

IBM Technology



G-Cloud 15 IBM – Storage Protect for Cloud (SP4C) Service Definition Document

Email: ukcat@uk.ibm.com

Contact: Anne-Marie Wheeler

Introduction

In today's environment of increasing ransomware, malware, accidental deletions and compliance/regulatory pressures, cloud-providers' native protection for SaaS and cloud workloads is often not sufficient under the "shared responsibility" model.

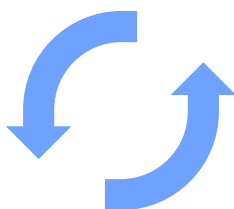
IBM Storage Protect for Cloud addresses these gaps by delivering SaaS-based backup, granular restore, self-service delegation, flexible storage choice, and enhanced security controls across key cloud platforms.



Shared Responsibility Model

Cloud Provider Responsibility

- Loss of service due to hardware or infrastructure failure
- Loss of service due to natural disaster or data center outage
- Short-term user error with recycle bin / version history
- Short-term administrative error with soft-delete for Groups, Mailboxes or services-lead rollback



Security & Compliance User Responsibility

- Loss of data due to malicious insiders or hackers deleting content
- Loss of data due to malware or ransomware
- Loss of data due to departing employees and deactivated accounts
- SLA compliance – recovery from prolonged outages
- Long-term accidental deletion or legal discovery coverage with selective rollback

Cloud Service Provider Recommendations

[Microsoft Services Agreement](#) →

b. We strive to keep the Services up and running; however, all online services suffer occasional disruptions and outages, and Microsoft is not liable for any disruption or loss you may suffer as a result. In the event of an outage, you may not be able to retrieve Your Content or Data that you've stored. We recommend that **you regularly backup your Content and Data** that you store on the Services or store **using Third-Party Apps and Services**.

[Salesforce Services Agreement](#) →

Even with the best of intentions, users and administrators have been in situations where they have either deleted large amounts of data, or have modified records, only to later realize that a mistake was made.

With tools like the Data Loader, it is very easy to mass delete or update records. And **a simple mistake in your source file or field mapping could spell disaster for your data**. It is recommended that you keep a **regular backup of your data and to do a manual point-in-time backup** before you proceed with any major data project within your organization.

By 2028, **75% of large enterprises will adopt backup as a service** (BaaS), alongside on-premise tools, to back up cloud and on-premise workloads, compared with 15% in 2024.

[Gartner](#)

By 2028, **75% of enterprises will prioritize backup of SaaS applications** as a critical requirement, compared with 15% in 2024.

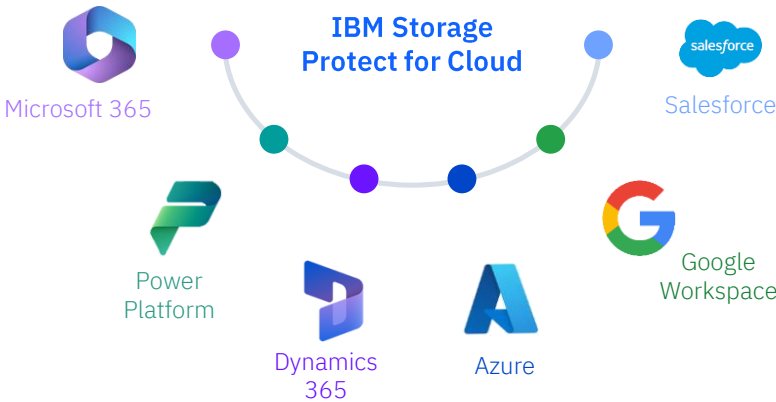
[Gartner](#)



IBM Storage Protect for Cloud

A comprehensive multi-workload data protection platform

Stress-free backup and restore so you can run your aaS data with full confidence. SP4C keeps your business moving forward with automatic 4x daily backups, on-demand backups and comprehensive, simple restores.



SCALE YOUR IT TEAM

Automatic one-click backup builds in best practices to protect critical data. Scale permissions to empower users to self-restore.

IMPROVE BUSINESS CONTINUITY

Recover data faster by quickly locating the instance, object, field data to restore. Compare backups to reduce human error.

PROTECT DATA FROM INTERNAL & EXTERNAL THREAT

Full-fidelity, granular restore helps organizations roll back to the point in time they need. Mitigate malicious attacks or accidental data loss.

