Data Protection as a Service for 2022

Backup as a Service (BaaS), as well as Disaster Recovery as a Service (DRaaS), means different things to different people. Cloud-powered data protection can take many different forms depending on a wide variety of factors — the size of the organization, the diversity of workloads, the geo-sovereignty requirements and several other considerations. According to **1,050** IT leaders in this unbiased research survey, there are four main tenants that organizations of all sizes should be looking for:

- **Deployed** from a cloud service without assembling hardware/software

- **Monitored** or curated by third-party experts

- **Managed** by a cloud-based UI experience

- **Transacted** through service providers

More importantly, regardless of individual interpretations of "BaaS" or "DRaaS", the survey data reveals that cloud-powered data protection, also referred to as Data Protection as-a-Service (DPaaS), is universally desirable and basically inevitable regardless of organization size or geography due to the assurance of data survivability and the presumption of economic benefits. Regardless of region, roughly **68%** of organizations currently using cloud-services somewhere within their current IT architecture are protecting at least some of their production servers with BaaS and/or DRaaS. And **97%+** plan to protect some of their servers with BaaS and DRaaS in the next two years. So, no matter what BaaS and DRaaS mean to you, or look like for your organization, they will be nearly inevitable in the next 24 months.

Leveraging an effective and efficient BaaS / DRaaS service can relieve your organization's IT team from the daily management of backup tasks and assuring a significantly higher likelihood of being able to recover when you need it most. One of the best ways to ensure that your IT team isn't bogged down by all the small things is to enable a solution that offers a wide breadth of services. Most IT professionals don't hate backups — they hate the operational burden of managing and maintaining backup systems. They want a solution that just works.

That is what organizations expect of every IT function — that it just works. Regarding "backups" and according to the survey, this translates to backup servers that are well maintained, patched and the right size. Protection jobs should be monitored to make sure nothing is failing, and capacity planning and budgeting should be accounted for. These are all some of the features a monitored backup can offer to their consumers. The BaaS and DRaaS market vary widely from provider to provider but some common services included outsourced servers, removal of daily management and monitoring of backup servers and jobs, and proactive management to optimize the backup process and assure recoverability.
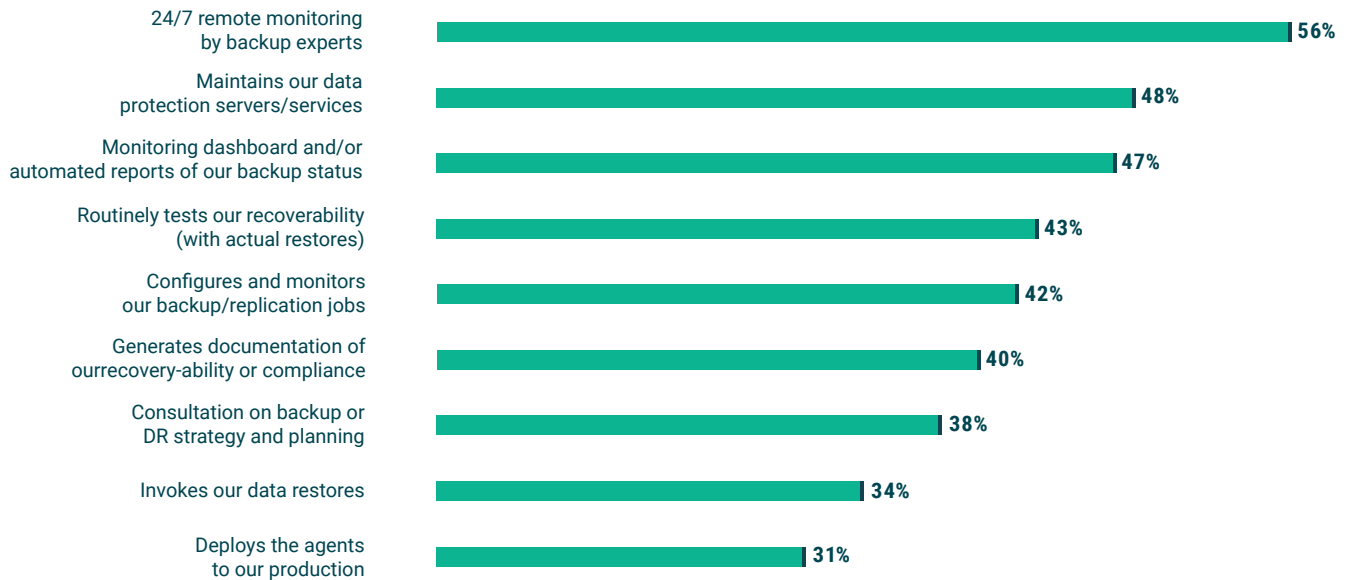
77%
of organizations expect to use the cloud as part of their data protection strategy by 2023.

46%
of organizations looking for BaaS are seeking cloud-hosted backup server services.

![Veeam logo]

What services does your organization's current BaaS provider offer?

