



BAAS SERVICE DEFINITION

Version: 5.5
Date: 11 August 2021

redcentric

AGILE • AVAILABLE • ASSURED

1 Service Overview

1.1 Introduction

Redcentric BaaS is a cost-effective, Cloud Backup and Disaster Recovery solution with additional endpoint protection and management features. Unlike traditional onsite tape or disk backup the Redcentric BaaS is a highly available cloud based service.

In addition to its comprehensive backup utilities the solution also provides vulnerability, patch management, remote desktop and drive health reports as well as full stack, next generation AI based protection against malware, with URL filtering and automated backup scanning. All this can be achieved through a unified easy to use portal.

1.2 Key Features and benefits

Features

- Highly available Cloud based Backup solution
- Continuous data protection
- Unified dashboards for both backup and security
- Automated data classification for compliance
- Consumption based billing

Benefits

Proactive Ransomware Protection - Avoid downtime by actively protecting files from unauthorised modification and/or encryption. Active Protection uses artificial intelligence and machine learning technologies and white-listing to keep your data safe.

Instant Restore - Manage your recovery time objectives (RTO) and minimise process disruption to seconds, all while maintaining your company's overall productivity with our unique runVM technology.

Complete Protection - Keep your infrastructure and data completely secure, whether you're facing growing amounts of data, adopting new business processes, or migrating to new applications, platforms or cloud. Our BaaS protects 20+ platforms - physical, virtual, cloud or mobile.

Block-chain Notarisation - Ensure data integrity with our innovative block-chain-based Notary technology which prevents damage to or tampering with your files by attacks targeting archive files.

Unmatched Simplicity - Save on licensing, education, integration and daily operations with a simple, scalable tool that manages any data protection task. Our easy-to-learn solution protects data with less effort, so IT generalists can perform backup tasks efficiently.

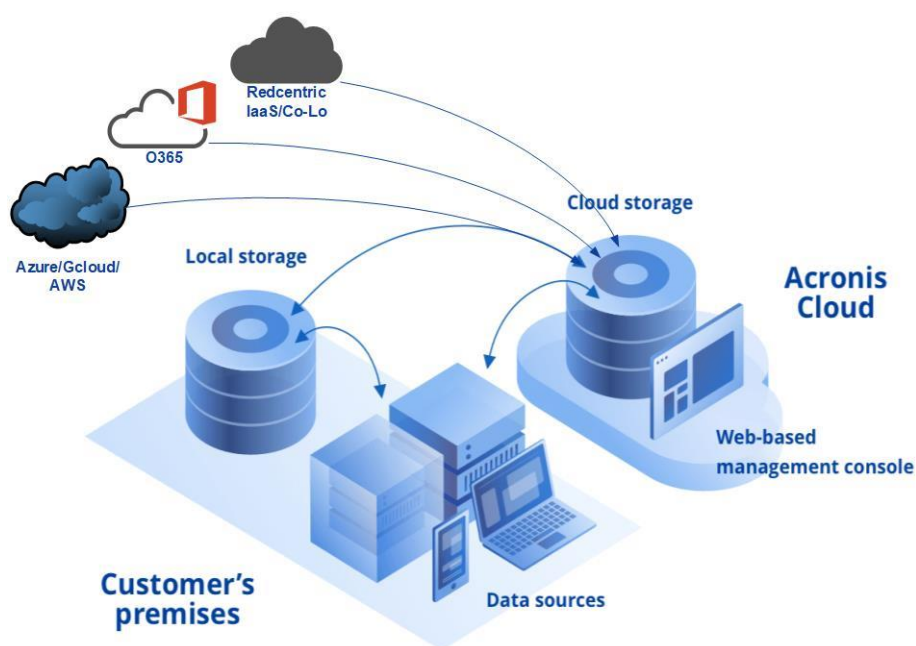
Hybrid Cloud Architecture - Manage all forms of data protection within one workflow through a centralised management and unified control interface. Back up to any kind of storage and recover any piece of data easily with minimum downtime.

2 Service Description

2.1 Introduction

The Redcentric BaaS solution can provide backup capabilities not only to customers on premise physical and virtual servers, but also public cloud services, Office 365 and mobile devices. It is an agent based system that backs up data straight to Acronis cloud storage. The same agent that performs the backup also analyses the systems it is backing up, providing invaluable endpoint information on a customisable dashboard.

2.2 Architectural Overview



2.3 Limitations/Exceptions

Legacy Operating Systems such as Sun/Oracle Solaris and IBM AIX are not supported.

