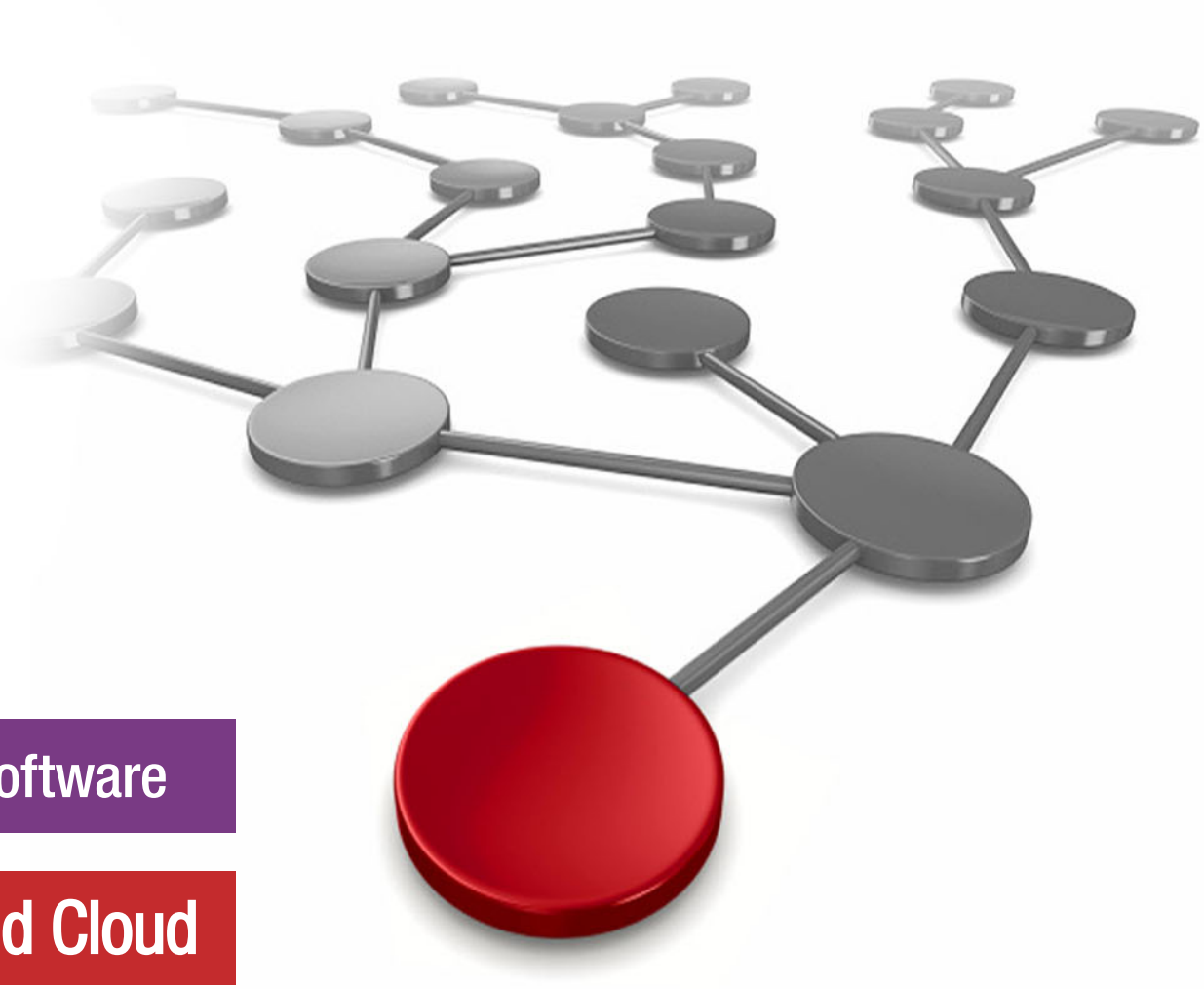
Draft Document for Review August 11, 2025 2:54 pm REDP-5759-00

Redbooks
ibm.com/redbooks

IBM Storage Protect for Cloud: Safeguarding Critical SaaS Environments

Meghan Grable
Robert Deselle
Phillip Gerrard
Del Hoobler
Daniel Michel



Systems Software

Hybrid Cloud

IBM

Redpaper

IBM Redbooks

SP4C: Safeguarding Critical SaaS Environments

August 2025

Note: Before using this information and the product it supports, read the information in “Notices” on page v.

First Edition (August 2025)

This document was created or updated on August 11, 2025.

Contents

Notices

This information was developed for products and services offered in the US. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:
IBM Director of Licensing, IBM Corporation, North Castle Drive, MD-NC119, Armonk, NY 10504-1785, US

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Trademarks

IBM, the IBM logo, and ibm.com are trademarks or registered trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the web at “Copyright and trademark information” at https://www.ibm.com/legal/copytrade.shtml

The following terms are trademarks or registered trademarks of International Business Machines Corporation, and might also be trademarks or registered trademarks in other countries.

Redbooks (logo) ®	IBM Cloud®	Redbooks®
IBM®	QRadar®	

The following terms are trademarks of other companies:

Microsoft, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Other company, product, or service names may be trademarks or service marks of others.