IBM Storage Protect for Cloud

Key benefits across all versions



Holistic backup + recovery for critical cloud workloads



Granular restore of users/groups/objects (not just full datasets)



Self-service restore delegation (offloading IT)



Flexible storage: IBM's storage or customer's own storage



SaaS deployment: globally delivered, no patches for you to apply



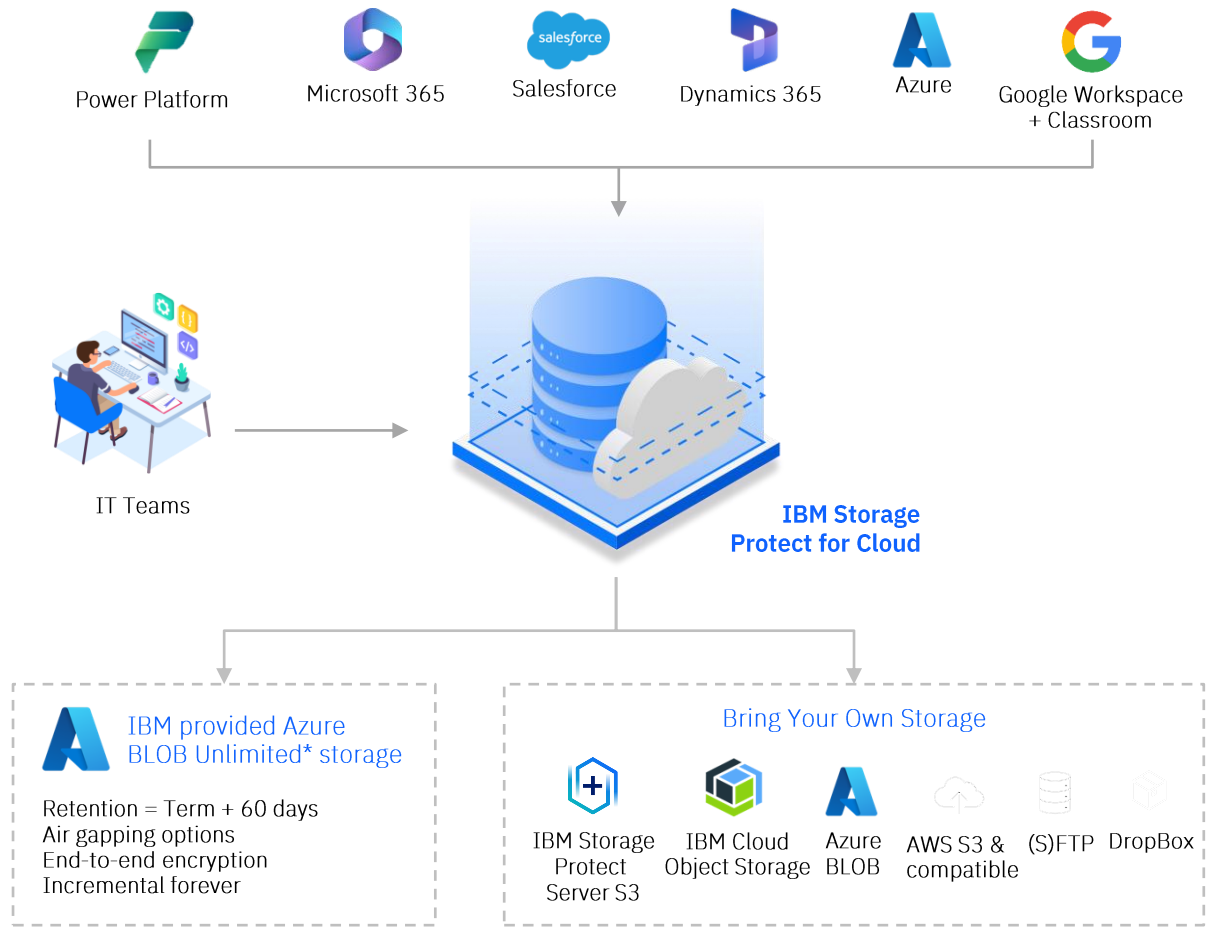
Built-in security: bring-your-own-encryption-keys, MFA, RBAC



Useful for business continuity, ransomware protection, compliance audit-trail

IBM Storage Protect for Cloud [Architecture](#)

