Solution Profile

2023-24 DCIG TOP 5

ACRONIS CYBER PROTECT CLOUD MICROSOFT AZURE BACKUP SOLUTION PROFILE

By
Ben Maas, DCIG Consulting Data Protection Analyst,
and Jerome Wendt, DCIG Principal Data Protection Analyst

Acronis Cyber Protect Cloud Microsoft Azure Backup Solution Profile

Table of Contents

Acronis Cyber Protect Cloud Microsoft Azure Backup Solution Profile

SOLUTION

Acronis Cyber Protect Cloud

COMPANY

Acronis
1 Van de Graaff Drive #301
Burlington, MA 01803
(781) 782-9000
acronis.com

DISTINGUISHING FEATURES OF CYBER PROTECT CLOUD

- Integrated data protection that combines backup and cybersecurity into one.
- Stores Azure backups on any type of storage – private or public cloud.
- Blockchain notary that provides proof of data authenticity.
- MSP-specific features such as multi-tenancy and integrated management dashboard.

DISTINGUISHING FEATURES OF TOP 5 MICROSOFT AZURE BACKUP SOLUTIONS

- Protect Azure VM instances.
- Protect on-premises applications and data.
- Protect both Windows and Linux VMs.
- Store backups on data storage outside of Microsoft Azure.

SOLUTION FEATURES EVALUATED:

- *Backup administration.*
- *Backup capabilities.*
- *Configuration, licensing, and pricing.*
- *Cyber resilience.*
- *Recovery and restores.*
- *Snapshot administration.*
- *Support.*

Microsoft Azure Keeping Pace

Since the 2020-21 DCIG TOP 5 Azure Backup Solutions report, the global market size of the public cloud services sector has grown from around $314 billion to a projected $591 billion in 2023.[1] Obtaining definitive numbers on each cloud provider's contribution to this overall revenue number remains difficult.

However, some estimates show Microsoft Azure continuing to slowly gain on Amazon AWS in both its Infrastructure as-a-Service (IaaS) and Platform as-a-Service (PaaS) offerings. In 2020 AWS held a 52.7 percent to 30.6 percent market share lead over Azure. That percentage shrunk by about 3 percent to a projected 49.2 percent to 33.1 percent in 2022.[2] If one adds in Software-as-a-Service (SaaS) offerings such as Microsoft 365 to the mix, Azure may potentially lead in revenue.[3]

As the public cloud matures, different vendors now specialize in different cloud features. Azure continues to specialize in giving organizations that rely heavily upon Microsoft software an easy on-ramp to the cloud.

However, this easy on-ramp to the cloud backfired on some organizations. An easy move to the cloud did not mean they were ready to embrace and manage the cloud. More organizations recognize they may need hybrid and multi-cloud solutions to meet their various IT needs.

This combination of events has not slowed cloud adoption. Rather, companies tend to take a more thoughtful approach about moving infrastructure, applications, and services to the cloud in general and Microsoft Azure specifically. As they do, they must move their backup strategies with them. Otherwise, they risk data loss and downtime due to human error, disaster, or even malicious attack.

The (Re)Emergence of Private Cloud

In early 2023, with the fog of inflation hovering, many prognosticators and apocryphal sources suggest the cost of public clouds exceeds its benefits. Further, many organizations have not experienced the savings that they expected when they moved to the public cloud.

DCIG believes that this has much to do with the applications and workloads that organizations migrated to the cloud. Legacy applications will not reap the benefits of the public cloud without a concerted effort to rearchitect them for cloud technologies. Only then can these applications and workloads capitalize on the public cloud's availability, global presence, and scalability.

This has led to organizations retaining their own private IT infrastructure. "Legacy" storage can be a particularly cost-effective solution for storing infrequently accessed data or backups, to include cloud backups. Enterprises, small and medium businesses (SMBs), and non-profits all should evaluate the best balance of on-premises vs private cloud vs public cloud for their data and workloads.

Microsoft Azure provides the core IaaS services that enterprises need to create a viable multi-cloud strategy. These core services include analytics, compute, database, identity management, networking, storage, virtual desktops, and web. Azure also offers specific services such as artificial intelligence, containers, DevOps, Kubernetes, machine learning, and serverless to assist organizations in achieving these objectives.

1. https://www.statista.com/statistics/273818/global-revenue-generated-with-cloud-computing-since-2009/ accessed 04/17/2023
2. https://www.statista.com/statistics/1202770/hyperscaler-iaas-paas-market-share/ accessed 04/17/2023
3. https://www.statista.com/statistics/1243513/top-10-cloud-vendors-by-revenue-fiscal-quarter-global/ accessed 04/17/2023

Acronis Cyber Protect Cloud Microsoft Azure Backup Solution Profile

The State of Microsoft Azure Backup Solutions

Despite Microsoft's establishment as a global leader in IaaS, there remains a limited number of available Microsoft Azure backup solutions. Even among those that support Azure, a number still bear more resemblance to on-premises backup software than those optimized for cloud backup.

Newly developed or rearchitected Microsoft Azure backup solutions usually are subscription-based SaaS solutions and are often cloud-native.

For instance, several Azure backup solutions require the installation of an agent on each instance or machine to perform backups. These solutions may also require the installation of a management service that the organization's IT staff must maintain.

