensurate with your brand? What is the cost of productivity lost by using a solution with a steep learning curve and hours of management time recovered? The real value of a backup solution lies in its ability to ensure that you are back up and running without a costly interruption or permanent loss of data.

IMMUTABILITY AND RANSOMWARE RECOVERY

As noted earlier, ransomware attacks have become increasingly common, and one component of a ransomware defense strategy involves the use of a backup and recovery system capable of creating immutable backups—that is, backups that cannot be encrypted by ransomware. A second part of a protective strategy would involve machine learning tools built in to the backup and recovery system that monitor application metadata to detect and alert you to signs of anomalous activity that might be indicative of a ransomware attack. Ideally, these tools would provide insight at a very granular level so you could quickly identify specific data blocks that had been compromised—and then quickly restore just those blocks rather than entire files, with a single click. This combination of machine learning tools operating in real time, coupled with the ability to recover infected data quickly from immutable backups, should be part of your protection strategy going forward.

BEYOND PROTECTION

For many organizations, the rationale for robust data protection is no longer just a matter of insurance and compliance. Many businesses are discovering that they can take advantage of their backup and recovery platform to explore new use cases—to create archives in the cloud, for example, or spin up test and DevOps environments with “real” data.

Your backup and recovery system needs to deliver on the fundamental tasks associated with rapid, reliable, and comprehensive backup and recovery—first and foremost. But many forward-looking organizations are also contemplating other uses for the data those systems are managing. It is worthwhile to consider how you might derive other value from your backup data and whether your backup and recovery solution provides the APIs and automation features that would enable you to capitalize on your existing data to explore new opportunities. Make sure the additional capabilities are not simply “checkbox” features but can provide true value to your business.

CONCLUSION

When considering a backup and recovery solution, you must look in two directions. There's the backward look: The system needs to be able to capture and secure key moments in your organization's digital life, and it needs to be able to quickly, reliably, and securely perform that function so that you can rapidly restore that digital life in the wake of whatever data disaster confronts you later. At the same time, there's a forward look: The system needs to be scalable enough and flexible enough to accommodate future growth and business needs.

Your organization's infrastructure will evolve in response to new business opportunities and customer demands, and the backup and recovery solution in which you invest needs to be able to evolve in step. Are you entirely on-premises? Partially in the cloud? Dynamically moving between multiple clouds from multiple providers? Whatever the case, it shouldn't matter to your backup and recovery system.

Your IT teams will evolve, too, so you need a solution that a generalist can master and manage effectively. That calls for simplicity, but it also calls for APIs and automation capabilities, so that a small team can manage your infrastructure effectively.

Finally, you must look at cost. Your data might be of incalculable value, but your budget is not unlimited. The total cost of ownership of a modern backup and recovery solution, one that can provide you with both the forward and backward-looking capabilities you need, should be lower than what you have been paying for your legacy system, even though it offers the innovative features that can enable you to do more with your data than ever before.

Get A Readiness Assessment

You've begun your datatude adjustment and realized that backup is just the beginning of what the Rubrik/ePlus solution can do for you. Now it's time to take the next step by having our engineers perform a thorough analysis of your current infrastructure, needs, and processes. We'll make strategic recommendations that show you a path to simpler data management, smart automation, and considerable cost savings.

datatude.eplus.com