High Level Architecture and Storage Options



100%

Software as a Service

7

Cloud Instances in initial roll-out

99%

Service availability

Automated

Version updates and fix deployment

Zero

Local infrastructure costs

2+2

Licensing options:

- Use IBM's Azure storage
- Bring your own storage
- Per user / per month
- Microsoft Entra ID/user/year
- Azure VM + Storage
- New: Google Workspace
- New: Google Classroom
- + free trial option



Solution Brief by Workload

IBM Storage Protect for Cloud

1. Microsoft 365
2. Dynamics 365
3. Google Workspace
4. Azure
5. Salesforce



1 | Microsoft 365

Use case

Protecting data within Microsoft 365 workloads — e.g., Exchange/Outlook, OneDrive, SharePoint, Teams— especially beyond the native retention windows or to guard against malicious deletion, ransomware, insider threats.

Exchange Online

Backup Outlook mailboxes, archives, folders, chats, calendars, contacts, messages, permissions and more



Sharepoint Online

Protect site collections or granular sites, lists, libraries, folders, items, metadata, security, and version history



Project Online

Protect Project Online plans, jobs, tasks, and files



Planner

Backup Planner tasks, buckets, progress, labels, and assignments are kept safe for anytime access



OneDrive for Business

Backup OneDrive for Business lists, libraries, folders, items, metadata, security, settings, and version history



Microsoft Teams

Teams channels, private channels, conversations, work files, meeting items, and more can be covered with ease.



Yammer

Backup Yammer message content, comments, events, and discussions



Teams Chat

Backup and export Teams chat messages to an HTML file



Public Folders

Mailboxes, messages, files, contacts, forms, and postings, all protected



Microsoft 365 Groups

Backup Microsoft 365 Groups, including files, conversations, notebooks, sites, and more



Power Automate

Public cloud service helps teams set up automated workflows between apps and services



Power BI

Unified, scalable platform for self-service and enterprise business intelligence that uncovers insights for making strategic decisions



IBM Storage Protect for Cloud Capabilities

- Flexible backup and incremental after initial full backup.
- Granular restore: e.g., recover deleted files for active users, restore hard-deleted mailbox or OneDrive accounts (even for departed users) for compliance/business continuity.
- Unusual-activity reporting: anomaly detection for ransomware/malware/data-loss.
- Centralized management: scheduling, tracking, reporting of backup/restore.

Why it matters

Many organizations rely on Microsoft 365 but assume “the cloud provider handles everything”. This solution ensures the data layer (users, files, mailboxes, groups) is protected under your control.

Key Business Value

Reduced costs, improved RPO/RT0, security

Ransomware Defence & Early Anomaly Detection

Ransomware - early event detection, quick investigation, remediation guidance.

Delegated Admin

Wall-off access and empower users with delegated administration reducing cost and improving SLAs

Highly Secure

End-to-end data encryption

Bring your own key

GDPR “right to be forgotten”

FedRAMP (data center), ISO 27001 certified

Bring your own storage (BYOS), airgap to tape

Dashboard reporting

Dashboard reporting for visibility and coverage control



2 | Dynamics 365

Use case

Backing up and restoring data in Dynamics 365 (CRM/ERP) applications where native restore capability may be limited or non-existent.

CRM Products



Back-Office ERP



Future Development

IBM Storage Protect for Cloud Capabilities

- Frequent backups (up to four times a day) to ensure availability and integrity of Dynamics 365 data.
- Granular restore: filter by content type, owner, date, file size, email subject, etc.
- Flexible storage: use IBM or your own.
- Compliance support: automated backup logs, audit trails to help demonstrate regulatory adherence.
- Use-cases: recover entity data and record field data; recover deleted documents for active users.

Why it matters

Dynamics 365 often houses critical customer, financial and operational data — loss or corruption can have major business impact. Native backup/restore for these workloads may be constrained.