Preface

IBM® Storage Protect for Cloud is an offering from IBM that delivers protection for your Software as a Service (SaaS) applications to give you peace of mind knowing that your SaaS data is protected. This IBM Redpaper publication will help you better understand its capabilities as well as install and configure the software to protect and monitor your backups.

Is your cloud data protected? Probably not as well as you think. While many organizations are confident they have the right protections in place, and that their Cloud Service Providers (CSPs) have them covered, chances are that this is not the case.

The explosive growth of ransomware and other cyberthreats is forcing IT professionals to reevaluate their data protection and disaster recovery strategies. To gain on-the-ground insights, Ponemon Institute researchers interviewed thousands of security and C-suite business leaders with firsthand knowledge of the data breach incidents at their organizations. That research revealed some startling numbers. In 2025, the average cost of a data breach is $4.44 million. Even though that is a slight drop from the 2024 average, that’s still a staggering number with a huge impact to all businesses. For the second year in a row, malicious insider attacks resulted in the highest average breach costs among initial threat vectors at $4.92 million. And, third-party vendor and supply chain compromise followed closely at $4.91 million.

For workloads running on CSP platforms, the risks are even greater. There is a huge worldwide effort, on the part of bad actors, to attack organizations doing business in the cloud and using CSPs to run their workloads. Software-as-a-service (SaaS) workloads such as Microsoft 365 (M365), Dynamics 365 (D365), Salesforce, Microsoft Azure (Azure), and Google Workspace, are of particular concern. This software has become an essential collaboration and management tool, especially now that so many people and teams are working remotely. The prevalence of these and other SaaS applications will rise as companies of all sizes try to gain competitive advantage by leveraging digital tools to work faster and smarter.

Thus, protecting business-critical apps and strengthening data resiliency is imperative. All these solutions generate business-critical data, and that data must be protected. But other than very limited built-in protections, CSPs leave most of the critical backup tasks up to their customers, and often, organizations don't realize this until it is too late.

Don’t be the next statistic. Ensure your SaaS data is adequately protected with IBM Storage Protect for Cloud.

Authors

This paper was produced by a team of IBM specialists from around the world.

Meghan Grable is a Global Growth Product Manager with over six years of experience in strategizing and scaling data protection solutions across SaaS and hybrid software environments. She focuses on driving Product-Led Growth (PLG) initiatives by leveraging data-driven development, user insights, and iterative experimentation. She has led cross-functional engineering, UX, and go-to-market teams to deliver resilient, compliance-ready solutions that address complex threats - including ransomware, malware, and operational errors. Meghan holds a degree in Service Design from the Savannah College of Art and Design and leverages her background in enterprise design thinking to design scalable, secure, and user-centric products. Her work bridges technical depth with strategic growth, enabling organizations to enhance cyber resilience while accelerating user adoption and retention through product experience.

Robert Deselle has dedicated the past 26 years to IBM and is currently a member of the IBM Storage Protect for Cloud Site Reliability Engineering (SRE) team. With 24 years of experience in customer service—specializing in IBM Storage Protect, IBM Storage Protect for Virtual Environments, and IBM Storage Protect Plus—Robert DeSelle has spent 20 of those years serving as a team lead for these products. His expertise spans DevOps, SRE practices within IBM Storage Protect for Cloud, and Microsoft Azure.

Phillip Gerrard is a Project Leader and Technical Content Specialist for the International Technical Support Organization working out of Beaverton, Oregon. As part of IBM for over 17 years he has authored and contributed to hundreds of technical documents published to IBM.com and worked directly with IBM's largest customers to resolve critical situations. As a team lead and Subject Matter Expert for the ADSM/TSM/IBM Storage Protect support team, he is experienced in leading and growing international teams of talented IBMers, developing and implementing team processes, creating and delivering education. Phillip holds a degree in computer science and business administration from Oregon State University.

Del Hoobler is a Principal Storage Software Specialist with more than 25 years of experience in the data resilience field. He designs and architects cyber resilience solutions for enterprise customers across all industries.

Daniel Michel is the lead of the Storage Protect for Cloud site reliability engineering (SRE) team. He is located in Frankfurt, Germany and he has 17 years of experience with IBM in various roles including Storage Engineer, Scrum Master, DevOps and SRE lead. He holds a degree in Computer Science from the University of Applied Sciences in Coburg, Germany. His areas of expertise include full stack software development, DevOps, and SRE in IBM Cloud® and Microsoft Azure.

Now you can become a published author, too!

Here’s an opportunity to spotlight your skills, grow your career, and become a published author—all at the same time! Join an IBM Redbooks® residency project and help write a book in your area of expertise, while honing your experience using leading-edge technologies. Your efforts will help to increase product acceptance and customer satisfaction, as you expand your network of technical contacts and relationships. Residencies run from two to six weeks in length, and you can participate either in person or as a remote resident working from your home base.

Find out more about the residency program, browse the residency index, and apply online at:

ibm.com/redbooks/residencies.html

Comments welcome

Your comments are important to us!

