COHESITY

CLOUD BACKUP:

A detailed **backup-as-a-service** evaluation guide and checklist

Boost data agility, operational efficiency, and cyber resilience

Table of Contents

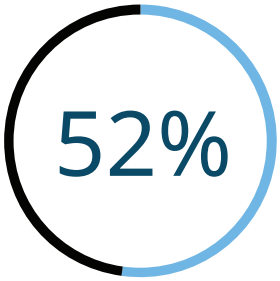
Backup for the cloud era 2
Advance data protection and operational freedom 4
Fortify security and ransomware readiness 6
Gain consumption and cost flexibility plus sustainability 8
Checklist: BaaS offerings 10
Put BaaS to Work 12

Backup for the cloud era

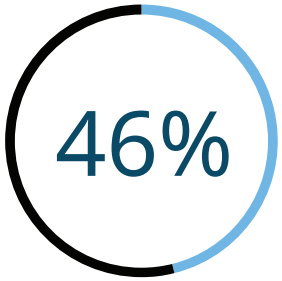
In recent years, IT modernization driven by cloud computing has led to rapid innovation and growth. Yet not all critical IT infrastructure has been leveled up consistently or at the same pace on cloud journeys, creating inefficiencies and cyber vulnerabilities that organizations can't afford.

The often overlooked modernization move to backup infrastructure in the cloud—beyond what SaaS vendors provide—can deliver the same kind of agility to your enterprise as running your modern apps in the cloud. That's because backup as a service (BaaS) is a business-continuity fundamental that consolidates legacy backup silos built before the cloud while improving and fortifying your cloud experience, operations, and costs. Moreover with BaaS, you can more effectively maximize the potential of all of your data for business insights while keeping your enterprise cyber resilient.

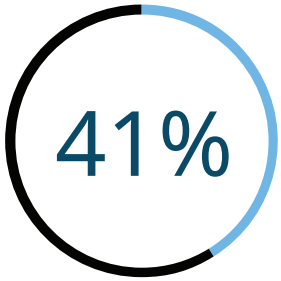
Most common benefits of cloud based data protection services



Improved security



Improved recoverability and reliability of backups



Reduced IT personnel costs

Source: Enterprise Strategy Group. "The Evolution of Data Protection Cloud Strategies," 2021.

Taking the next step on your cloud journey

As you evaluate BaaS offerings, it's important to know what available capabilities to consider, including how your data will be protected and how your enterprise will be charged. This guide details important evaluation criteria and provides a checklist to reference on your cloud journey.

Comparing cloud backup solutions starts with understanding how an offering supports these critical BaaS capabilities:

1. Advancing data protection and operational freedom
2. Fortifying security and ransomware readiness
3. Delivering consumption and cost flexibility with sustainability

Current challenges assessment

Before you evaluate a cloud backup offering, it can be helpful to clarify some key differences between a backup and recovery environment managed on premises by your organization (aka self-managed) and one managed by a backup vendor and hosted in the cloud. Table 1 outlines 10 common backup and recovery challenges with self-managed, on-premises only solutions.

10 common backup and recovery challenges with self-managed, on-premises only solutions

1. Siloed infrastructure (e.g., separate servers, dedicated storage targets, etc.) is costly to purchase, increasing CapEx
2. Lack of support for modern, cloud-native and SaaS application protection, putting the business at a competitive disadvantage
3. Complex management with multiple, fragmented UIs for different data sources to configure backup workflows, adding to IT frustration
4. Bolt-on cloud gateways required to migrate data onsite and into different public clouds, creating complexity
5. Forklift upgrades and disruptive updates, requiring planned downtime
6. Slow restores causing RTO misses and/or last point in time only restores, negatively affecting RPOs
7. Variable and/or fixed block deduplication with compression, increasing costs
8. Lack of ransomware protection capabilities, adding risk to the business
9. Inability to reuse data due to fragmentation, keeping insights hidden
10. Slow rollout of modern capabilities, hindering innovation

Table 1: Assessing self-managed, on-prem backup and recovery environments

Digital business moves fast. Cloud backup helps you not only keep up but accelerate your cloud and digital transformation journey.

1 Advance data protection and operational freedom

Business and regulatory requirements for what types of information your organization must safeguard—and for how long—change. You want a comprehensive cloud backup solution that can adapt quickly when they do. Without a consistent way to support retention policies and service-level agreements (SLAs) for all of your cloud-native, software-as-a-service (SaaS), and on-prem applications, how can you ensure all your data is protected and your already stretched internal IT staff isn't overburdened?