Key Business Value

Reduced costs, improved RPO/RTO, security

Search & Compare Tools

Compare backup-to-backup to minimize human error

Delegated Admin

Wall-off access and empower users with delegated administration reducing cost and improving SLAs

Highly Secure

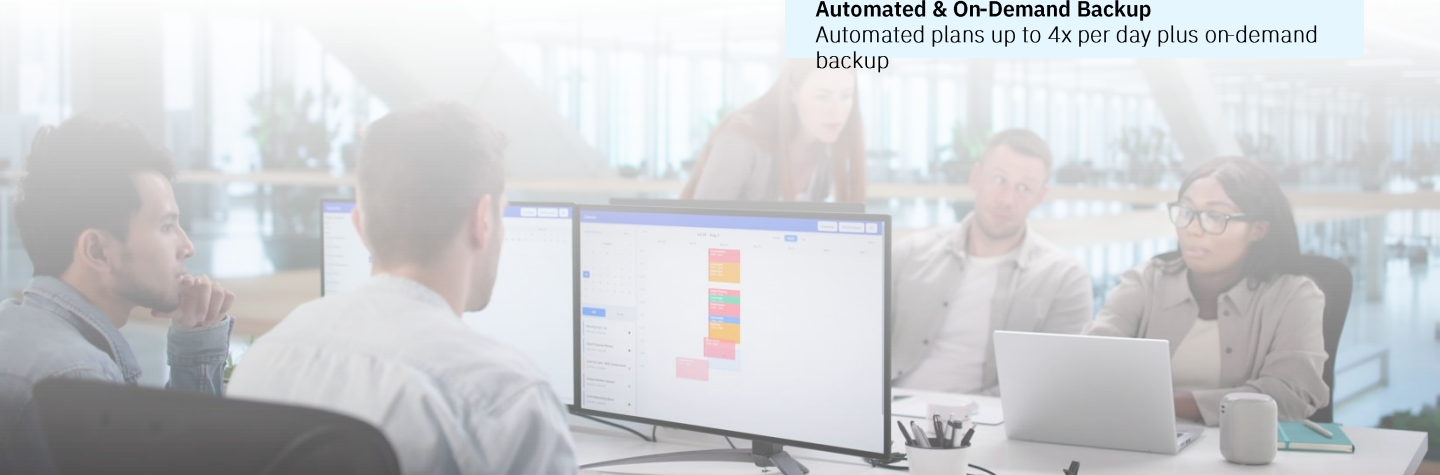
End-to-end data encryption
Bring your own key
GDPR “right to be forgotten”
FedRAMP (data center), ISO 27001 certified
Bring your own storage (BYOS), airgap to tape

Dashboard reporting

Dashboard reporting for visibility and coverage control

Automated & On-Demand Backup

Automated plans up to 4x per day plus on-demand backup



3 | Google Workspace

Use case

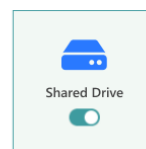
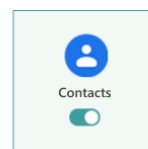
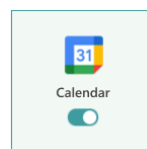
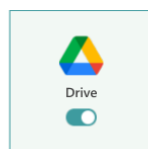
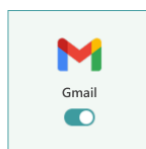
Protecting data in Google Workspace — such as Gmail, Drive, Docs, Sheets, etc. — with more control and flexibility than built-in protections.

Automatic Backups for Long-Term Recoverability

Backup Gmail, Drive, Calendar, Contacts, shared Drives, and Classrooms 4x per day

Support for chat coming soon (1H25)

Automatically scan for, update and protect selected content by user or application.



IBM Storage Protect for Cloud Capabilities

- Ensures availability and integrity of data with backup up to four times a day.
- Self-service restore delegation empowers users and reduces IT burden.
- Granular restore filtering (content type, owner, date, size, subject).
- Enhanced security: BYOK encryption keys, MFA, role-based access controls.
- Flexible storage: IBM or customer-owned.
- Use cases include: recover deleted documents outside native restore window; intelligent monitoring of anomalies/unauthorized access.

Why it matters

As more organizations adopt Google Workspace for collaboration, the risks of data deletion, misuse, or internal threats grow. Microsoft-centric protections may not cover Google workloads.

Key Business Value

Reduced costs, improved RPO/RTO, security

Streamline Backups

Simple configuration with automatic backups 4X per day

Highly Secure

End-to-end data encryption
User account tokens add a layer of security to ensure sensitive data compliance needs are met
FedRAMP (data center), ISO 27001 certified
Bring your own storage (BYOS), airgap to tape

Comprehensive Restore Options

Quickly restore at the organization, object, record, and field levels
Search for and filter content for restore based on properties, backup times and more
Choose to overwrite or merge content and restore security with it, and easily select a recovery point for your data.

