DCIG *Top 5*
All-in-One DRaaS Solution Profile

by Jerome Wendt, DCIG President & Founder

SOLUTION

Acronis Cyber Disaster Recovery Cloud

COMPANY

Acronis International GmbH
1 Van de Graaff Drive
Suite #301
Burlington MA 01803
(781) 782-9000

Acronis.com

ALL-IN-ONE DRaaS SOLUTION INCLUSION CRITERIA

- May offer a physical or virtual backup appliance
- May deliver backup-as-a-service (BaaS)
- Must offer its own backup software
- Must deliver recovery services in the cloud

MOST SUITABLE ENVIRONMENTS FOR AIO DRAAS SOLUTIONS INCLUDE:

- Protection and recovery of up to 50 VMs; and/or
- Protection and recovery of up to 10 physical machines; and/or
- 10 or more TBs of data to protect

The New Need for DRaaS

Disaster recovery-as-a-service (DRaaS) solutions represent the next step in the evolution of backup software. Existing backup software already equips many organizations to successfully backup their applications within prescribed backup windows.

Using this software, they may backup to disk, cloud, or tape or use snapshots and replication to protect data. These techniques have largely successfully solved long-standing backup challenges freeing organizations to focus on recovery.

Recovery presents an entirely new set of challenges for organizations to understand and address. They must achieve specific recovery time objectives (RTOs) of minutes or hours for each application. They must define each application's recovery point objective (RPO) to determine how much, if any, data loss an application can sustain prior to recovery. Organizations must also determine where they want to recover, the applications they want to recover, and the order in which they want to recover them.

Various DRaaS solutions have emerged in response to this new organizational need for recovery. These DRaaS solutions equip organizations to simultaneously automate, accelerate, and simplify recovering their applications individually or at scale.

The Two Classifications of DRaaS Solutions

Providers deliver DRaaS solutions in two general forms—all-in-one (AIO) and hybrid DRaaS solutions. AIO DRaaS solutions include the core features for organizations to implement DRaaS in turnkey manner. These solutions generally offer physical or virtual backup appliances, backup software, and a purpose-built cloud offering.

In comparison, hybrid DRaaS solutions consist of a cloud purpose-built for DR or a general-purpose cloud such as AWS. Hybrid DRaaS providers then pair them with backup software from one or more providers with one of these types of clouds to deliver a hybrid DRaaS solution. Going down this path gives the providers more flexibility to create a hybrid DRaaS solution according to an organization's specific needs.

Inclusion and Evaluation Criteria for AIO DRaaS Solutions

DCIG specifically focused on AIO DRaaS solutions in this analysis with solutions that possessed the following characteristics. These include:

- A physical or virtual backup appliance that may be installed in the customer environment with its own backup software, or the offering is available as a purpose-built backup-as-a-service (BaaS) offering;
- Provides its own cloud offering that is situated in a data center that can host a disaster recovery
- Pairs its backup solution with its cloud offering to create an AIO DRaaS solution
- The product is shipping and available by September 1, 2019
- Information available for DCIG to make an informed, defensible decision.

DCIG identified eleven different solutions that met these inclusion criteria. DCIG evaluated each of these solutions in the following seven areas:

1. ***Pricing*** to include the subscription costs; the different subscription periods available; and, the events and services the solution includes with each subscription.
2. ***Orchestration*** to include the types of services that a provider offers for recovery, such as runbooks and testing; the types of recoveries it supports; and, the types of cloud infrastructure the provider makes available to host the recovery.
3. ***Protected environments*** to include the types of applications, data, hypervisors, and operating systems protected by the provider's backup software.
4. ***Disaster recovery (DR) testing*** to include the DR testing options available, the maximum duration of DR tests, and the number of virtual and physical hosts that an organization can recover in the provider cloud.
5. ***Recovery*** to include the service level agreements (SLAs) that a provider offers for recovery times; who determines if a recovery should occur; and, the levels of availability and redundancy that the provider's cloud offers.
6. ***Cloud choice*** to include the industry certifications the provider's cloud offers and the countries or continents where its data centers are located.
7. ***Support*** to include the individuals that provide the support, support response times, and the ways in which each provider handles multiple concurrent DRs.

AIO DRaaS Solution Profile

Acronis Cyber Disaster Recovery Cloud

Upon DCIG's completion of reviewing the multiple, available AIO DRaaS solutions, DCIG ranked Acronis Cyber Disaster Recovery Cloud as a Top 5 solution. Acronis uses the following products in its portfolio as the building blocks for its disaster recovery solution.

- Acronis Active Protection
- Acronis Cyber Backup
- Acronis Cloud Storage
- Acronis Cyber Cloud for Enterprise
- Acronis Local Cloud Appliance
- Acronis Cyber Notary
- Acronis Disaster Recovery Service

Acronis Cyber Disaster Recovery Cloud represents the outcome of multiple acquisitions coupled with product innovation and integration by Acronis over many years. Key technologies that Acronis offers that differentiate it from other Top 5 AIO DRaaS offerings include:

- ***Block-chain authentication.*** Acronis uses blockchain technology in its Cyber Notary offering. Cyber Notary uses a distributed database, or a blockchain, across a decentralized system to prevent data tampering. As it stores data, it also creates a cryptographic hash unique to each file. Using Cyber Notary, organizations can verify their data's authenticity and security.
- ***Built-in AI-based anti-ransomware technology.*** Acronis utilizes its Active Protection software to constantly monitor and scan data files in an organization's systems. As Acronis scans these files, its artificial intelligence (AI) feature detects and identifies suspicious patterns of behavior. Using this feature, it may identify known as well as unreported strains of ransomware. Should ransomware begin to encrypt files, Acronis takes action to detect and halt this process.
- ***Protects iOS and Android mobile devices.*** Using Acronis organizations may centrally protect and recover the data residing on mobile devices along with their other data.

The Acronis Disaster Recovery Service solution epitomizes what small and midsize organizations expect an AIO DRaaS solution to deliver. It brings together an on-premises backup appliance, backup software, and a private cloud to create a turnkey DRaaS solution. Equally important, Acronis addresses key new challenges such as ransomware and protecting data on mobile devices. Including these features makes it practical for organizations to potentially adopt Acronis as their sole backup and recovery solution. ■