5 Important Questions to Ask Yourself Before Renewing Your Backup Software

To change or not to change? Does your current backup solution meet these key criteria?

Overview

We all know that nothing ever stays the same, and this has never been truer than in today's modern IT environments. The data landscape of today is evolving and changing so much that it can be difficult to keep pace. The cloud, multi-cloud, SaaS, containers, automation, data privacy – they all contribute to this increasing rate of change. Ransomware and other internal and external threats are transforming the data landscape. With all this in mind, when your existing backup solution(s) responsible for protecting your data comes up for a maintenance renewal or a major refresh, it makes sense to seriously re-evaluate if the time for change is now. Yes, it's a big decision with a wealth of variables to consider, from financial implications to the increasing demands of your environment. However, at the end of the day, you need to be confident that the solution you choose will be ready for what your business will need over the next several years and beyond.

Sure, it may seem easy to stick with your existing backup solution, but if it's unable to address your needs, how "easy" is it really? How much effort is it taking for you to support your existing solution? How many different solutions do you have to renew at different times every year? In addition, as your applications and data sets grow, point backup products can multiply, adding management complexity that makes the environment that much more difficult to support. With so much change happening so fast in the environment, maintaining the status quo will not serve you or your organization in the long run. In fact, according to the Enterprise Strategy Group, 91% of IT professionals believe their IT organization has to move faster than it did three years ago![1]

By taking a structured approach, you can quickly identify the key considerations you need to make a smart and informed decision about your backup and recovery software solution. Evaluate the current state of your backup solution(s) and see how new technology developments may warrant change. Pose these five questions below to your current backup vendors as well as those you are considering. It's a great way to determine their ability to meet your needs today and tomorrow. You may be surprised by the answers!

1 Can I really manage all of our data with this solution?

Managing multiple backup and recovery point products for different data sets is a time and resource drain. Even more, it means that even simple tasks like finding the data you need are exacerbated by having to look in multiple places. Who's backing up what? What might you miss?

To be sure that the backup and recovery solution is ready to support all your data, ask these secondary questions:

- Can it back up your data wherever it exists? On-premises? Across multiple clouds? Hybrid? Virtual? Physical? Unstructured? SaaS? Application? Containers?
- Can it quickly restore data to anywhere it's needed? Across clouds? Across hypervisors?
- Does it depend on a lot of customization like scripts or proprietary hardware to meet the service level agreement (SLA) needs of your organization?
- Will it provide you with a single user interface to manage data protection and recovery operations across your global data workloads?
- Can you use it to apply consistent policies across all your data while segmenting data sets for storage in the infrastructure tiers that best deliver value to your organization?
- Does it have built-in protection to ensure the backup data itself is safe from threats like ransomware and other malware, or does it rely on other components or products?

[1] ESG Master Survey Results, 2021 Data Infrastructure Trends, September 2021

2 Is it both easy to use and flexible?

By using the terms easy to use and flexible, we don't' mean basic or limited. Look for solutions that offer straightforward and automated deployment options, an intuitive user interface, and the ability to define SLAs with ease. From initial purchase to the ongoing management and support, backup and recovery software should simplify your processes, not add more complexity. Ask these questions as well:

- How easy is it to change things within the backup solution? Is it a case of "painting everything with the same brush" or can you tailor the solution to meet your evolving data needs?
- Is the solution "self-driving" or do you need a lot of hands-on oversight? How much automation and intelligence are built-into the solution? Does it leverage machine learning or AI to support more efficient operations?
- Can the solution easily manage and migrate data to, from, and within the cloud, as well as between clouds? Can the solution do all these things with native capabilities, or must it rely on scripts, gateways, or other third-party products?

Scale-out technology is another consideration when looking at simplifying the backup infrastructure. Having a solution that can support multiple deployment scenarios gives you the flexibility to install what you need, where you need it, and how you want it. This also can simplify things financially as you only need to purchase enough to cover your immediate needs with the knowledge that you can seamlessly scale the infrastructure when required.

