TECHNICAL VALIDATION

IBM Storage Protect for Cloud

Simplifying Data Backup and Restoration for Cloud-native Applications

By Alex Arcilla, Senior Validation Analyst
Enterprise Strategy Group

November 2023

This Enterprise Strategy Group Technical Validation was commissioned by IBM and is distributed under license from TechTarget, Inc.

Contents

Introduction

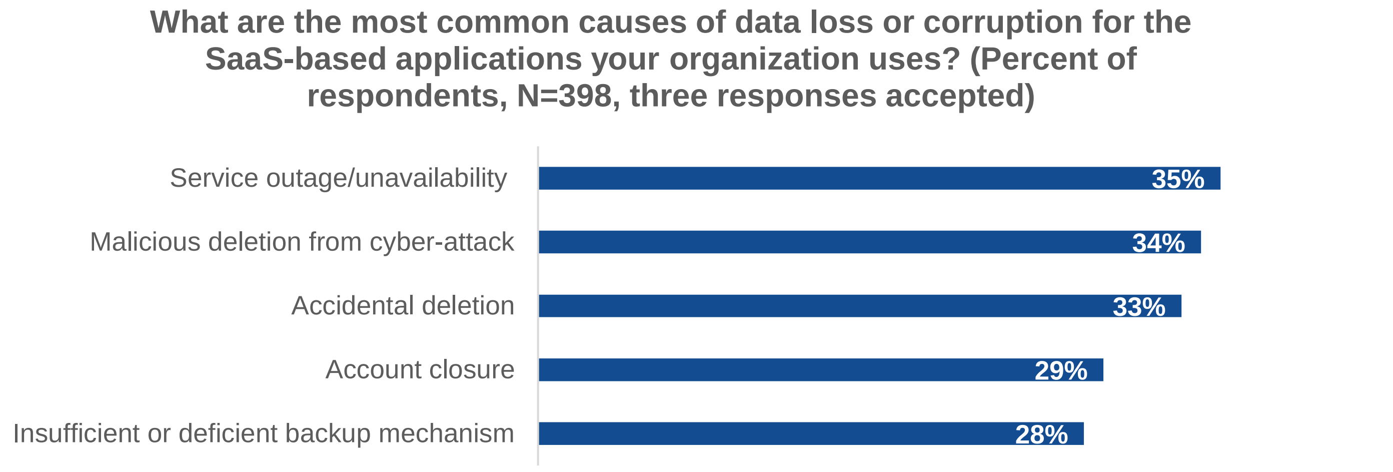
This Technical Validation from TechTarget's Enterprise Strategy Group documents our evaluation of IBM Storage Protect for Cloud. We reviewed how this platform can simplify the way organizations back up and restore data for widely adopted SaaS-, PaaS-, and IaaS-based applications and workloads, specifically Microsoft 365, Microsoft Dynamics 365, Microsoft Azure, Salesforce, and Google Workspace.

Background

When using a cloud service provider's (CSP's) SaaS, PaaS, or IaaS, organizations are bound by the shared responsibility model. While CSPs are responsible for maintaining the performance, availability, and security of their service and underlying infrastructure, organizations consuming those services are responsible for ensuring that any data used and stored within those services remains whole and secured.

Fulfilling this shared responsibility is a must, especially with SaaS applications, as Enterprise Strategy Group's (ESG's) research uncovered that 53% of respondents have experienced some data loss and corruption in the past year.[1] This data loss and corruption in SaaS-based applications does not only originate from cyber attacks; two of the top five causes are attributed to user or administrator error, specifically accidental deletion or closure (see Figure 1).[2] These specific causes are also of great concern for IaaS-based applications.[3]

Figure 1. Most Common Causes of Data Loss or Corruption in SaaS-based Applications



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Public cloud adoption—from a SaaS, PaaS, and IaaS perspective—has not abated, as 54% of respondents to ESG research stated that 21% to 50% of their business applications are now public cloud-resident.[4] As the amount of cloud-resident application data increases, the need to protect against data loss or corruption becomes more critical. Not protecting against data loss carries great risk, including disrupting normal business operations and leaking data

[1] Source: Enterprise Strategy Group Research Report, *Data Protection for SaaS*, February 2023.
[2] Ibid.
[3] Source: Enterprise Strategy Group Complete Survey Results, *Cloud Data Protection Strategies at a Crossroads*, July 2023.
[4] Source: Enterprise Strategy Group Research Report, *2023 Technology Spending Intentions Survey*, November 2022.

to unauthorized users and bad actors, both of which could lead to lost revenue and lost customer goodwill. The risk of ransomware payouts has also increased as prominent brands have experienced high-profile security breaches.