Dashboard Reporting

Simple dashboard display gives immediate insight into your backup history and reporting on backup jobs' status.



4 | Azure

Use case

Safeguarding workloads within Microsoft Azure (including Azure Virtual Machines, Azure Blob storage, Azure SQL, Azure DevOps, Azure AD/Entra ID, AD B2C) against data loss, corruption, deletion, or cyber-attack.

IBM Storage Protect for Cloud Capabilities

- Broad coverage: Protects Azure VMs, Blob storage, Entra ID, Azure SQL, DevOps etc.
- Frequent backups (up to 4x/day) and capability to restore specific objects or entire workloads.
- Granular restore: e.g., restore a deleted Entra group and its membership; restore specific Blob objects/folders even if deletion time is unknown.
- Centralized tracking and reporting of backup/restore jobs.
- Enhanced security (BYOK, MFA, RBAC) and flexible storage options.



Microsoft Entra ID and Azure AD B2C



Azure Virtual Machine
Windows or Linux



Azure File Storage



Azure Blob Storage



Azure DevOps



Azure SQL

Why it matters

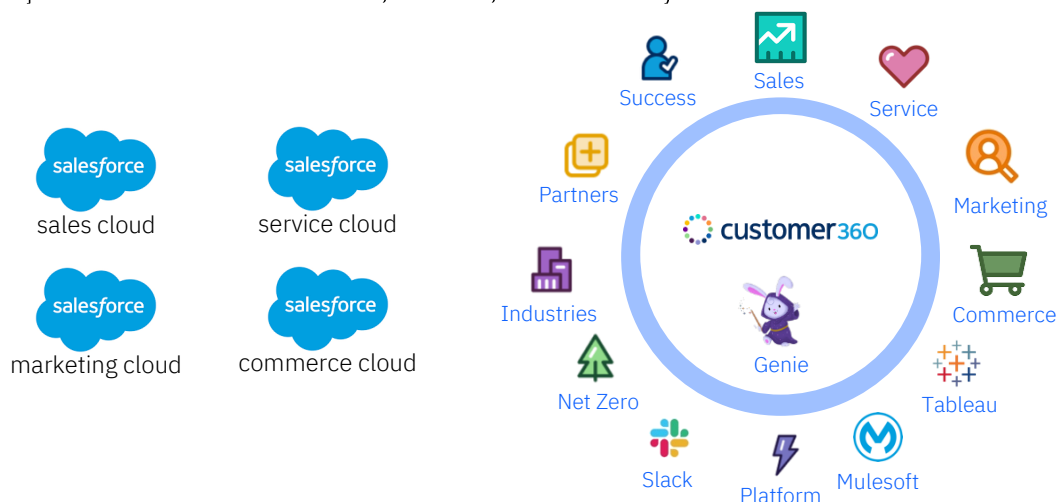
Cloud-native workloads are increasingly business-critical (e.g., IaaS, PaaS). Traditional backups may not cover cloud objects like AD groups, Blob containers, DevOps repos. This protects you from gaps.



5 | Salesforce

Use case

Protecting data in Salesforce — including customer records, sales pipelines, financials, service case data — which is often critical and subject to data-loss risk due to deletion, user error, malicious activity or ransomware.



IBM Storage Protect for Cloud Capabilities

- Backup + restore of your Salesforce applications with granular control.
- Enable self-service restores (delegated) to reduce IT bottlenecks.
- Anomaly detection: Monitor large additions/deletions/updates via dashboard summarizing backup history, object changes, API usage, user activity.
- Granular restore filtering (content type, owner, date created, file size, etc.).
- Storage flexibility: IBM or your own.
- Use-cases: recover deleted documents/users; meet compliance/regulatory retention requirements.

Why it matters

Salesforce environments hold high-value business data that supports revenue generation, customer success and operations. Loss or corruption of this data has a direct bottom-line impact.

Key Business Value

Reduced costs, improved RPO/RT0, security

Search & Compare Tools

Quick search and compare capabilities enable faster data recovery while reducing human errors and complexity.

After backup is complete, perform in or out-of-place granular restoration of Salesforce data while maintaining full fidelity and user mapping.