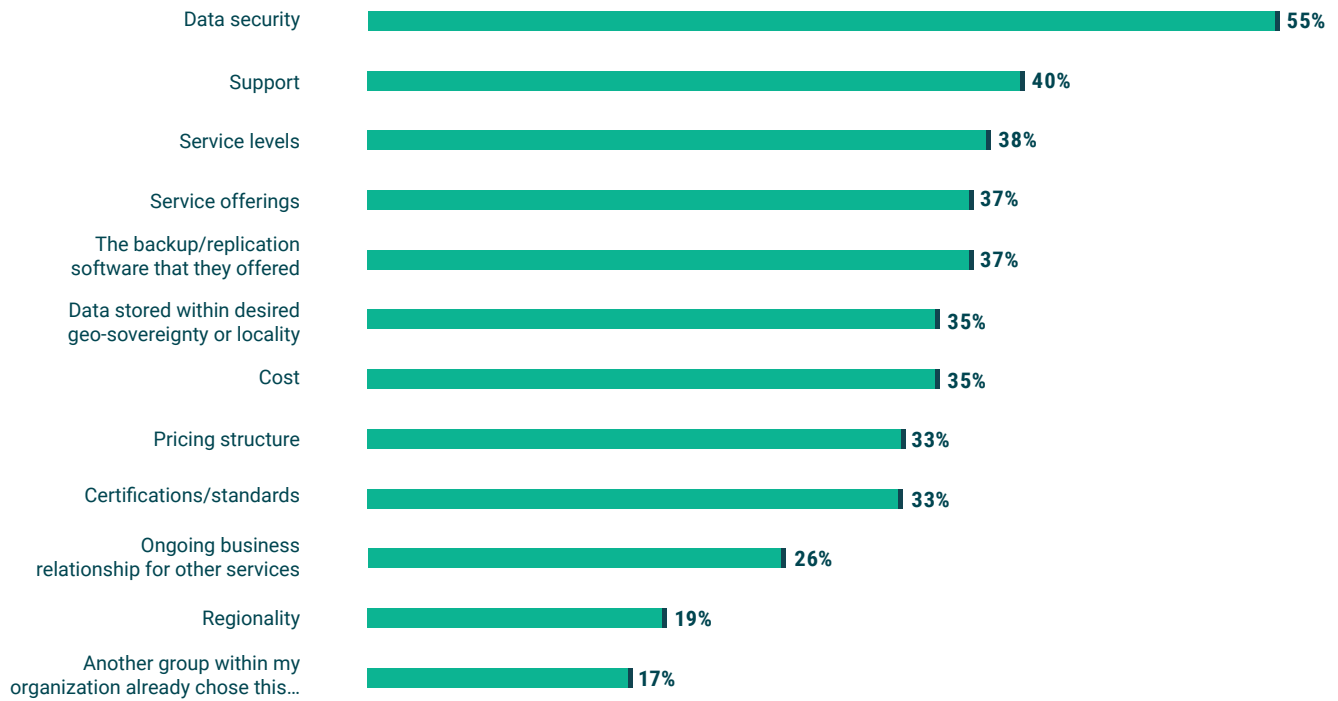| Service	Percentage
24/7 remote monitoring by backup experts	56%
Maintains our data protection servers/services	48%
Monitoring dashboard and/or automated reports of our backup status	47%
Routinely tests our recoverability (with actual restores)	43%
Configures and monitors our backup/replication jobs	42%
Generates documentation of ourrecovery-ability or compliance	40%
Consultation on backup or DR strategy and planning	38%
Invokes our data restores	34%
Deploys the agents to our production	31%

Notably, the chart also shows that "ad-hoc" activities, such as deploying agents or invoking restores, are the least offered by service providers, since those activities are most often performed by the subscriber's IT professionals. These circumstantial, reactive actions are not really what BaaS and DRaaS cater to, instead they strive to reduce operational strain which, in turn, increases the odds of a well-protected environment.

As previously mentioned, BaaS and DRaaS are already mainstream choices for data protection from datacenters to edges to clouds — for organizations of all sizes. According to survey respondents currently using BaaS or DRaaS for their production servers, there are four key considerations when choosing a data protection service provider:

- **Security —** naysayers often start every as-a-service concern with "the cloud" being a security risk; but in reality, when as-a-service is done correctly, it can be more secure than traditional on-premises architectures. Hence, the first consideration when choosing a provider is how they assure that your data will be secure.

- **Quality of experience —** after you know your data is secure, its time to focus on the quality of your experience with a provider. Consider them a "service partner" not just a "service provider," so how well do they engage with your teams? Will they be responsive to your needs? How easy are they to actually transact (billing/dashboards) on a recurring basis?

- **Solution capabilities —** now that you know your data is a secure and that you will have a good experience working with a particular provider, examine their solution capabilities. This is mostly determined by how they've architected their servers within their own datacenter(s) or by leveraging cloud-infrastructure elsewhere, as well as which data protection software tools they've chosen to offer 'as a Service'.

- **Economics —** economic benefits (not to be confused with 'always cheaper') is often what drives organizations to initially consider 'as a Service', as opposed to self-deployed or self-managed. With that gate already decided, the guidance above is about choosing between service providers. That said, transaction costs don't matter if you aren't able to get the capabilities, quality of service and assurance of security that you need.

Why did your organization choose
your current BaaS provider?

Data security	55%
Support	40%
Service levels	38%
Service offerings	37%
The backup/replication software that they offered	37%
Data stored within desired geo-sovereignty or locality	35%
Cost	35%
Pricing structure	33%
Certifications/standards	33%
Ongoing business relationship for other services	26%
Regionality	19%
Another group within my organization already chose this…	17%

The Veeam perspective

Veeam has been enabling cloud-powered data protection for nearly a decade —
always through our partner ecosystem which currently boasts **13,000** service
providers offering a range of BaaS and DRaaS solutions from self-managed to
concierge delivered. Services powered by Veeam deliver top solution capabilities
with an exceptional quality of experience, all while keeping organizations' data safe
and secure. But don't take our word on it, check out a Veeam service provider near
you at www.veeam.com/find-a-veeam-cloud-provider.

Click here to view the complete
research Global report