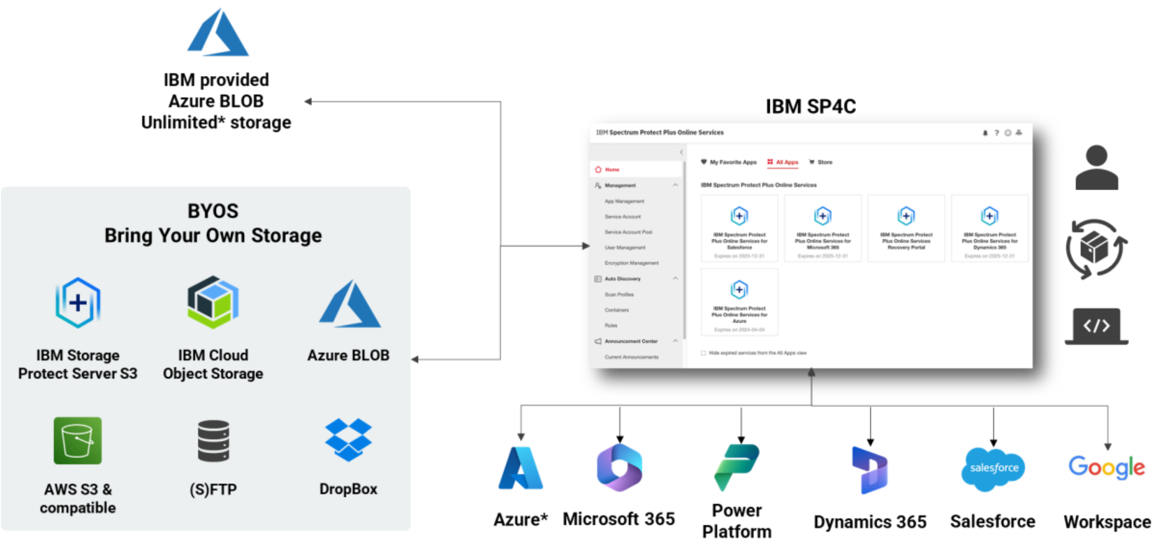
IBM Storage Protect for Cloud

IBM Storage Protect for Cloud (SP4C) has been designed to back up and recover data for SaaS-, PaaS-, and IaaS-based applications, helping organizations fulfill their part of the shared responsibility model. Delivered via the SaaS model, IBM SP4C provides data backup and recovery for:

- Microsoft 365, including Exchange, SharePoint, OneDrive for Business, Teams, Groups, Project, Power BI, Power Automate, and Power Apps.
- Microsoft Azure, including Active Directory, Virtual Machine, and BLOBs/Files Storage.
- Microsoft Dynamics 365, including Sales, Marketing, Commerce, Customer Service, and Field Service.
- Salesforce, including Sales, Marketing, Service, and Commerce Clouds.
- Google Workspace, including Gmail, Drive, Calendar, Contacts, Shared Drive, and Classroom.

IBM SP4C enables organizations to backup and restore data for the aforementioned SaaS-, PaaS-, and IaaS-based applications via the centralized dashboard (see Figure 2). Once selecting the application to back up, organizations can choose their backup storage: either IBM's Azure BLOB Storage (unlimited in most cases) or bring your own storage. Incremental backups are continuous for the desired length of time, plus an added six months. IBM SP4C also enables organizations to back up data up to four times daily.

Figure 2. IBM Storage Protect For Cloud



Source: IBM and Enterprise Strategy Group, a division of TechTarget, Inc.

With IBM SP4C, organizations can experience the following benefits, regardless of the cloud-native applications or services supported:

- **Improved recovery time objectives (RTO) and recovery point objectives (RPO).** Instead of relying on a centralized IT group for recovering data, internal groups using these applications can delegate a local administrator to perform backup and restoration in case of service disruption. By delegating administrators within end-user groups, organizations can improve RTOs and RPOs, thus helping to satisfy internal service-level agreements (SLAs).

- **Reduced IT expenses.** Delegating local administrators for data backup and recovery of cloud-native applications and services helps decrease the associated time and effort that a centralized IT group would typically spend on these tasks.
- **Scaled IT teams.** Local administrators can empower a select number of end users to restore the data of specific applications. By offering "self-service" backup and restoration options, organizations essentially scale the IT teams supporting backup and restoration activities.
- **Faster detection and remediation of suspicious events and anomalies.** By leveraging the incremental backups, IBM SP4C can decrease the time and effort needed to locate and remediate suspicious activity quickly. Organizations can also monitor additions, deletions, or updates across objects and trigger alerts for unusual activity (e.g., bulk changes made in a brief time period).
- **Enhanced data security.** Aside from encrypting data end to end (both at rest and in flight), IBM SP4C enables organizations to supply their own encryption keys. For added security, all data can be air gapped to tape. The solution also helps organizations comply with FedRAMP[5] (for IBM Azure data center), ISO 27001[6], and GDPR, including GDPR's "right to be forgotten."[7]
- **Real-time visibility and control.** With IBM SP4C's centralized dashboard, administrators can configure the scope of data to back up (e.g., U.S. sales data backed up four times daily) and assess data backup and recovery status in real time.

For managed service providers (MSPs) that want to offer IBM SP4C, IBM provides a Partner Portal to manage multiple clients. As partners, MSPs can assume tasks IBM would manage by default, acting as their clients' IT team. Partners can also buy licenses in bulk and manage those licenses for their own clients downstream.

Enterprise Strategy Group Technical Validation

Enterprise Strategy Group validated the benefits that IBM SP4C can deliver to organizations. Using online demonstrations of specific use cases, we evaluated how IBM SP4C simplifies data backup and restoration as well as anomaly detection so that organizations can control and secure their data.

Protect Against Breaches and Ransomware

The persistent threat of breaches and ransomware requires organizations to take a more active role in defending against this threat. Leveraging the "forever" incremental backups, IBM SP4C uses anomaly detection and machine learning to identify suspicious pattern file changes or objects within and across backups.