Delegated Admin

Wall-off access and empower users with delegated administration reducing cost and improving SLAs

Highly Secure

End-to-end data encryption

Bring your own key

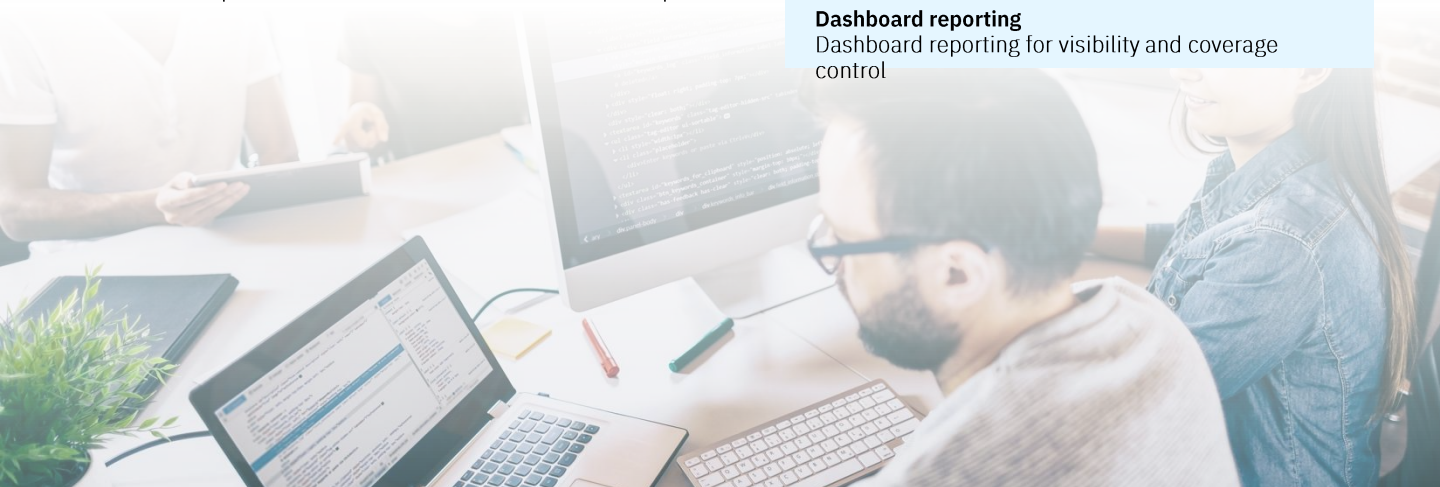
GDPR "right to be forgotten"

FedRAMP (data center), ISO 27001 certified

Bring your own storage (BYOS), airgap to tape

Dashboard reporting

Dashboard reporting for visibility and coverage control



Key Technical Features (common across all areas)

- SaaS-delivered: globally available, no infrastructure to install/maintain.
- Backup frequency: up to 4x daily (depending on platform) to minimize data-loss window.
- Granular restore: ability to select individual objects, folders, files, records, dates.
- Delegated restore/self-service: you can empower business users to restore items without IT bottleneck.
- Flexible storage: either use IBM's managed storage or your own storage (on-premises or cloud).
- Enhanced security: BYOK (bring your own encryption keys), MFA, RBAC for restore operations.
- Audit/compliance support: logs, trails, reporting for regulatory readiness.
- Anomaly-/unusual-activity monitoring (in selected offerings) to detect data-threats proactively.



Business Benefits



Reduced risk of data loss — not relying solely on vendor retention/restore windows.



Improved business continuity — faster recovery, less downtime and disruption.



Operational efficiency — delegated restores reduce IT workload; centralized management simplifies operations.



Regulatory/compliance readiness — audit logging, backup/restore delinquency support helps demonstrate governance.



Flexibility and control — choose storage, control encryption keys, decide restore scope.



Resilience to cyber-threats — detect anomalies, recover from ransomware or insider threats.

Typical Customer Scenarios

- A company using Microsoft 365 accidentally deletes a large number of OneDrive files beyond the vendor retention window; with the Microsoft 365 variant, they restore the deleted content without activating full-scale recovery.
- A business using Dynamics 365 suffers a corrupted batch update to CRM records — with the Dynamics 365 variant they use filtering to restore the affected entity/record-sets only, instead of full system rollback.
- A remote-first company using Google Workspace sees unusual login behavior and wants to then restore deleted team files — the Google Workspace variant offers anomaly alerts and granular restore.
- An infrastructure-centric organization with large Azure workloads (VMs, Blob storage, Azure AD groups) wants to protect against mis-deletions of AD groups or Blob containers — the Azure variant restores those specific objects.
- A sales-driven enterprise using Salesforce wants to monitor API-based mass deletions and be able to recover pipeline data quickly — the Salesforce variant provides monitoring and granular restore of object changes.