We want our papers to be as helpful as possible. Send us your comments about this paper or other IBM Redbooks publications in one of the following ways:

- Use the online **Contact us** review Redbooks form found at:

  ibm.com/redbooks

- Send your comments in an email to:

  redbooks@us.ibm.com

- Mail your comments to:

  IBM Corporation, IBM Redbooks
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400

Stay connected to IBM Redbooks

- Find us on LinkedIn:

  https://www.linkedin.com/groups/2130806

- Explore new Redbooks publications, residencies, and workshops with the IBM Redbooks weekly newsletter:

  https://www.redbooks.ibm.com/subscribe

- Stay current on recent Redbooks publications with RSS Feeds:

  https://www.redbooks.ibm.com/rss.html

1

Introduction

This chapter provides and introduction to IBM Storage Protect for Cloud (SP4C) as well as outlining key features and principles that the product is built on.

In this chapter:

1.1 Introduction to IBM Storage Protect for Cloud

The explosive growth of ransomware and other sophisticated cyber threats is compelling IT professionals across industries to fundamentally reevaluate their data protection and disaster recovery strategies. The damage they inflict continues to grow as the global average cost of a data breach hit $4.44 million in 2025 (2025 Cost of a Data Breach Report). Among the most pressing concerns are software-as-a-service (SaaS) workloads, particularly Microsoft 365, which has become a cornerstone for communication, collaboration, and productivity in modern enterprises. As remote and hybrid work models become the norm, reliance on cloud-based platforms like Microsoft 365 has surged, making them prime targets for cyber criminals.

While these platforms offer significant operational benefits, many organizations mistakenly assume that data residing in SaaS environments is automatically protected. In reality, Cloud Service Providers (CSPs) like Microsoft, follow a shared responsibility model, which means that while they ensure the infrastructure's uptime and security, the responsibility for backing up and retaining critical business data still falls on the organization who owns the data. The risk of accidental deletions, malicious insider actions, or ransomware attacks further underscores the need to have robust third-party backup and recovery solutions in place to ensure data resiliency.

As digital transformation accelerates, the adoption of SaaS tools is expected to grow even more rapidly. Businesses of all sizes are embracing these tools to increase agility, reduce costs, and drive innovation. However, to truly leverage the benefits of SaaS platforms while mitigating risk, IT leaders must prioritize resilient data protection strategies that extend beyond traditional perimeters and address the unique challenges of cloud-native environments.

IBM Storage Protect for Cloud is an enterprise-grade solution designed to meet this demand by delivering reliable backups, fast recovery, and proactive threat detection across today's most critical cloud workloads. Combining robust security features, centralized management, and flexible deployment options, IBM Storage Protect for Cloud empowers IT teams to safeguard their data against ransomware, accidental loss, and compliance risks - ensuring business continuity in a rapidly evolving digital environment.

1.2 IBM Storage Protect for Cloud Key Highlights

By integrating IBM Storage Protect for Cloud into your data protection strategy, your organization can achieve a higher level of resilience against the ever-evolving landscape of cyber threats, ensuring business continuity and data integrity across all your SaaS platforms. SP4C provides the following features related to cloud-based workloads:

Comprehensive Protection for SaaS, IaaS, and PaaS Workloads

IBM Storage Protect for Cloud offers a robust backup and recovery solution tailored for various SaaS applications, including Microsoft 365, Power Platform, Azure, Entra ID, Google Workspace, Salesforce, and Dynamics 365. By providing full and incremental backups, along with granular restoration capabilities, it ensures that your organization's critical data remains secure and recoverable, even in the face of threats like ransomware or accidental deletions.

Proactive Threat Detection and Recovery

Beyond just backup and recovery, IBM Storage Protect for Cloud includes features for proactive threat detection. It can analyze unusual activities within your environment, providing

alerts for potential ransomware attacks or other anomalies. This early warning system enables organizations to respond swiftly to threats, minimizing potential damage and downtime.

Advanced Security and Compliance Features

Security is paramount in today's digital landscape. IBM Storage Protect for Cloud incorporates advanced security measures such as encryption of data both in transit and at rest, role-based access controls (RBAC), and the option to use your own encryption keys. These capabilities protect sensitive data from unauthorized access while supporting compliance with industry regulations. Additionally, the solution can be configured to send logs and audit data to leading security information and event management (SIEM) platforms such as Splunk and QRadar®. This integration enables organizations to centralize security monitoring, detect anomalies faster, and respond to threats more effectively as part of a broader cybersecurity strategy.

Centralized Management and Reporting

Managing backups across multiple platforms can be complex. IBM Storage Protect for Cloud simplifies this with a centralized management console that provides comprehensive tracking, management, and reporting of backup data and restore processes. This unified approach allows IT administrators to efficiently oversee data protection activities across the organization.

Flexible Deployment Options

Understanding that organizations have diverse infrastructure needs, IBM Storage Protect for Cloud offers flexible deployment options. Whether you prefer to store backups in IBM's Microsoft Azure environment, your own cloud infrastructure, or even on SFTP/FTP servers, the solution adapts to your specific requirements, ensuring seamless integration into your existing systems.

2

IBM Storage Protect for Cloud Features and Supported Workloads

In this chapter we describe and provide a more detailed look at the features of the IBM Storage for Cloud offering. This includes an overview of the SaaS offering, details on the supported workloads that can be protected and the notable features and advantages SP4C offers when used to protect these cloud based workloads.