Enterprise Strategy Group Testing

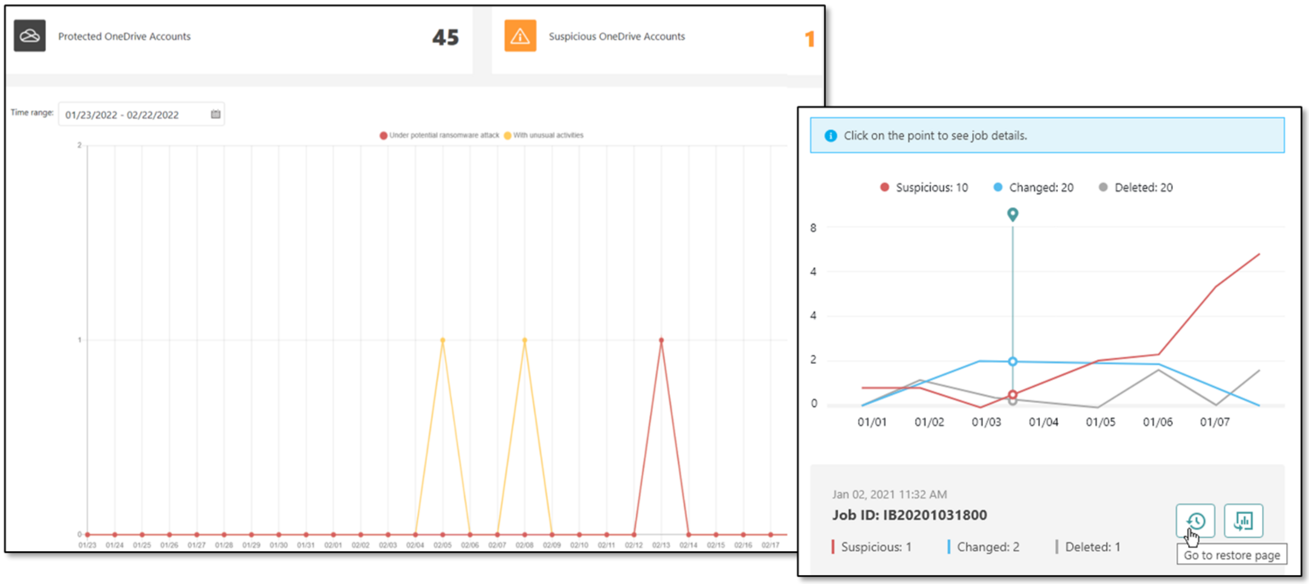
Enterprise Strategy Group first navigated to IBM SP4C Microsoft 365. From the sidebar, we chose **Microsoft 365 Unusual Activities Report** to see the screen displayed in Figure 3. Based on comparing incremental backups of 45 OneDrive accounts, SP4C flagged two suspicious activities (in orange) and one potential ransomware attack (in red) in one account.

Clicking on the OneDrive account displaying suspicious activity, we could investigate the events occurring over a given timeframe, including the number of suspicious events detected, the number of changes made to data during a backup, and the number of objects deleted (or corrupted) when the backup occurred. We could also restore objects based on a good incremental backup.

[5] FedRAMP is a U.S. government program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
[6] ISO 27001 is an international standard focused on information security.
[7] GDPR's "right to be forgotten" gives end users the right to have their personal data erased, without undue delay, by the data controller when that data is no longer necessary to the purpose for which it was collected or processed.

For the other applications supported by SP4C, alerts and rules could also be created to detect suspicious activity, such as frequency of data changes occurring between subsequent backups.

Figure 3. Early Detection, Investigation, and Remediation of Suspicious Activity in Microsoft 365


Protected OneDrive Accounts 45

Suspicious OneDrive Accounts 1

Time range: 01/23/2022 - 02/22/2022

Click on the point to see job details.

Jan 02, 2021 11:32 AM

Job ID: IB20201031800

Suspicious: 1 | Changed: 2 | Deleted: 1

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

High-profile ransomware events have promoted organizations to be more diligent about detection and prevention. In fact, Enterprise Strategy group research found that 30% of respondents noted that detecting and stopping data breaches in real time is one of their three most significant data security challenges.[8]

Enterprise Strategy Group validated that IBM SP4C can help organizations address this challenge. With IBM SP4C Microsoft 365, we observed how anomalies, such as data modifications, deletions, and suspicious activities, were flagged by applying anomaly detection and machine learning within and across incremental backups. Organizations can then identify, isolate, and respond to suspicious activity more quickly by, for example, knowing which backup is clean when recovering data.

Delegate Administrator Rights

Instead of relying on central IT groups to complete all data backup and restoration tasks, organizations can use IBM SP4C to delegate administrator rights to select people working closely with specific cloud-native applications and associated data. Local administrators can monitor and restore data or assign "self-service" recovery responsibilities to select end users.

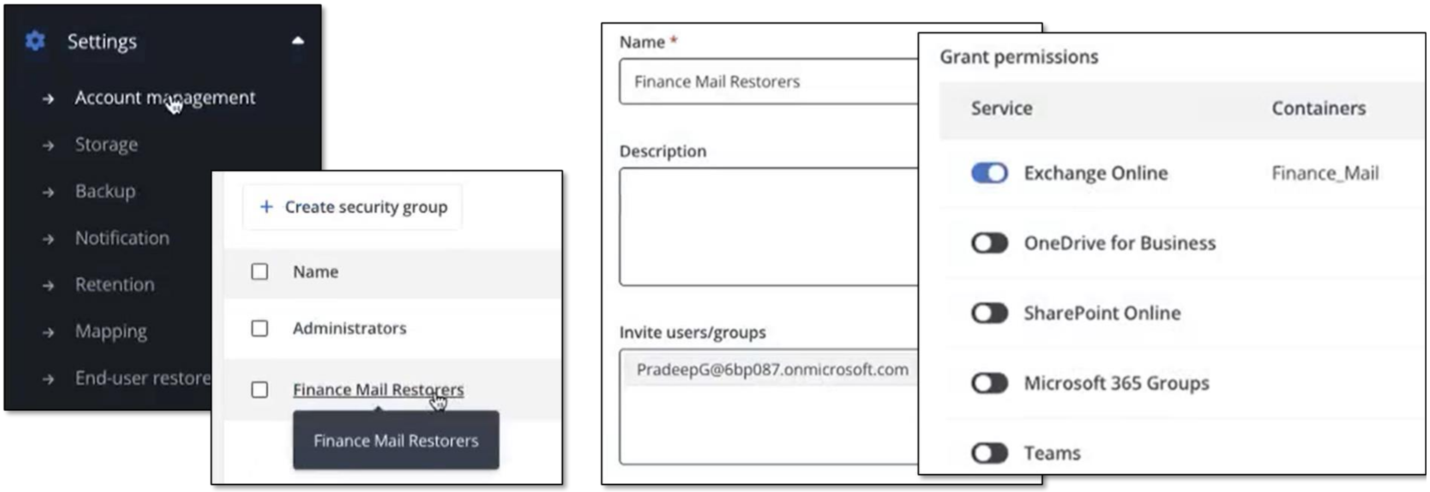
Enterprise Strategy Group Testing

Enterprise Strategy Group considered the use case in which end users located globally within multiple regions use Microsoft 365. While each region had an administrator, data recovery responsibilities for a specific scope of data were assigned to individuals.