Summary

IBM Storage Protect for Cloud offers a unified, SaaS-based solution across five key cloud platforms — Microsoft 365, Dynamics 365, Google Workspace, Azure and Salesforce — to address the common challenge of protecting cloud-native data and applications beyond vendor-native retention and restore capabilities.

With features such as granular restore, frequent backups, delegated self-service, flexible storage, and enhanced security, the solution enables organizations to strengthen their data resilience, support business continuity, and meet regulatory/compliance demands.

If you would like further information or have any questions, please contact a member of the IBM team or visit.

<https://www.ibm.com/products/storage-protect-for-cloud>

Trial IBM Storage Protect for Cloud

- Free 30-day trial
- Setup in 10 minutes
- Enterprise scale 100,000s users
- Convert to an enterprise license in flip of a switch

Sign up here:

ibm.biz/TrySP4CM365
ibm.biz/TrySP4CSalesforce
ibm.biz/TrySP4CD365
ibm.biz/TrySP4CAzure
ibm.biz/TrySP4CGoogleWS



Service Description

IBM Storage Protect for Cloud

This Service Description describes the Cloud Service. The applicable order documents provide pricing and additional details about Client's order.

1. Cloud Service

IBM Storage Protect for Cloud is an IBM data backup and restore service that enables users to migrate, manage and protect data.

1.1 Offerings

The Client may select from the following available offerings.

1.1.1 IBM Storage Protect for Cloud Microsoft 365 with Storage

The Cloud Service is provisioned in an Azure infrastructure environment, which includes compute, virtualization, networking capabilities as well as unlimited Azure storage capacity to support the solution.

1.1.2 IBM Storage Protect for Cloud Microsoft 365 without Storage

The Cloud Service provides all required infrastructure, but it does not include Azure storage capacity to support the solution. Clients who choose this configuration of the Cloud Service can "Bring Your Own Storage" (BYOS) which Client has separately acquired from the Azure cloud.

1.1.3 IBM Storage Protect for Cloud Salesforce with Storage

The Cloud Service is provisioned in an Azure infrastructure environment, which includes compute, virtualization, networking capabilities as well as unlimited Azure storage capacity to support the solution.

1.1.4 IBM Storage Protect for Cloud Salesforce without Storage

The Cloud Service provides all required infrastructure, but it does not include Azure storage capacity to support the solution. Clients who choose this configuration of the Cloud Service can "Bring Your Own Storage" (BYOS) which Client has separately acquired from the Azure cloud.

1.1.5 IBM Storage Protect for Cloud Dynamics 365 with Storage

The Cloud Service is provisioned in an Azure infrastructure environment, which includes compute, virtualization, networking capabilities as well as unlimited Azure storage capacity to support the solution.

1.1.6 IBM Storage Protect for Cloud Dynamics 365 without Storage

The Cloud Service provides all required infrastructure, but it does not include Azure storage capacity to support the solution. Clients who choose this configuration of the Cloud Service can "Bring Your Own Storage" (BYOS) which Client has separately acquired from the Azure cloud.

1.1.7 IBM Storage Protect for Cloud Microsoft Entra ID

The Cloud Service is provisioned in an Azure infrastructure environment, which includes compute, virtualization, networking capabilities as well as unlimited Azure storage capacity to support the solution.

1.1.8 IBM Storage Protect for Cloud Azure Virtual Machines with Storage

The Cloud Service is provisioned in an Azure infrastructure environment, which includes compute, virtualization, networking capabilities as well as Azure storage capacity to support the solution.

1.1.9 IBM Storage Protect for Cloud Azure Virtual Machines without Storage

The Cloud Service provides all required infrastructure, but it does not include Azure storage capacity to support the solution. Clients who choose this configuration of the Cloud Service can "Bring Your Own Storage" (BYOS) which Client has separately acquired from the Azure cloud.