Cloud backup can be much more valuable to your business than an insurance policy. For the most advanced data source protection with operational freedom, choose a BaaS with the following five key operational features:

Broad data sources support

Backups should be simple. Yet it's difficult today to manage backing up all the mission-critical data in applications across your environment because of the various cloud platforms, services, and APIs with different policies, SLAs, and retention periods. This creates complexity. What's needed for optimal simplicity is a single BaaS solution that supports a broad set of workloads across multiple environments and clouds—a service that consolidates and protects cloud workloads such as Amazon EC2 and RDS as well as SaaS applications (like M365) with a single, unified service that goes well beyond the built-in protections ofcloud providers.

With a modern BaaS solution, you eliminate legacy backup silos and implement comprehensive, consistent, enterprise-class protection for a broad set of data sources. These include:

- Cloud-native apps
- SaaS workloads and apps
- Home-grown cloud apps
- Virtual and physical servers
- Traditional and containerized applications
- Relational and distributed databases
- Files and unstructured data

Benefits of sending non-protection secondary copies of data to the cloud

41% Better security compared to on-premises resources

38% Beter availability compared to on-premises resources

37% More elastic scalability

36% Ability to support higher levels of end-user concurrency

35% Faster time to deploy or time to value for new projects

Source: Enterprise Strategy Group. "From Data Backup to Data Intelligence," 2022.

Unified management

Organizations founded before cloud computing are likely to self-manage the backup and recovery of some workloads while fully embracing cloud-based offerings such as M365, Salesforce, and Workday. No matter where data resides or how it's deployed, your organization needs it to have the same level of enterprise protection—without creating management silos in the process. The right BaaS solution unifies backup and recovery management in one UI. So even if you want to use the management UIs that come with your SaaS apps (e.g., M365 and SFDC), you still have complete visibility into them and all your self-managed on-prem apps and workloads through one console. Be sure any BaaS solution you are considering fully unifies backup data across hybrid and multicloud and allows you to use a single interface to quickly search data globally, and recover it anywhere.

Operational simplicity

Cloud providers operate under a shared responsibility model. They guarantee infrastructure uptime. It's your responsibility to protect your organization's data. For example, although Microsoft 365 (M365) runs in the cloud on Microsoft Azure, each of the M365 productivity apps, as well as Teams and SharePoint, has its own limited protection policy. As the war for talent tightens, IT experts spending a majority of their time on routine tasks such as managing protection by workload and cloud providers will look for new opportunities to make a greater positive impact on the business. Enterprise-grade BaaS reduces your IT staff burdens by routinely creating and executing hundreds of policies, giving your experts time to focus on innovation. It secures data while giving you visibility into it and simplifying how you protect it over multiple cloud services and on-prem apps.

High reliability and performance—no disruptive upgrades

In today's fast-paced digital business world, your IT operations and lines-of-business teams want backups to be flexible, available, scalable, and reliable. A modern BaaS solution can help you achieve SLAs and accelerate business outcomes by making the data you need available when you need it while countering ransomware attacks. Cloud backup doesn't interrupt business—it's always-on, updated in place, and ready to protect.

Little-to-no data center footprint

Legacy backup infrastructure typically includes a patchwork of products that make your data more vulnerable to cyberattacks. Cloud backup from individual SaaS vendors means you have plenty of points for ransomware to find a way in. A single, consolidated BaaS offering with little to no on-prem hardware strengthens your protection by reducing your data center footprint, and thus your attack surface.

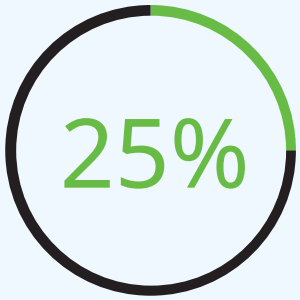
What to ask vendors: Advancing data protection and operational freedom

- What is your organization's (business and application owners') tolerance for downtime due to backup-related updates and upgrades?
- How do you expect your next solution to back up all the different data sources available to your enterprise?
- How much time is your staff spending managing backups for SaaS, cloud-native, and on-prem apps and data?
- What processes are in place to help you quickly adapt to changing regulatory or business requirements for data protection and retention?
- What changes in your IT environment are you considering to reduce your on-prem infrastructure and cybersecurity risk profile?

2 Fortify security and ransomware readiness

Enterprise data is under attack, and cybercriminals are getting richer. By 2031, ransomware will attack a business every 2 seconds—costing its victims $265B annually, according to Cybersecurity Ventures. That's why in addition to improving your IT agility, your organization needs to strengthen its security posture and better defend your data against ransomware.