[8] Source: Enterprise Strategy Group Complete Survey Results, *The Cloud Data Security Imperative*, April 2023.

We observed how to delegate additional administrators and their permissions (see Figure 4). From the global administrator page of IBM SP4C Microsoft 365, we navigated to the **Account Management** option in the sidebar. We created a security group to delegate limited restoration rights to select individuals (via email addresses), granting permissions to specific Microsoft 365 applications. For example, the "Finance Mail Restorers" security group included users within the finance organization allowed to restore data for Exchange Online only.

Figure 4. Assigning Restoration Permissions to Users Within a Security Group



Name *: Finance Mail Restorers

Description:

Invite users/groups: PradeepG@6bp087.onmicrosoft.com

Grant permissions

Service	Containers
● Exchange Online	Finance_Mail
○ OneDrive for Business	
○ SharePoint Online	
○ Microsoft 365 Groups	
○ Teams	

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

Minimizing RTOs and RPOs is critical for restoring normal business operations as quickly as the business demands. However, submitting data restoration tickets to a central IT group can add unnecessary delay, as they also must deal with other issues throughout the organization.

Enterprise Strategy Group validated that IBM SP4C can help organizations to take this burden off of central IT by enabling designated administrators with data restoration rights to local end users of the cloud-native application protected by IBM SP4C. By creating security groups, select users outside of IT can be assigned data restoration permissions to specific applications. Should data need to be recovered, local users can respond more quickly, without needing to submit requests to IT. RTOs and RPOs can then decrease and ensure business continuity.

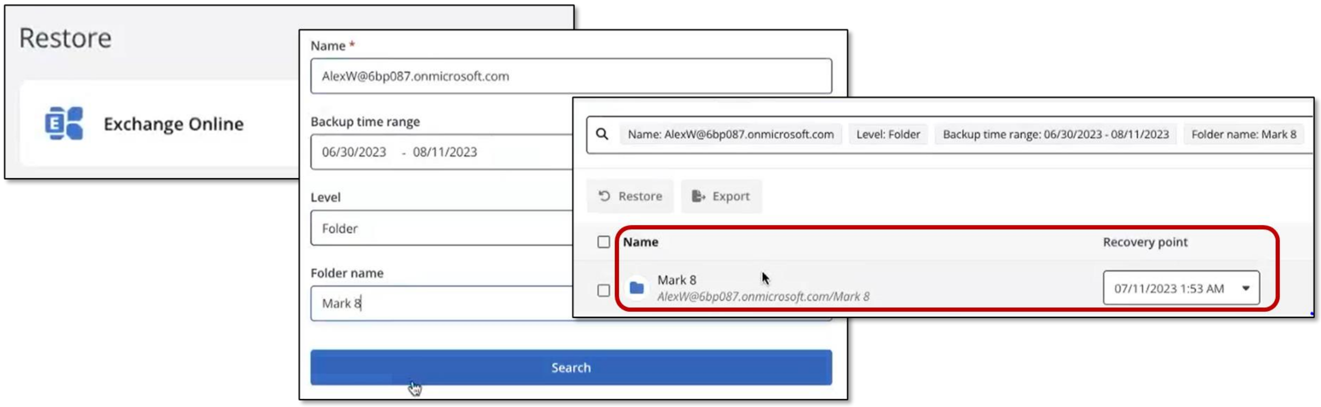
Simplify Data Restoration

Once administrator rights have been delegated, the process for restoring data is simple and consistent across the supported cloud application suites and Microsoft Azure services. Simplifying this workflow also helps to improve RTOs and RPOs, as time spent on these tasks is minimized.

Enterprise Strategy Group Testing

We then reviewed how lost data can be restored for both Microsoft 365 and Microsoft Azure. Enterprise Strategy Group (ESG) first considered the case in which a user reported accidently deleting a file from an Exchange account named "Mark 8." After logging in as administrator, we clicked on the **Exchange Online** panel (see Figure 5).

Figure 5. Searching for Accidently Deleted Data From an Exchange Account in Microsoft 365



Restore

Exchange Online

Name *: AlexW@6bp087.onmicrosoft.com

Backup time range: 06/30/2023 - 08/11/2023

Level: Folder

Folder name: Mark 8

Search

Name: AlexW@6bp087.onmicrosoft.com | Level: Folder | Backup time range: 06/30/2023 - 08/11/2023 | Folder name: Mark 8