1.1.10 IBM Storage Protect for Cloud Azure Blob/File/Object with Storage

The Cloud Service is provisioned in an Azure infrastructure environment, which includes compute, virtualization, networking capabilities as well as Azure storage capacity to support the solution.

1.1.11 IBM Storage Protect for Cloud Azure Blob/File/Object without Storage

The Cloud Service provides all required infrastructure, but it does not include Azure storage capacity to support the solution. Clients who choose this configuration of the Cloud Service can "Bring Your Own Storage" (BYOS) which Client has separately acquired from the Azure cloud.

1.1.12 IBM Storage Protect for Cloud Google Workspace with Storage

The Cloud Service is provisioned in an Azure infrastructure environment, which includes compute, virtualization, networking capabilities as well as unlimited Azure storage capacity to support the solution.

1.1.13 IBM Storage Protect for Cloud Google Workspace without Storage

The Cloud Service provides all required infrastructure, but it does not include Azure storage capacity to support the solution. Clients who choose this configuration of the Cloud Service can "Bring Your Own Storage" (BYOS) which Client has separately acquired from the Azure cloud.

1.2 Additional Services

1.2.1 IBM Storage Protect for Cloud Microsoft 365 eDiscovery

eDiscovery provides tenant-wide search capabilities for Microsoft Exchange content. The meta-data search can find, export, or delete content across multiple containers. The Cloud Service, IBM Storage Protect for Cloud Microsoft 365, is the prerequisite for IBM Storage Protect for Cloud Microsoft 365 eDiscovery.

1.2.2 IBM Storage Protect for Cloud Dynamics 365 Audit Data

Audit Data backup provides a record of all the changes made in the Dynamics 365 environment between incremental backup jobs. The Cloud Service, IBM Storage Protect for Cloud Dynamics 365, is the prerequisite for IBM Storage Protect for Cloud Dynamics 365 Audit Data.

1.2.3 IBM Storage Protect for Cloud Google Classroom

Classroom provides backup and restore capabilities for Google Classroom data. The Cloud Service, IBM Storage Protect for Cloud Google Workspace, is the prerequisite for IBM Storage Protect for Cloud Google Workspace Classroom.

2. Data Processing and Protection Data Sheets

IBM's Data Processing Addendum at <http://ibm.com/dpa> (DPA) and the Data Processing and Protection Data Sheet(s) (referred to as data sheet(s) or DPA Exhibit(s)) in the links below applies to IBM's processing of personal data on behalf of Client.

<https://www.ibm.com/terms/?id=E64A5680839511EC93C02AA4DE91E682>

3. Service Levels and Technical Support

3.1 Service Level Agreement

IBM provides the Client with the following availability service level agreement (SLA). IBM will apply the highest applicable compensation based on the cumulative availability of the Cloud Service as shown in the table below. The availability percentage is calculated as the total number of minutes in a contracted month, minus the total number of minutes of Service Down in the contracted month, divided by the total number of minutes in the contracted month. The Service Down definition, the claim process and how to contact IBM regarding service availability issues are in IBM's Cloud Service support handbook at <https://www.ibm.com/support/pages/node/731179>.

Availability	Credit (% of monthly subscription fee*)
Less than 99.9%	2%
Less than 99.0%	5%
Less than 95.0%	10%

* The subscription fee is the contracted price for the month which is subject to the claim.

3.2 Technical Support

Technical support for the Cloud Service, including support contact details, severity levels, support hours of availability, response times, and other support information and processes, is found by selecting the Cloud Service in the IBM support guide available at <https://www.ibm.com/support/home/pages/support-guide/>.

4. Charges

4.1 Charge Metrics

The charge metric(s) for the Cloud Service are specified in the Transaction Document.

The following charge metrics apply to this Cloud Service:

- Authorized User is a unique user authorized to access the Cloud Services in any manner directly or indirectly (for example, through a multiplexing program, device or application server) through any means.
- Terabyte (TB) is 2 to the 40th power bytes of data processed by, analyzed, used, stored, or configured in the Cloud Services.
- Virtual Server is comprised of processing units, memory and input/output capabilities that executes requested procedures, commands or applications made available to the Cloud Services.

5. Additional Terms

For Cloud Service Agreements (or equivalent base cloud agreements) executed prior to January 1, 2019, the terms available at <https://www.ibm.com/acs> apply.