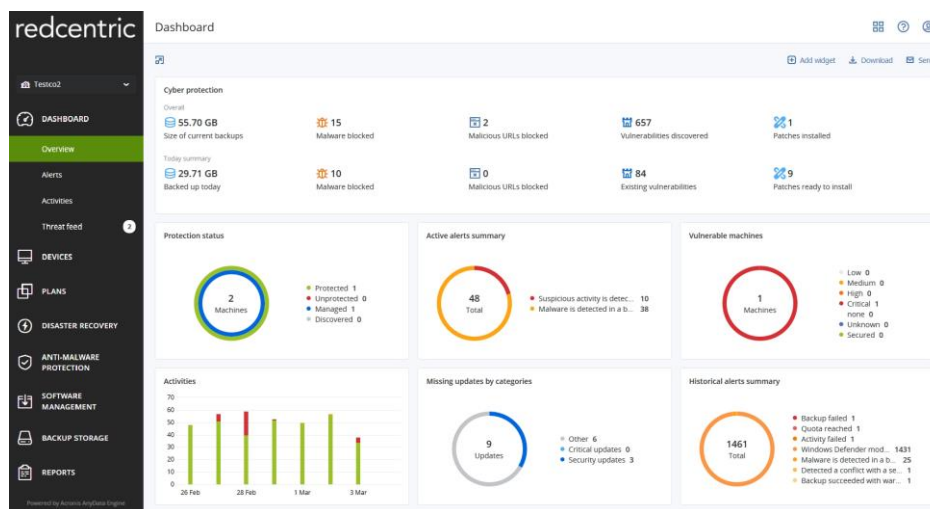
Auto discovery and auto agent deployment are currently limited to Windows devices

2.4 Supported Systems

Server O/S	Virtual	Applications	Cloud	Endpoints	Mobile
<ul style="list-style-type: none"> Windows Server Windows Server Essentials Linux 	<ul style="list-style-type: none"> VMware vSphere Microsoft Hyper-V Scale Computing HC3 Citrix XenServer Red Hat Virtualization Linux KVM Oracle VM Server 	<ul style="list-style-type: none"> Microsoft Exchange Microsoft SQL Server Microsoft SharePoint Microsoft Active Directory Oracle Database SAP HANA 	<ul style="list-style-type: none"> Microsoft 365 G Suite Microsoft Azure Amazon EC2 	<ul style="list-style-type: none"> Windows PC Mac 	<ul style="list-style-type: none"> iPhone iPad Android

2.5 Monitoring

Customers will have access to their own customisable dashboard that provides a quick overview of all the endpoints connected to the Protection suite, giving you a wealth of easily accessible information and triggers that can also be set based on customer defined thresholds.



2.6 Data Storage and Encryption

Users set the password that is used for encryption and the algorithm will encrypt your data at-source with government-approved AES-256 encryption. The password you assign for backup can't be retrieved by anyone else, so you will need to memorize it, this is done by design to adhere to the highest security standards, additionally you can set different passwords for each backup plan when additional internal security is required. In case of a targeted or malware attack, your password won't be found in the agent/program files, and thus there will be no way to decrypt the backup file(s). All management communication between your system and the Acronis Cyber Cloud runs through secure channels with SSL encryption.

All aspects of your data are completely secure at any given time in Tier-IV-designed and SSAE-18 compliant datacenters.

2.7 Location

The Acronis Cloud Datacenter is located in London, UK

It has SOC-1, SOC-2, ISO 9001, ISO22301, ISO27001, Tier 4 and HIPPAA certifications

More information on the Acronis Datacenters can be found here: <https://www.acronis.com/en-gb/data-centers/>

2.8 Service Management RACI – Backup

Task	Customer	Redcentric
Pre Sales		
Backup feature analysis (Management level, Agent function, Data types, Retention levels, RPO)	✓	✓
Identification of Endpoint and Storage Consumption requirements	✓	✓
License Model recommendation (Workload Centric/Storage Centric)		✓
High Level Design		✓
Initial Build		
Create Customer within the BaaS Portal		✓
Customer user initial account creation		✓
Assignment of licenses		✓
Customer Training		✓
Office 365 connection validation (where applicable)	✓	✓
Operational Service Management		
Acronis Cloud Service Monitoring and support		✓
Technical Support		✓
Service Health Review	✓	✓
Backup Monitoring Success/Failure	✓	
Agent Deployment	✓	
Endpoint device support	✓	
Access requests		✓
Offboarding		✓
Service Outage/Incident tracking		✓
Premium Service		
Backup Schedule Workshop	✓	✓
Backup Monitoring Success/Failure		✓
Backup Restarts		✓
Agent Failure Tracking and triage		✓
Restoration Assistance	✓	✓

2.8 Solution Features

The base features are extensive and these can be discussed during the engagement, in addition add-ons can be purchased that further expand the solutions capabilities.