Restore | Export

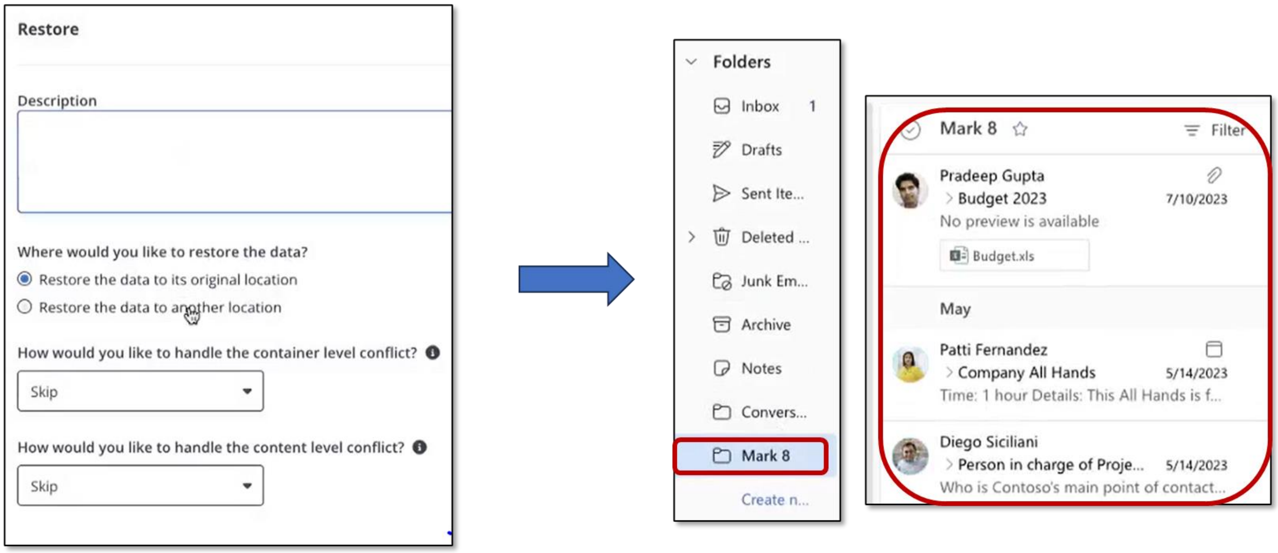
Name	Recovery point
Mark 8 AlexW@6bp087.onmicrosoft.com/Mark 8	07/11/2023 1:53 AM

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

We entered the search terms for locating the accidentally deleted data: email account, backup time range, level of recovery to conduct (i.e., at folder level), and data name (or folder name, in this case). The search uncovered the folder to be restored.

We then specified the criteria for the restore, such as where to place the restored data and how to handle conflicts (see Figure 6). After an observed short period of time, the folder was restored to the email account. Folder contents were also verified to be restored.

Figure 6. Restoring Data to an Email Account



Restore

Description

Where would you like to restore the data?

● Restore the data to its original location

○ Restore the data to another location

How would you like to handle the container level conflict?: Skip

How would you like to handle the content level conflict?: Skip

Mark 8 — Filter

Pradeep Gupta — Budget 2023 — 7/10/2023
No preview is available
Budget.xls

May

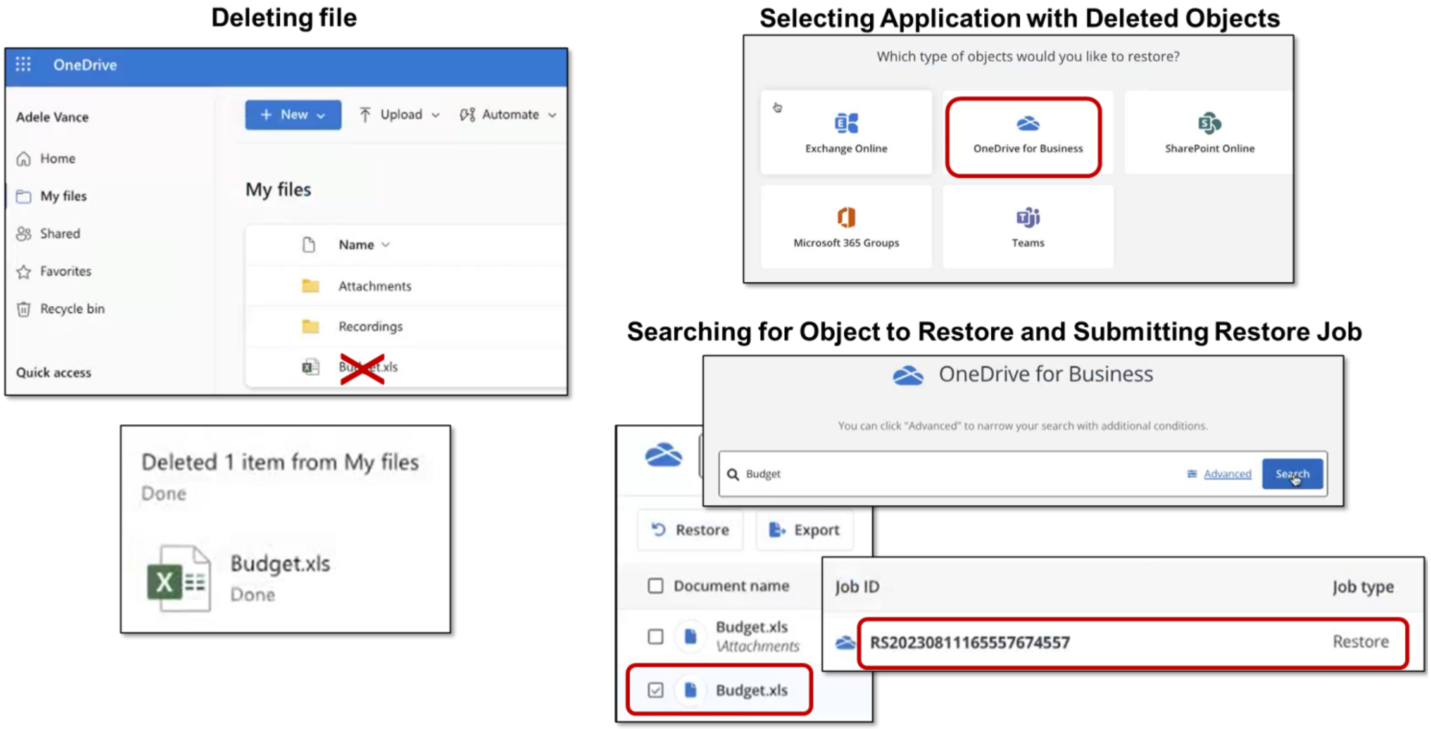
Patti Fernandez — Company All Hands — 5/14/2023
Time: 1 hour Details: This All Hands is f...

