

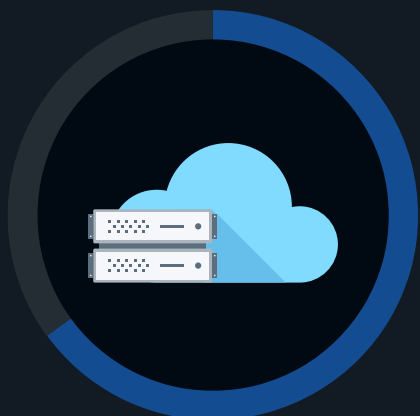
Cloud Data Protection Strategies at a Crossroads

The broad adoption of public cloud services and containers as sources and repositories of business-critical data puts the onus on data owners to deliver on data protection SLAs for cloud-resident and container-based applications and data. As vendors and the cloud ecosystem evolve and add as-a-service consumption options, end-users are making incorrect comparisons and assumptions, leading to lasting challenges and a market at a crossroads. TechTarget's Enterprise Strategy Group recently surveyed IT professionals familiar with and/or responsible for data protection technology decisions for their organization to gain insights into these trends.

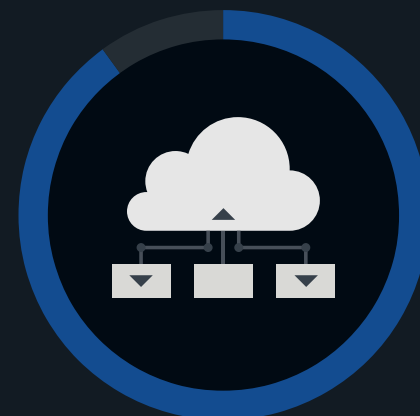
Notable findings from this study include:



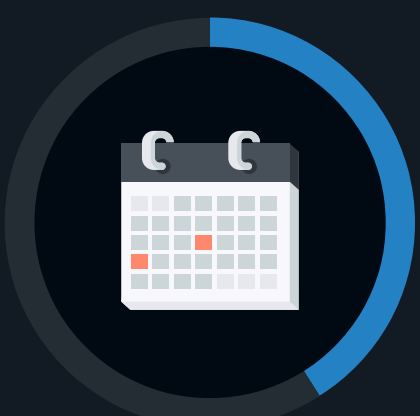
76%
of organizations believe that BaaS can be **just as granular as on-premises backup solutions.**



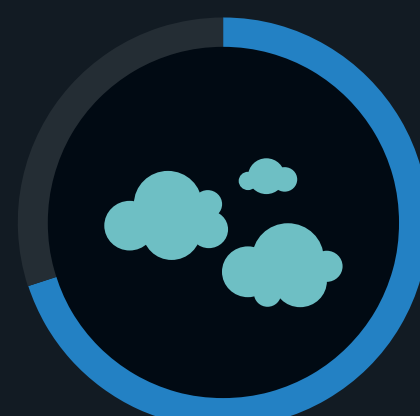
65%
of organizations leverage cloud object storage for older backups and archives.



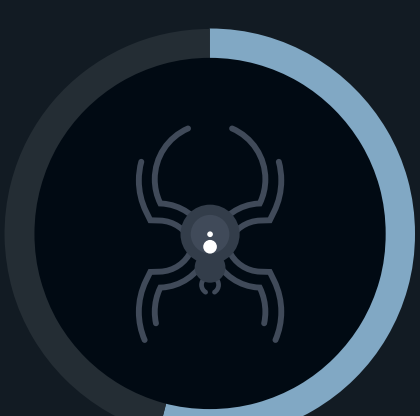
90%
of organizations could **not** recover 100% of data they backed up in a public cloud service.



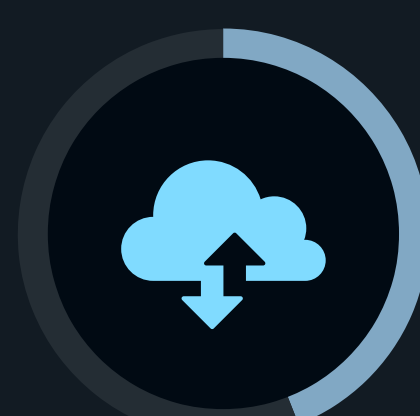
41%
of organizations reassess their cloud data protection strategy annually.



70%
of multi-cloud organizations prefer to protect multiple unique public cloud service provider environments with different data protection tools for each.



54%
of organizations that had to recover data in the last 12 months attributed these efforts to a cybersecurity event.



44%
of organizations will consider a public cloud-based data protection solution that integrates an on-premises storage solution for local recovery.

For more from this Enterprise Strategy Group study, read the full research report, *Cloud Data Protection Strategies at a Crossroads*.

[LEARN MORE](#)