Base Features (Included with any Workload or GB backup License Purchase)	Advanced Backup	Advanced Disaster Recovery	Advanced Security	Advanced Management
<ul style="list-style-type: none"> Backup <ul style="list-style-type: none"> File backup Image backup Applications backup Network shares backup Backup to cloud storage Backup to local storage Disaster Recovery <ul style="list-style-type: none"> Test failover Cloud-only VPN connection Security <ul style="list-style-type: none"> CyberFit score Vulnerability assessment Active protection Antivirus and anti-malware without local signature-based detection Device control Management <ul style="list-style-type: none"> Group management of workloads Centralized plans management Remote desktop Remote assistance Hardware inventory 	<ul style="list-style-type: none"> Continuous data protection Backup support for Microsoft SQL Server Clusters, Microsoft Exchange Clusters, Oracle DB, SAP HANA Data protection map and compliance reporting Scheduled backup reports 	<ul style="list-style-type: none"> Production and test failover to Acronis Cloud Runbooks: disaster recovery orchestration VPN-less deployment option IPsec Multisite VPN support, L2 site-to-site open VPN Multiple templates Custom DNS configuration 	<ul style="list-style-type: none"> URL filtering Exploit prevention Enhanced signature-based detection Anti-malware scans of data in the Acronis Cloud: Offload client endpoints to enable more aggressive scans and ensure malware-free backups Forensics data in backups Smart protect plans Automatic allow listing Safe recovery: AV definition updates and anti-malware scans as part of recovery process to prevent threat recurrence Remote device wipe Windows anti-malware management 	<ul style="list-style-type: none"> Automated patch management Software inventory collection Drive health monitor Fail-safe patching Report scheduling

3 Billing

3.1 Introduction

There are two overarching models for purchase, both of which are usage based models; you will only be charged for the quantities consumed each month.

GB Model

In this model, a cost for total backup storage ingested will be charged, regardless of any standard endpoints used. Additional Advanced packs can be purchased on a per workload/instance where needed.

Workload Model

In the Workload model you pay for both agent type/count as well as a cost for storage backup when using Acronis Cloud Storage as the destination as with the GB model, additional Advanced packs can be purchased where needed.

3.2 Decision Point

The decision on which model to go with will be discussed with the customer before onboard as the combination of agent/storage requirements can have a large impact as to which model is more cost effective for the customer.

Premium Service

The BaaS can be provisioned as both self service or with a premium option; with the premium option, Redcentric can provide monitoring, and remediation of backup failures on behalf of the customer, as well as restoration assistance, advice and personalised recommendations.

Self Service Capabilities

As part of the onboarding process Redcentric will provision the customer in the Redcentric Self Service system, this will allow customers once onboarded to add and remove base and advanced license packs as well as review the detailed billing breakdown each month.

4 Out of scope/exclusions

In addition to any other exclusions specifically mentioned in this Service Definition, the following are excluded from Redcentric's Service:

- Customers are responsible for managing their own Windows Licenses
- The design and performance of the Customer's on premise computing environment;
- The design and performance of the Customer's Internet connectivity where not taken as an additional service;
- The impact to performance or stability due to the customers installed applications

5 Support

We can offer in-depth, responsive and SLA-backed support from a team that is accessible and accountable and that knows your business. We work within the ITIL framework to ensure a consistently high standard of service desk provision and an enduring commitment to continuous improvement.

5.1 End of life operating systems

If the system being backed up has an operating system that is no longer supported by the manufacturer support will be provided on a reasonable endeavours basis

If service desk has exhausted their resources in resolving a problem, the recommendation will be to upgrade to a supportable operating system.

5.2 Hours of Service

Hours of Service are 24/7

5.3 Service Levels

Availability

Availability is defined as the end user can login to the Cyber Protect Portal and make changes to the connected agents.

SLA

Acronis Cloud service maintains an availability of 99.95% but the overall availability is dependent on the connectivity path used to access the service. If the customers network connectivity is provided by Redcentric please refer to the agreements in place.

For more information regarding service availability, fault reporting, change control and communication please see the Redcentric welcome pack.

5.4 Service lifecycle

Changes to service

As a cloud service, changes may occur to both the interface and functionality of the product, any such change that can impact customers backups will be communicated to the customers prior to the change.

Changes to the Service Description will be reflected on the Server description page with referable versioning

Termination and Service Suspension

Termination and suspension terms are set within the customers Master Services Agreement (MSA)

Expected Lifecycle

Acronis has not declared any support or extended support end dates for the cyber protect products. Additional information can be found here <https://www.acronis.com/en-in/support/lifecycle/business.html>

6 Glossary

6.1 Introduction

This section provides a glossary of terms and acronyms specific to this document. Please add the terms and acronyms specific to the product or service (project).

Term/Acronym	Definition
BAAS	Backup As A Service
BOM	Bill of Materials
NA	Not Applicable
OM	Operational Measurements
OSS	Operational Support Systems
PC	Personal Computer
RACI	R – Responsible; A – Accountability; C – Consulted; I – Informed RACI is part of the DRIVE process
RFI	Request For Information
RFP	Request For Proposal
RTM	Requirements Traceability Matrix
SCM	Supply Chain Management
SR	Service Request
TS	Technical Specifications
TSS	Technical Security Specifications

HEAD OFFICE

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522

E sayhello@redcentricplc.com

W www.redcentricplc.com