Diego Siciliani — Person in charge of Proje... — 5/14/2023
Who is Contoso's main point of contact...

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

ESG then observed how an end user assigned "self-service" rights can restore data in Microsoft 365. After logging into an end-user account, we navigated to OneDrive for Business and deleted the "budget.xls" file (see left-hand side of Figure 7). We then navigated to the self-service portal (see right-hand side of Figure 7) and noted that this end user was given restoration rights to multiple Microsoft 365 applications, unlike the previous use case in which the administrator only had rights to restore data in Exchange.

Figure 7. Self-serve Restoration of an Accidently Deleted File


Deleting file

Selecting Application with Deleted Objects

Searching for Object to Restore and Submitting Restore Job

Deleted 1 item from My files
Done
Budget.xls
Done

Which type of objects would you like to restore?

OneDrive for Business

You can click "Advanced" to narrow your search with additional conditions.

Budget

Job ID	Job type
RS20230811165557674557	Restore

☐ Document name
☐ Budget.xls \Attachments
☑ Budget.xls

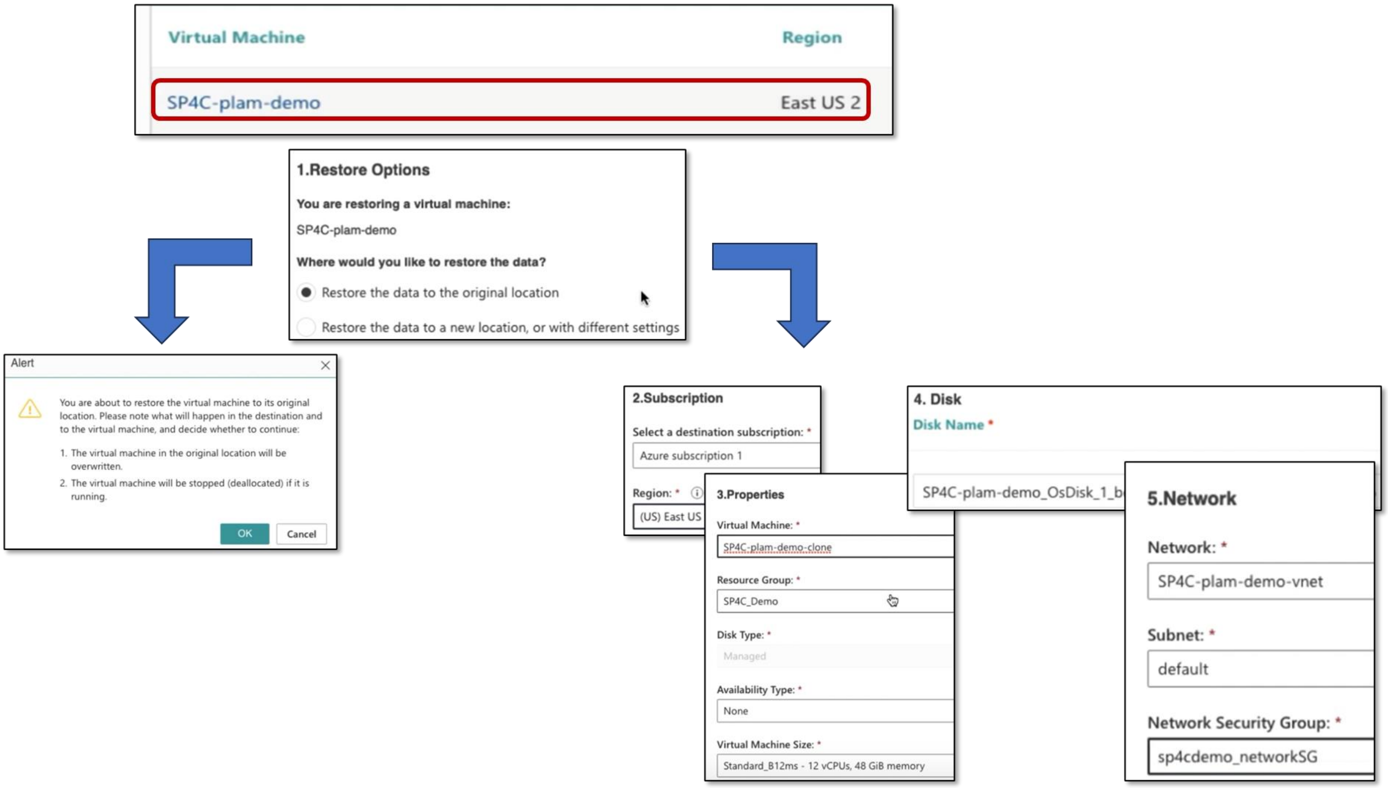
Source: Enterprise Strategy Group, a division of TechTarget, Inc.

After clicking on the **OneDrive for Business** panel, we entered the search term *budget*, which resulted in a number of object names containing that term. After clicking the check box next to the “budget.xls” item, we clicked on the **Restore** button, and the file was restored according to the related Job ID.

Finally, ESG observed how data can be restored in Microsoft IaaS and PaaS platforms. We considered the case in which an administrator needs to restore a virtual machine (VM). From the IBM SP4C Microsoft Azure webpage, we chose the **Azure Virtual Machine** option, the specific VM to restore—“SP4C-plam-demo” in the “East US 2” region—and the backup to use (see Figure 8).