In this chapter:

2.1 IBM Storage Protect for Cloud Overview

IBM Storage Protect for Cloud is a fully managed, SaaS-based backup and recovery platform designed to safeguard enterprise data across popular cloud-native workloads including Azure, Microsoft 365, Dynamics 365, Salesforce, and Google Workspace. As a true SaaS solution, it requires no deployment or patching and provides centralized managed dashboard, enabling businesses mitigate risk against cyber attacks, accidental deletion, and avoid compliance related fines.

At its core, this solution enables backups up to four times daily, with granular restore capabilities that allow recovery based on filters such as content type, owner, creation date, and even file size. Item-level restores are supported across services such as emails, Teams chat, SharePoint files, Power BI datasets, Salesforce records, Azure VMs, and more, providing target-specific recovery without full-environment rollbacks.

Security and compliance are built into the platform: backup operations are encrypted, role-based access ensures proper governance, multi-factor authentication is supported, and audit logs provide comprehensive visibility into all administrative and user actions. It also includes unusual activity detection and alerts, which help identify ransomware or malicious behavior within backups and enable rapid response.

In summary, IBM Storage Protect for Cloud offers enterprises a modern, scalable, and secure backup platform that simplifies data protection, improves recovery time, and strengthens compliance posture without the burden of managing infrastructure.

2.2 IBM Storage Protect for Cloud Supported workloads

2.2.1 Azure

IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID delivers comprehensive, cloud-based data protection for critical Azure workloads, including Microsoft Entra ID (formerly Azure Active Directory), Azure Virtual Machines, Azure Blob, File, and Object Storage, as well as Azure SQL databases, Azure DevOps repositories, and Azure AD B2C tenants. IBM Storage Protect for Cloud enables organizations to schedule frequent, encrypted backups—up to four times a day—to safeguard sensitive business data against a wide range of risks, such as cyberattacks (including ransomware), hardware failures, accidental deletion, or natural disasters. Backups are transmitted and stored using industry-standard encryption protocols, ensuring data privacy and regulatory compliance. With support for both full and incremental backups, IT administrators can optimize storage utilization and reduce network bandwidth consumption. Automated backup policies, real-time monitoring, and granular restore options empower IT teams to quickly recover specific objects (such as an individual VM, Entra ID user, or SQL table) or entire workloads, minimizing application downtime and ensuring business continuity. The robust audit trails and role-based access controls further enhance security and governance.

A key capability of IBM Storage Protect for Cloud Azure is its support for granular restore operations. Administrators and authorized end users can recover specific objects, files, folders, or even metadata, instead of restoring entire workloads, significantly reducing downtime and operational impact. Additionally, for Microsoft Entra groups and blobs that have been deleted beyond standard retention periods, granular recovery is available–for example, administrators can restore a deleted group and its memberships, or recover specific blobs or

directories from any backup point, including merge or overwrite options for flexible, targeted data restoration.

IBM Storage Protect for Cloud Azure also features a robust calendar restore function, often referred to as “Calendar View Recovery”, which allows users or administrators to easily pinpoint and browse recovery points by date. This capability streamlines the process of locating the exact moment for restoration after data loss events such as accidental deletion, corruption, or ransomware attacks. Together with anomaly detection and self-service recovery options, these features provide organizations with granular, efficient, and secure mechanisms to ensure their Azure ecosystem remains resilient and compliant in the face of diverse threats.