82% of business, IT, and cybersecurity executives believe that cyber risk is greater today than it was two years ago[1]

3 Is your solution future-proof?

Technology and business requirements change fast! As a result, your data protection needs today won't likely be the same three years or even one year from now. Just think of all the new workloads and applications you've adopted in the past three years or how your infrastructure has changed through hyper-convergence, the introduction of containers, SaaS, or your shift to the cloud. While it can be hard to predict what your environment may need in the coming years, you can opt to select a backup and recovery solution that stays one step ahead. As you anticipate changes in your infrastructure and application environment, ask these questions:

- Is the solution truly technology-agnostic? Can it support heterogeneous and hybrid environments? Or is it limited to only a few options?
- Does it offer industry-leading integration with a wide selection of storage arrays, storage platforms, and cloud storage options? This level of integration can help drive snapshot-based protection, replication, and rapid disaster recovery.
- Does it offer native-cloud integration with public clouds, including Amazon AWS, Microsoft Azure, Oracle Cloud and Google Cloud? Or does it need separate tools to manage those workloads?
- Does it provide extensive APIs to enable deeper integrations across your data and applications? Can it plug into your other tools like ServiceNow, Splunk, VMware vRealize, or vCloud Director?
- Will the backup solution force you to deploy or add new tools or solutions each time a new workload is introduced into your environment or is everything built into the platform already?

Addressing these criteria will ensure that you can easily move your data or adopt new infrastructure as your business goals and supporting technologies continue to change.

87% of IT professionals believe cloud computing has enabled their organization to better and/or more cost-efficiently protect data[2]

[1] ESG Master Survey Results, Cybersecurity in the C-suite and Boardroom, March 2021

[2] ESG Master Survey Results, 2021 Data Infrastructure Trends, September 2021

4 Does the math add up?

Let's face it, cost is always a key consideration. When looking at the renewal contract for your backup and recovery solution, be sure to think about all the elements that go into its total cost of ownership.

- Consider how much time your team spends on backup and recovery management, including daily and weekly administration, patches and refreshes, and managing support issues. If you use multiple products that number can grow exponentially.
- Calculate the infrastructure requirements for your data protection solution. Is there a third-party or proprietary technology required? Can you easily scale and add capacity as you need it, or must you predict your storage needs and risk over-provisioning?
- Is the infrastructure permanent? Or can it be scaled up and down with demand? This can be a key factor in mitigating costs for in-cloud data protection.
- What is the downtime risk of your solution? How long might it take you to recover the backup solution itself during a downtime event and what will that cost your business?
- Can you easily move data between storage tiers – including disk, object storage, and the cloud – based on data policies and service level requirements? Is the data being natively deduplicated at the source and target to further reduce storage needs? Does deduplication or cloud storage access require additional hardware?
- Can you change vendors for your storage, compute, or cloud? Are there dependencies with the backup to any of those? How would a change to any of those affect your backup?

Renewal costs are merely the tip of the iceberg. Be sure to study all financial elements related to each solution you consider. What else is required to keep your existing backup solution viable? Is there another point product needed? Special hardware? Other licensing? It's important to have the complete picture when looking at the costs of continuing to prop up your existing solution or evaluating a new one.

5 Ready for change? What are the risks?

If you're not as happy with the answers to previous questions when contemplating your current backup solution(s), you're ready for a change. But what about the risks involved with making a switch? Change is always a little nerve-wracking, especially when a misstep may mean downtime or data loss. So before taking this final step, be sure any solutions you evaluate can answer not only the previous questions, but these as well:

- How fast can the new solution be ready to back up your data?
- How long will it take to transition your existing backup workloads to the new solution? Is that process automated, or will it be manually intensive?
- How much of your team's time is required? Will additional services or training be needed? What are the costs associated there? If you are short-staffed, can the new vendor manage your environment remotely for you?
- What is the total cost of your current solution, including new hardware, software, and installation? What do those costs look like as you scale? What about next month? Next quarter? Next year? Do those costs change?
- What is the customer support experience like? What are their SLAs? How easy are they to engage for all your sites and team members globally?
- Lastly, what do you do about the old backup data? Is there a way to migrate important backups to the new solution?

When evaluating a new solution, you want to be sure that it isn't just the latest shiny object – you want to make sure it can meet your needs today and tomorrow. You need it to be flexible, cost-effective, scalable, automated, and (most importantly) proven. By weighing your options carefully during this important decision, you'll realize the simplicity, lower cost, and modern features your organization's data requires. Even better, you'll be ready for whatever tomorrow holds for your data.

Learn more about how you can drive down IT costs while improving data availability and increasing IT resiliency with Commvault Intelligent Data Services **here >**

COMMVAULT
Be ready™

commvault.com | 888.746.3849