We then chose to restore either to the VM’s original location or to a new location. IBM SP4C flagged that restoring the VM to the original location would overwrite the VM and, if running, would cease operation. However, if restoring to a different location, we were guided to make the appropriate changes, if needed, to the Azure subscription used, the location, VM properties (such as name and machine type), disk type, and network connections. In both cases, clicking on **Restore** would submit the request and could be tracked for status.

Figure 8. Restoring an Azure VM



Virtual Machine	Region
SP4C-plam-demo	East US 2

1.Restore Options

You are restoring a virtual machine:

SP4C-plam-demo

Where would you like to restore the data?

● Restore the data to the original location

○ Restore the data to a new location, or with different settings

Alert

You are about to restore the virtual machine to its original location. Please note what will happen in the destination and to the virtual machine, and decide whether to continue:

1. The virtual machine in the original location will be overwritten.
2. The virtual machine will be stopped (deallocated) if it is running.

2.Subscription

Select a destination subscription: * Azure subscription 1

Region: * (US) East US

3.Properties

Virtual Machine: * SP4C-plam-demo-clone

Resource Group: * SP4C_Demo

Disk Type: * Managed

Availability Type: * None

Virtual Machine Size: * Standard_B12ms - 12 vCPUs, 48 GiB memory

4. Disk

Disk Name * SP4C-plam-demo_OsDisk_1_b

5.Network

Network: * SP4C-plam-demo-vnet

Subnet: * default

Network Security Group: * sp4cdemo_networkSG

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

The workflow for restoring data should be as simple as possible, as restoration permissions can be granted to anyone in the organization. Simple workflows also improve RTOs and RPOs as they minimize the time to restore data needed to maintain normal business operations.

Enteprise Strategy Group validated that IBM SP4C can help organizations restore data across SaaS-, IaaS- and PaaS-based applications. We observed how IBM SP4C recovered data for both Microsoft 365 and Microsoft Azure, specifically when data is accidentally deleted. Workflows were supported with “wizards” that simplified how data is located and restored.

Search for Data Using Incremental Backups

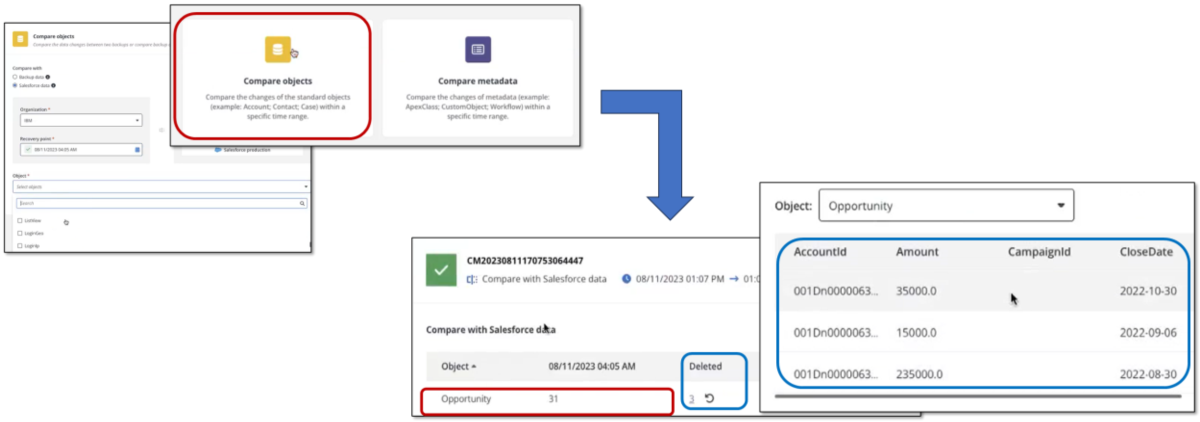
When restoring data, it is important to easily locate the data to be restored so that ongoing business operations are minimally disrupted. Organizations can leverage IBM SP4C’s incremental backups to locate data by comparing changes in data between backups or to actual production data.

Enterprise Strategy Group Testing

Enterprise Strategy Group validated how IBM SP4C enables organizations to backup and restore data by examining the capability within Salesforce. This capability is required, as Salesforce end-user agreements have explicitly stated that customers should perform regular backups of all data, as well as manual point-in backups for any data project.

We began by navigating to the **Compare** functionality of IBM SP4C Salesforce. We saw that IBM SP4C can either compare changes made in objects or metadata. In this case, we searched for accidentally deleted data associated with the object named "Opportunity." After choosing the **Compare Objects** option, we set the parameters to locate our data (see Figure 9) by comparing the latest backup to Salesforce production data. IBM SP4C located the "Opportunity" object and noted that three specific items were deleted.

Figure 9. Comparing Objects Within a Specific Backup to Salesforce Production Data



Compare objects
Compare the data changes between two backups or compare backup

Compare with
○ Backup data
● Salesforce data

Organization *: IBM
Recovery point *: 08/11/2023 04:05 AM
Salesforce production

Object *: Select objects
Search
□ ListView
□ LoginGeo
□ LoginIp

Compare objects
Compare the changes of the standard objects (example: Account; Contact; Case) within a specific time range.

Compare metadata
Compare the changes of metadata (example: ApexClass; CustomObject; Workflow) within a specific time range.