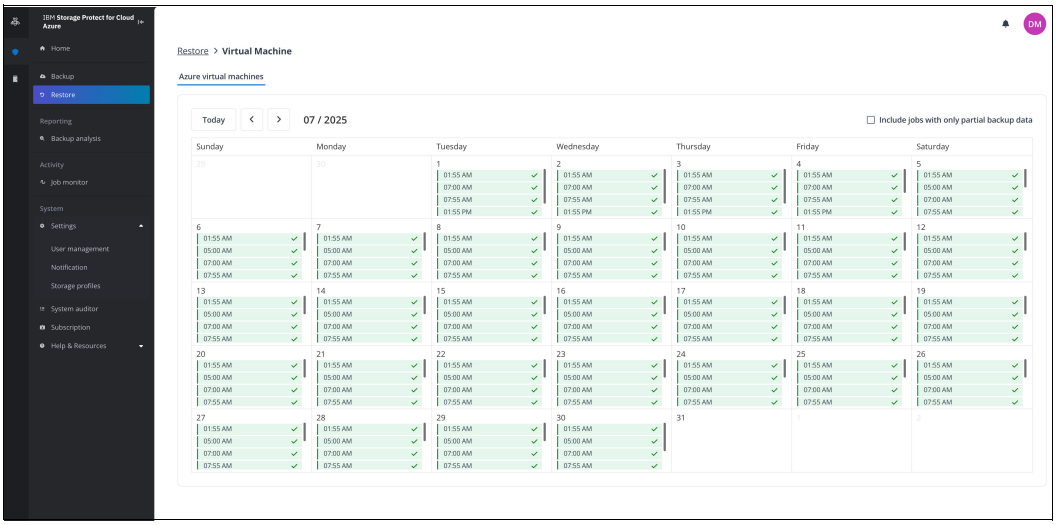


Figure 2-1 SP4C Azure Restore ‘Calendar View Recovery’ panel

By centralizing management and automating compliance reporting, IBM Storage Protect for Cloud Azure VMs, Storage, and Entra ID helps organizations efficiently protect, manage, and recover their Azure-based data assets. The unified administration console simplifies configuration, monitoring, and reporting across all protected Azure resources, while built-in compliance features streamline regulatory reporting for mandates such as GDPR and HIPAA. Integration with native Azure APIs ensures seamless operation with minimal disruption to existing cloud workflows. Advanced analytics and alerting capabilities enable proactive identification of backup failures or policy deviations, allowing rapid remediation. This end-to-end solution reduces the operational burden on IT staff, lowers total cost of ownership, and provides assurance that critical cloud data is always protected and recoverable.

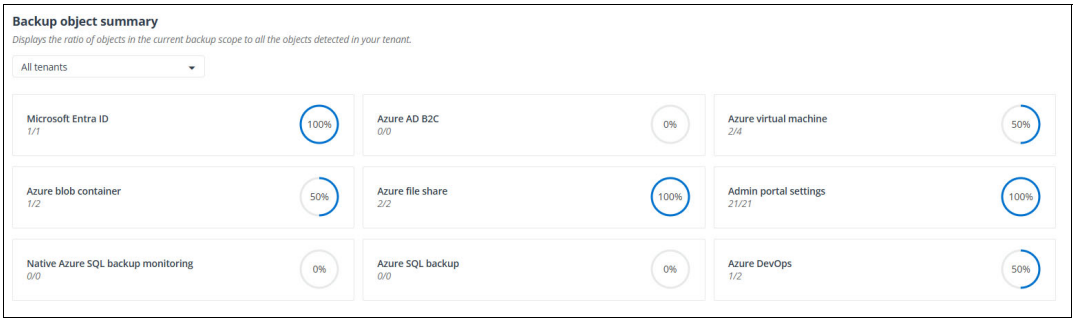


Figure 2-2 SP4C Azure backup object dashboard

2.2.2 Microsoft 365

IBM Storage Protect for Cloud Microsoft 365 is a Software-as-a-Service (SaaS) solution designed to provide comprehensive backup and recovery for Microsoft 365 data, including Exchange Online, OneDrive, SharePoint Online, Microsoft 365 Groups, Teams, Microsoft Teams Chat, Project Online, Public Folders, Viva Engage, Power BI, Power Automate, and Power Apps. The service allows clients to back up their Microsoft 365 data either IBM's provided unlimited Azure storage, or to their own storage environment. With the evolving nature of ransomware and cyber attacks, IBM Storage for Cloud helps organizations address the limitations of the Microsoft 365 shared responsibility model by enabling automated, policy driven backups up to four times daily, granular search and restore capabilities, and robust encryption for both in transit and at rest. This includes the ability to bring your own encryption key (BYOK) giving the client more control. In addition, IBM Storage Protect for Cloud continuously monitors for unusual activities and provides customized alerts to system administrators. Once alerted, system administrators can utilize smart assist restore capabilities to ensure the recovered data is clean and not affected by the original attack.

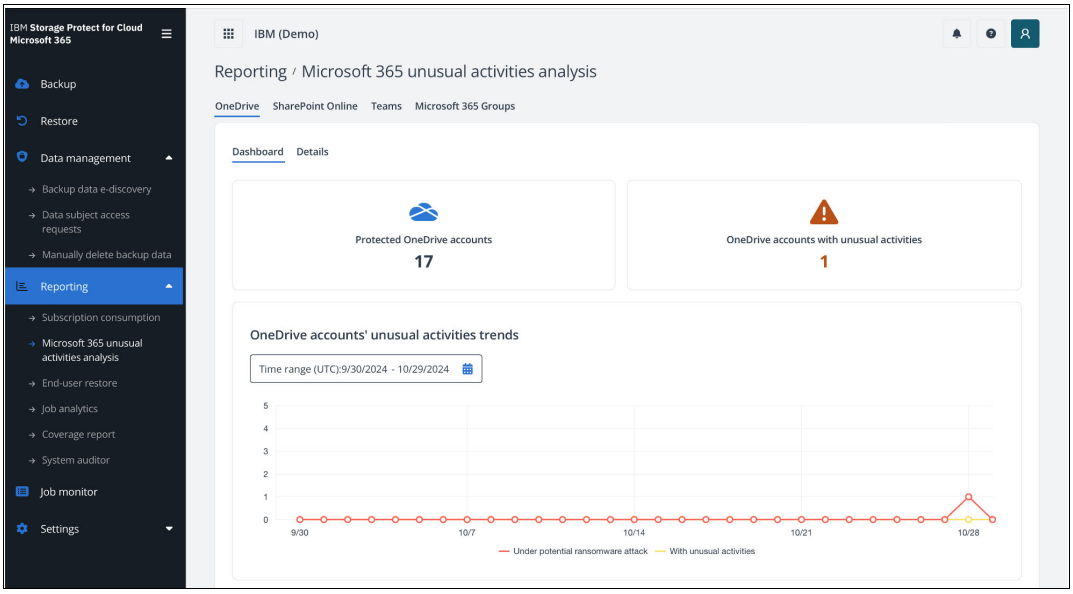


Figure 2-3 SP4C M365 unusual activities reporting panel

The platform features a centralized, web-based management console hosted in IBM's Azure environment, allowing administrators to monitor backup jobs, configure retention policies, and generate details reports. Self-service and delegated administration features allow end users and administrators to recover lost of corrupted files quickly, minimizing downtime. The solution also supports advanced security features such as role-based access control (RBAC) and multi-factor authentication (MFA). This ensures only authorized personnel can access sensitive backup data.