BaaS can help your business refuse to pay ransom, yet not all BaaS offerings deliver the same ransomware readiness capabilities. Be sure you invest in a BaaS solution that has critical anti-ransomware features, including the following:



of organizations say malicious deletion is their top cause of SaaS data loss.

Source: Enterprise Strategy Group. "The Evolution of Data Protection Cloud Strategies," 2021.

Immutable snapshots

Your data is better protected in cloud backup built with immutable snapshots that are impossible for ransomware to encrypt, modify, or delete. The right BaaS helps ensure your structured and unstructured data—everything from emails to audio and video files to images—is backed up and ready to be recovered should a worst-case ransomware attack happen.

Anomaly detection and alerting

The average number of days to identify and contain a breach was 277, according to the "Cost of a Data Breach 2022" survey. Such an extensive period of time allows cybercriminals to not only encrypt, but also exfiltrate your data to sell it on the dark web. That's why powerful automated anomaly detection in near-real time is an important feature of a BaaS offering. With cloud backup, you can continually track normal system operations to quickly spot irregularities and abnormal user behaviors that can signify a ransomware attack. Together with alerting, these capabilities can signal potential danger and initiate remediation—both of which help minimize the blast radius of a ransomware attack.

Strict access controls

Compromised credentials were the most common initial attack vector in 2022, according to the "Cost of a Data Breach 2022" survey. That puts the onus on your organization to manage your users' identity and access privileges more effectively. The best BaaS offerings support granular role-based access control (RBAC) to prevent unauthorized parties from threatening your data. You should also look for one that includes multi-factor authentication (MFA)—a two-step something you "have" and something you "know" process—to authenticate and mitigate against phishing schemes and other password hacks.

Data isolation

Before the cloud era, the most common way to recover enterprise data was to physically bring data stored on tapes in an offsite facility back onsite. Yet that process is no longer compatible with meeting the recovery SLAs that the business demands.

Modern BaaS isolates data from your production environment by moving backup data offsite to the cloud and securing it. For instance, modern BaaS can create isolation for services in AWS by moving the data into a separate tenant. So if you need to rapidly recover after a ransomware attack, you can do so without reinfecting your production environment.

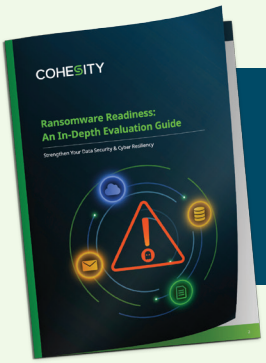
Rapid data recovery at scale

Given the prevalence of ransomware and the indications there is no slowing of malware development in sight, your organization must be ready to recover quickly from a cyberattack. This includes having processes and technologies that give you a way to confidently recover your data at scale.

You need a cloud backup service that can quickly recover all types of data sources—such as hundreds of VMs, large databases or large volumes of unstructured data, M365 productivity data, and more—instantly, at scale, to any point in time and location.

What to ask vendors: Fortifying security and ransomware readiness

- How do you defend all your different apps and workloads from ransomware?
- How do you prevent unauthorized access to your business data today?
- What plans do you have in place for data recovery from ransomware at scale?



Ransomware Readiness: An In-Depth Evaluation Guide

may also be helpful during your decision-making process.

3 Gain consumption and cost flexibility plus sustainability

Data-driven is the new normal in business. That's why businesses are increasingly striving to use the data they collect and protect to discover new insights and accelerate product and services time to market. Yet the data powering businesses is growing at exponential rates, which makes keeping it more costly. The move to a service provider model is a win-win for the business's bottom line as well as for your IT and procurement teams. A BaaS subscription reduces time spent in procurement, contracting with multiple backup hardware and cloud vendors to get started. BaaS subscriptions also simplify renewals. Predictable pricing eliminates budget surprises, too.

As you consider BaaS for improving your financial management and transparency, be sure you choose a provider that gives you both predictability and choice.