In many respects, this mimics the way IT admins have maintained end point and server devices for decades. While necessary when protecting physical machines, its value becomes more dubious when backing up virtual machines (VMs) or cloud instances.

Newly developed or rearchitected solutions usually are subscription-based SaaS solutions, and are often cloud-native. Cloud-native solutions may scale up or down based on demand and are usually managed and maintained by the provider. The provider manages the SaaS service to include ongoing software maintenance such as fixes, patches, and upgrades.

These SaaS solutions typically utilize snapshot APIs provided by the hypervisor or cloud storage to provide consistent backups. While they offer agents to protect specific application use cases, they predominantly use snapshots to protect applications and data.

Providing protection of serverless and containerized applications represents another potential area of growth for Microsoft Azure backup solutions. Only five Microsoft Azure backup solutions currently support either the Azure Kubernetes Service or containerized applications.

Common Features across All Microsoft Azure Backup Solutions

DCIG identified twelve solutions in the marketplace that offer backup capabilities for Microsoft Azure. These solutions target organizations of various sizes based on the capabilities described in their User Guides or published data sheets. Attributes that all these solutions generally had in common include support for the following:

1. ***Microsoft 365 integration.*** As organizations move more of their commodity services, such as email and scheduling, to the cloud they often select software-as-a-service (SaaS) providers. The most popular of these SaaS providers is Microsoft. The ability to backup and restore email, calendars, and contacts from Microsoft 365 has become standard in many of the solutions that DCIG evaluated.
2. ***Single-sign-on (SSO) integration.*** One of the more important aspects of security is providing authentication and authorization using third-party software. Modern applications often achieve this using OAUTH2 or SAML, often referred to as single-sign-on (SSO). All the evaluated solutions integrate with SSO.
3. ***Back up all Windows Server versions from 2012 forward.*** Organizations may choose from multiple Microsoft Windows operating systems (OSes) to host their VMs in Microsoft Azure. Any of these backup solutions will protect applications hosted on any Microsoft Windows OS released since 2012.
4. ***Back up several Linux distributions.*** Organizations may also select from among seven Linux releases available in Microsoft Azure. Solutions that protect Linux support all the major Linux distributions, including CentOS/RHEL, Debian/Ubuntu, and SUSE Linux.
5. ***Perform incremental and full backups.*** Every backup solution gives organizations the option to perform full and incremental backups. Most create a first full backup and then do incremental backups thereafter.

Acronis Cyber Protect Cloud Microsoft Azure Backup Solution Profile

Acronis Cyber Protect Cloud takes a holistic approach to data protection by delivering both backup and cyber security together.

Acronis Cyber Protect Cloud

Upon DCIG's completion of reviewing multiple, available Microsoft Azure backup solutions, DCIG ranked Acronis Cyber Protect Cloud as a TOP 5 solution. Acronis Cyber Protect Cloud has offerings for both individuals and organizations though it primarily focuses on Managed Service Providers (MSPs) that serve small and midsized enterprises (SMEs).

Acronis takes a holistic approach to data protection by delivering both backup and cyber security together. Its Cyber Protect agent delivers anti-virus and anti-malware protection in addition to backups, data loss prevention (DLP), detection and response, disaster recovery, vulnerability and patch management, and URL filtering. Acronis also protects Microsoft 365 as part of its broader solution.

Acronis Cyber Protect Cloud offers the following features that help distinguish it from other TOP 5 offerings:

- ***Private cloud backups stored on general-purpose cloud storage.*** Acronis Cyber Protect provides hybrid cloud data protection. It backs up endpoints (desktops and laptops) as well as on-premises and general-purpose cloud servers. Cyber Protect may then store backups on cloud storage available on its own infrastructure as well as from various cloud providers, to include Microsoft Azure Blob.
- ***IT integration.*** Many SMEs utilize Microsoft software in their on-premises IT infrastruc-ture and plan to expand into Microsoft Azure. Acronis Cyber Protect Cloud includes several features that IT staff may leverage as they adopt Azure. Its Operating System patch management feature ensures that server instances running in Azure are on recent OS versions to reduce the attack surface susceptible to bad actors. Acronis also supports auto-detection of new endpoints in Azure and remote installation of agents on them through Active Directory. To protect instances residing in general-purpose public clouds, enterprises must install an agent on them to back them up.
- ***Blockchain Notary.*** Cyber Protect Cloud utilizes blockchain technology to optionally notarize each file modification it detects. This provides proof of data authenticity with an immutable, publicly verifiable certificate with a specific timestamp. To verify authenticity, Blockchain Notary confirms the file matches the checksum contained in the blockchain.
- ***MSP-specific features.*** Acronis supports multiple options within Cyber Protect Cloud to meet the specific needs of MSPs. For instance, its multi-tenancy option permits MSPs to manage numerous organizations from a single integrated dashboard. Acronis also permits an MSP to customize Cyber Protect so it may provide a unique offering for each tenant. ■

About DCIG

The Data Center Intelligence Group (DCIG) empowers the IT industry with actionable analysis. DCIG analysts provide informed third-party analysis of various cloud, data protection, and data storage technologies. DCIG independently develops licensed content in the form of DCIG TOP 5 Reports and Solution Profiles. Please visit **www.dcig.com.**