IBM Storage Protect for Cloud Microsoft 365 empowers end users to recover their own data through the IBM Storage Protect for Cloud Recovery Portal. This service offers a dependable and user-friendly solution for restoring data, delivering robust protection for Microsoft 365 environments.

With IBM Storage Protect for Cloud Microsoft 365 early ransomware detection, you know you are protected with early detection of potential suspicious behavior. Using the provided reporting capabilities, IT Admin can be assured they are notified when any problems arise.

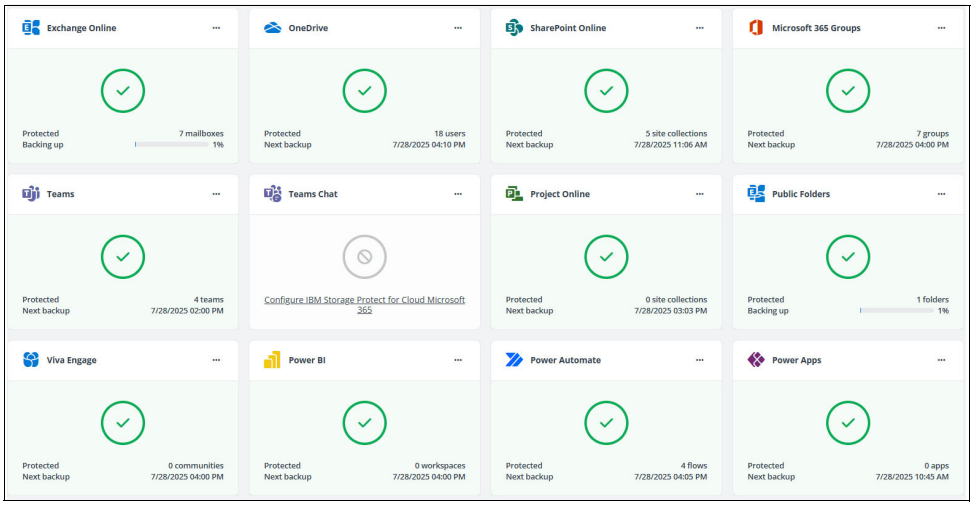


Figure 2-4 SP4C M365 dashboard

2.2.3 Dynamics 365

Microsoft Dynamics 365 is a suite of intelligent business applications that combines CRM (Customer Relationship Management) and ERP (Enterprise Resource Planning) capabilities. It ultimately unifies business processes through the cloud, AI, and data-driven insights. In an enterprise setting, Dynamics 365 is used to streamline operations across sales, finance, customer service, supply chain, marketing, and more — helping organizations improve productivity and decision-making.

Under the shared responsibility model, Microsoft manages the security of the cloud infrastructure (physical hosts, network, and data centers), while the customer is responsible for securing their data, users, access permissions, and compliance configurations within Dynamics 365. This means enterprises must actively manage backups, user authentication, and data governance to ensure full protection and compliance.

IBM's Storage Protect for Cloud provides a robust SaaS backup solution for Dynamics 365 CRM by offering frequent, encrypted, and granular backups with flexible storage options (unlimited IBM-hosted or BYOS). Enterprises create their backup scopes, schedules, and policies to meet regulations and internal RTO and RPO standards.

Restore granularity in IBM Storage Protect for Cloud for Dynamics 365 is a key feature that empowers administrators and end users to recover exactly what they need. You can restore specific tables (entities), individual records, or even down to the field level within a record. This precision helps reduce downtime and preserves data integrity. The compare method allows you to compare two recovery points in the same backup cycle to find the data that may have been lost or have unexpected changes in the comparison results and recover the records in time. With this level of granularity and control, organizations can confidently meet both operational recovery needs and compliance requirements.