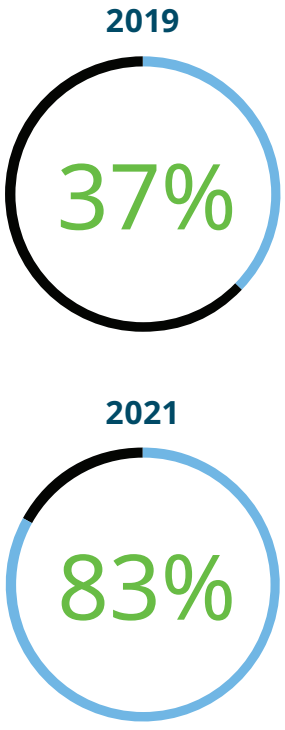
Easy adoption

Flexibility is a top driver for enterprises considering BaaS. Make sure the BaaS offering you choose offers manageable commitment times (e.g., one year) and you only pay for the capacity you need. Also consider whether the billing is easy to understand—metered in a transparent and granular way—for maximum cost predictability. Unlike self-managed offerings that only permit one option, modern BaaS solutions maximize flexibility with multiple licensing options, including front-end, back-end, or user-based licenses. A BaaS offering should make implementation simple—sign up, set up your account, connect your data sources, and automatically detect your workloads. You should be able to start protecting mission-critical data and applications within minutes.

License portability

Organizational leaders make IT investments to achieve business results. Technologies shouldn't force you to change how or where you plan to deploy them. If your organization requires backup that supports workloads and apps running both onsite and in the cloud, look for a BaaS provider that delivers license portability between consumption models.

We send secondary data copies to public cloud infrastructure services for non-protection purposes (i.e., dev/test, analytics, etc.)



Source: Enterprise Strategy Group. "From Data Backup to Data Intelligence," 2022.

Support for data sovereignty requirements

In a recent ESG survey, organizations expressed increasing concern around compliance and data sovereignty/location issues. If your leadership is going all-in on cloud, BaaS offerings can help you meet data sovereignty requirements. The best BaaS solution operates within data center private clouds and atop leading public clouds that can segment your data by regions across the globe in accordance with national and local regulations.

Transparent, pay as you grow pricing—no hidden costs

In uncertain economic times, it can be important to preserve cash for innovation. BaaS allows your organization to shift from making capital expenditures to a more predictable, operational expense model. At the same time, the right BaaS solution eliminates provisioning and hidden cloud costs, such as data ingress and egress charges. Look for an offering that gives you a secure and efficient way to protect and consolidate your backup data in the cloud and that allows you to do more with your data to discover insights and lower your risk.

Sustainability benefits

Your brand is now being evaluated not only on how well you take care of your customers and employees, but also on how hard you are working to protect our planet. Cloud backup lowers physical hardware footprints in your data center, which reduces your energy consumption—a key objective of corporate environmental, social, and governance (ESG) initiatives. Find a BaaS offering that works in concert with your ESG goals.

What to ask vendors: Gaining consumption and cost flexibility with sustainability

- How have your investments in backup changed over the past several years?
- In what ways has and is your organization optimizing IT to drive innovation during times of economic uncertainty?
- What are some of your organization's ESG goals?

Checklist: BaaS offerings

Take the next step to cloud-driven IT modernization with BaaS. It's an ideal way to advance your protection goals for all your data sources, gain operational freedom, fortify your environment against ransomware, and optimize costs. As you evaluate BaaS offerings, this checklist of key capabilities can help you discover the best-fit solution for your organization.

Capabilities		Vendor 1	Vendor 2	Vendor 3
Advance data source protection and operational freedom	Broad data sources support	☐	☐	☐
	Unified management	☐	☐	☐
	Operational simplicity	☐	☐	☐
	High reliability and performance—no disruptive upgrades	☐	☐	☐
	Low-to-no data center footprint	☐	☐	☐
Fortify security and ransomware readiness	Immutable snapshots	☐	☐	☐
	Anomaly detection and alerting	☐	☐	☐
	Strict access controls	☐	☐	☐
	Data isolation	☐	☐	☐
	Rapid data recovery at scale	☐	☐	☐
Gain consumption and cost flexibility plus sustainability	Easy adoption	☐	☐	☐
	License portability	☐	☐	☐
	Support for data sovereignty requirements	☐	☐	☐
	Transparent, pay-as-you-grow pricing—no hidden costs	☐	☐	☐
	Sustainability benefits	☐	☐	☐

"Cohesity's Backup as a Service offering enables us to protect our valuable user data without having to purchase a lot of extra storage infrastructure upfront. Since we didn't need to procure any hardware, we were up and running on Cohesity BaaS offering within an hour."

Jake Parham
IT Manager, St. Johns County Sheriff's Office

Put BaaS to Work

Go further, faster in your IT modernization by adopting BaaS. With simpler, more efficient, and more secure enterprise-grade protection for the wide variety of data sources your organization now relies on, your enterprise boosts agility. Meet business SLAs and compliance requirements. Save IT data management time and headaches. Achieve your ESG goals. It's all possible with the right BaaS offering.

Learn more about BaaS from Cohesity.

COHESITY