CM20230811170753064447
Compare with Salesforce data   08/11/2023 01:07 PM → 01:0

Compare with Salesforce data

Object	08/11/2023 04:05 AM	Deleted
Opportunity	31	3

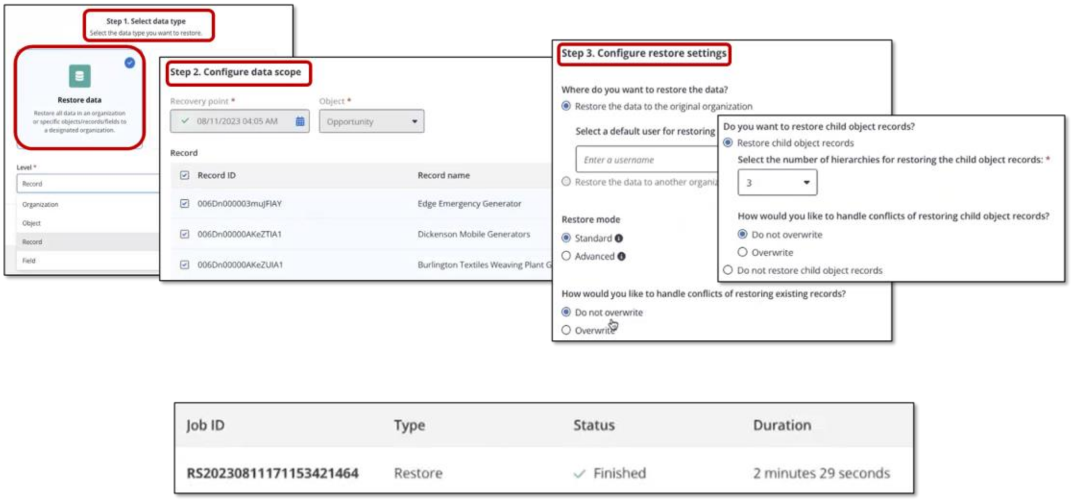
Object: Opportunity

AccountId	Amount	CampaignId	CloseDate
001Dn0000063...	35000.0		2022-10-30
001Dn0000063...	15000.0		2022-09-06
001Dn0000063...	235000.0		2022-08-30

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

To restore those three items, we selected them and clicked on **Restore**. Using a wizard (see Figure 10), we chose the data type (object) and clicked on the **Restore Data** panel. We proceeded to define the scope to be restored (all three items) and recovery criteria, such as where to place the restored data, whether any parent-child relationships were to be maintained, and how to manage data conflicts. Once submitting the request, we observed that IBM SP4C took less than three minutes to complete.

Figure 10. Restoring Accidently Deleted Salesforce Data



Step 1. Select data type
Select the data type you want to restore.

Restore data
Restore all data in an organization or specific objects/records/fields to a designated organization.

Level *: Record
Organization
Object
Record
Field

Step 2. Configure data scope

Recovery point *: 08/11/2023 04:05 AM
Object *: Opportunity

Record

☑	Record ID	Record name
☑	006Dn000003muJFIAY	Edge Emergency Generator
☑	006Dn00000AKeZTIA1	Dickenson Mobile Generators
☑	006Dn00000AKeZUIA1	Burlington Textiles Weaving Plant G

Step 3. Configure restore settings

Where do you want to restore the data?
● Restore the data to the original organization
Select a default user for restoring
Enter a username
○ Restore the data to another organi

Restore mode
● Standard
○ Advanced

How would you like to handle conflicts of restoring existing records?
● Do not overwrite
○ Overwrite

Do you want to restore child object records?
● Restore child object records
Select the number of hierarchies for restoring the child object records: *
3
How would you like to handle conflicts of restoring child object records?
● Do not overwrite
○ Overwrite
○ Do not restore child object records

Job ID	Type	Status	Duration
RS20230811171153421464	Restore	✓ Finished	2 minutes 29 seconds

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

Enterprise Research Group (ESG) research uncovered that only 26% of organizations have been able to recover 100% of Salesforce data, despite the stringent objectives typically placed on RTOs and RPOs.[9] Correctly identifying the scope and type of data to be restored must be addressed to improve overall recoverability.

ESG validated that IBM SP4C enables organizations to locate and identify the exact data to be restored by leveraging the incremental backups. We considered the case in which data was accidentally deleted and located by comparing backups with Salesforce production data. Data location and recovery occurred within minutes. Since RPO was minimized, normal business operations continued with minimal interruption.

Conclusion

CSPs have made it clear that customers are responsible for protecting against any loss of data they store in their public clouds. With the continuing adoption of public cloud services, organizations are acutely aware of the costs of not fulfilling this responsibility. Not protecting against data loss carries great risk, disrupting normal business operations and leaking data to unauthorized users and bad actors, which can lead to lost revenue and lost customer goodwill. The risk of ransomware payouts is also growing as prominent brands have experienced high-profile security breaches.

IBM SP4C has been designed to simplify how organizations back up and recover data for SaaS-, PaaS-, and IaaS-based applications, specifically Microsoft 365, Microsoft Azure, Microsoft Dynamics 365, and Salesforce. With IBM SP4C, organizations can improve RTOs and RPOs, not only by making backup and recovery tasks easier to complete, but also by assigning data recovery responsibilities to end users of the applications. Centralized IT organizations no longer need to complete all recovery operations. IBM SP4C also helps to close security gaps, as organizations can locate potential threats and breaches when comparing the “forever” incremental backups.

Enterprise Strategy Group (ESG) validated that IBM SP4C can:

- Protect data against breaches and ransomware by simplifying how to track changes in data between incremental backups, using visualizations or alerts against rules.
- Delegate data recovery rights to end users of select applications instead of submitting requests to a central IT team responsible for troubleshooting all IT issues, thus reducing time to recovery.
- Streamline data restoration workflows so that RTOs and RPOs improve.
- Further improve RTOs and RPOs by reducing the time and effort involved in searching for the data to be restored among the incremental backups.

Fulfilling the shared responsibility model when using any public cloud service is imperative when it comes to protecting data against loss. Not doing so has real business consequences. If your organization is looking for a data backup and recovery solution for your critical cloud-native applications, ESG recommends looking closely at IBM SP4C.

[9] Source: Enterprise Strategy Group Complete Survey Results, *SaaS Data Protection: A Work in Progress*, November 2022.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

About Enterprise Strategy Group
TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

✉ contact@esg-global.com
🖥 www.esg-global.com