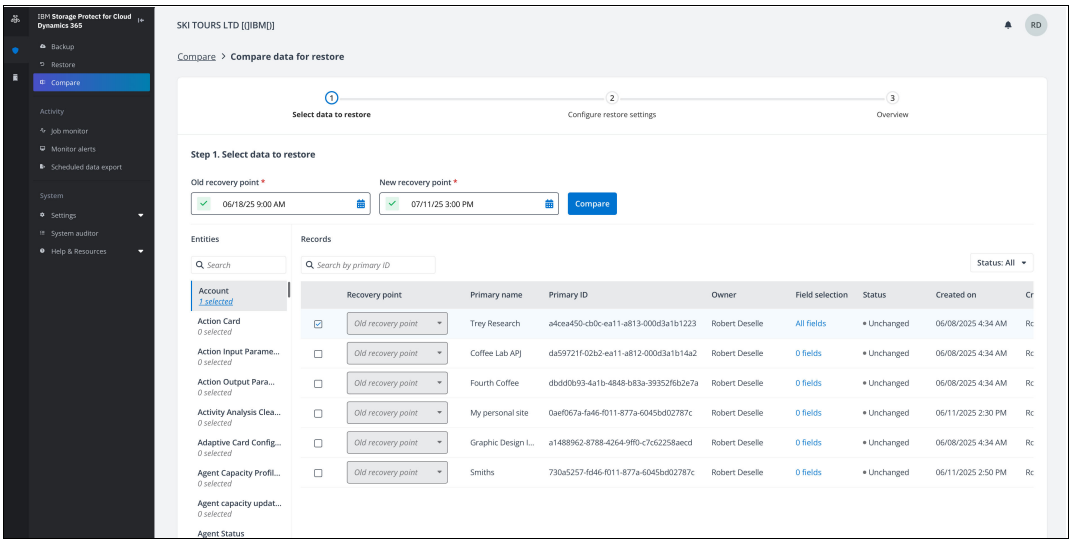


Figure 2-5 SP4C Dynamics 365 Compare Data for Restore panel

IBM Storage Protect for Cloud delivers powerful, enterprise-grade backup and recovery for Microsoft Dynamics 365, ensuring your critical customer and operational data is always protected. With support for automated, encrypted backups and flexible storage options, including unlimited IBM-hosted or bring-your-own storage, you stay in control of your data. Granular restore capabilities let you recover exactly what you need, from entities down to individual fields, cutting downtime and avoiding unnecessary data loss. Enterprises retain full control over access, compliance, and recovery workflows to fulfill their data protection requirements stemming from the shared responsibility model.

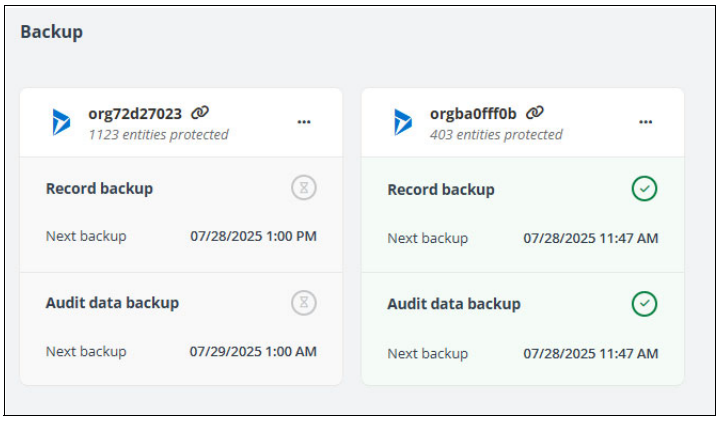


Figure 2-6 SP4C Dynamics 365 backup information tile

2.2.4 Salesforce

Salesforce is a cloud-based customer relationship management (CRM) platform that offers a suite of applications for sales, service, marketing, commerce, and analytics — all designed to help businesses manage customer relationships and drive growth. In an enterprise setting, Salesforce is widely used to centralize customer data, automate workflows, personalize customer engagement, and gain real-time insights across teams and business units.

Under the shared responsibility model, Salesforce ensures the security, availability, and performance of the underlying cloud infrastructure, including servers, databases, and core

application services. Meanwhile, customers are responsible for managing their data, user permissions, backup and recovery strategies, and compliance settings within the platform.

IBM Storage Protect for Cloud Salesforce delivers comprehensive backup and recovery of your Salesforce environment—including metadata, record data, and file attachments. These backups preserve relationships between objects and attachments to enable full fidelity restores. With granular restore options, you can selectively recover specific records, related attachments, or entire data hierarchies, all while filtering by owner, date, or other metadata for precise RPO tuning. Furthermore, before fully restoring, you can compare backup data and metadata to show the differences between objects or metadata in two different backups. Storage options include IBM-hosted Azure storage or customer-provided targets, with encryption at rest and in transit and support for bring your own key and role-based access controls. The solution also includes sandbox seeding capabilities, enabling teams to populate Salesforces sandboxes with real data for safe and effective development, testing, and training.

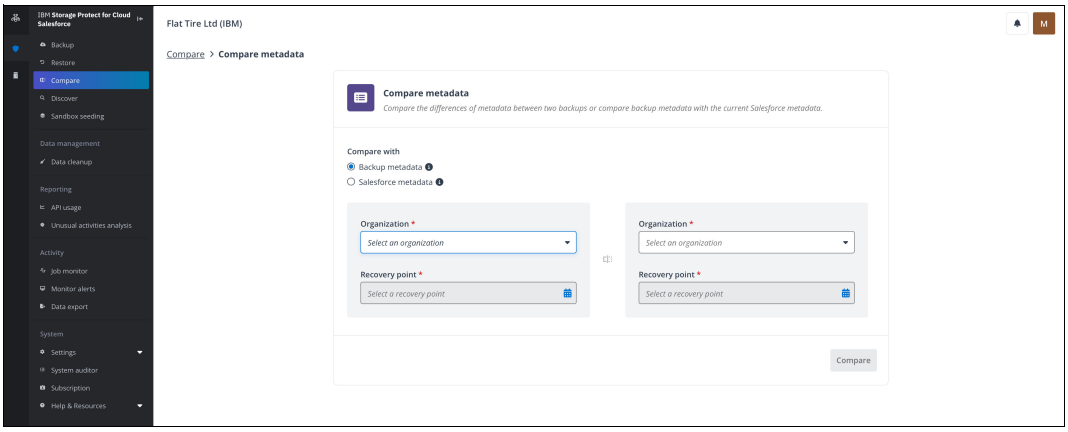


Figure 2-7 SP4C Salesforce Compare Metadata panel

IBM Storage Protect for Cloud offers comprehensive protection for Salesforce environments, backing up metadata, records, and attachments with full accuracy and integrity. It supports both IBM-hosted and bring-your-own storage options, with built-in encryption and role-based access controls for added security. Granular restore features allow businesses to recover exactly what they need–whether it's a single record, related files, or an entire object structure—quickly and efficiently.

2.2.5 Google Workspace

Google Workspace is a cloud-based productivity and collaboration platform developed by Google. It includes widely used tools like Gmail, Google Drive, Docs, Sheets, Slides, Calendar, Chat, and Meet, all integrated to support seamless communication and workflow across teams. In an enterprise setting, Google Workspace enables employees to collaborate in real time, share files securely, manage schedules, and streamline daily operations from virtually anywhere.

Under the shared responsibility model, Google is responsible for the security and availability of the underlying infrastructure, including data center operations, network security, and service reliability. Customers are accountable for managing user access, data classification, sharing permissions, and implementing proper backup and recovery strategies to protect their data within the platform.

IBM Storage Protect for Cloud provides comprehensive backup and recovery for Google Workspace, covering Gmail, Drive (including Shared Drives), Calendar, Contacts, Classroom, and Vault data. It offers flexible, item-level or account-level restore options through a user-friendly recovery portal, allowing for targeted data recovery based on search or calendar criteria. Backups are encrypted both in transit and at rest and can be stored on IBM-hosted Azure Blob storage or customer-provided storage. With role-based access controls and support for multi-region retention, the solution ensures data security and compliance.

IBM Storage Protect for Cloud is the ultimate solution for safeguarding your Google Workspace data with unmatched depth and flexibility. Its intuitive calendar-based restore feature lets users quickly pinpoint and recover data tied to specific dates, dramatically reducing downtime and simplifying recovery. Whether you choose IBM-hosted or bring-your-own storage, your backups are encrypted end-to-end and fully customizable to meet enterprise compliance needs. Purpose-built for reliability and control, Storage Protect for Cloud combines powerful automation, granular restore capabilities, and enterprise-grade security to deliver peace of mind and uninterrupted productivity in even the most demanding environments.

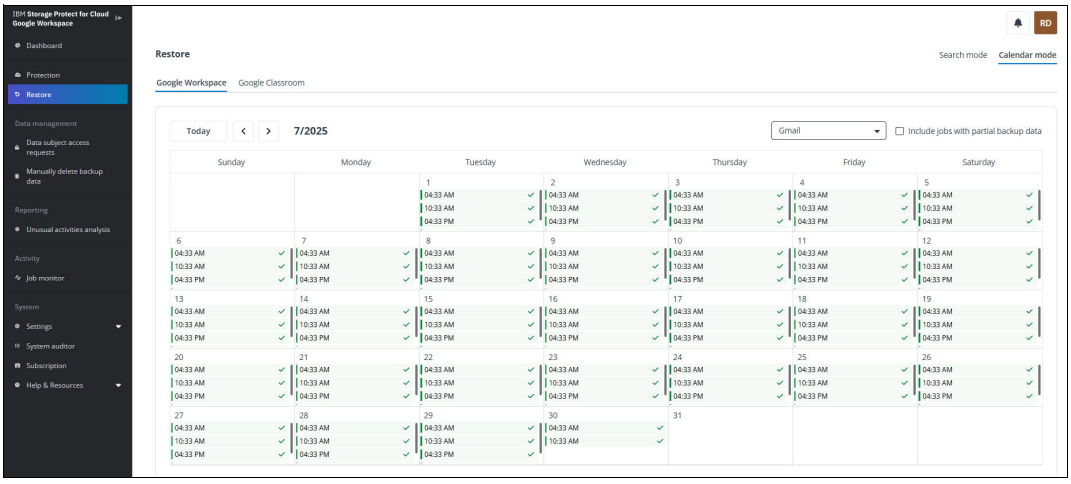


Figure 2-8 SP4C Google Workspace Restore 'Calendar View Recovery' panel

Whether you choose IBM-hosted or bring-your-own storage, your backups are encrypted end-to-end and fully customizable to meet enterprise compliance needs. Purpose-built for reliability and control, Storage Protect for Cloud combines powerful automation, granular restore capabilities, and enterprise-grade security to deliver peace of mind and uninterrupted productivity in even the most demanding environments.

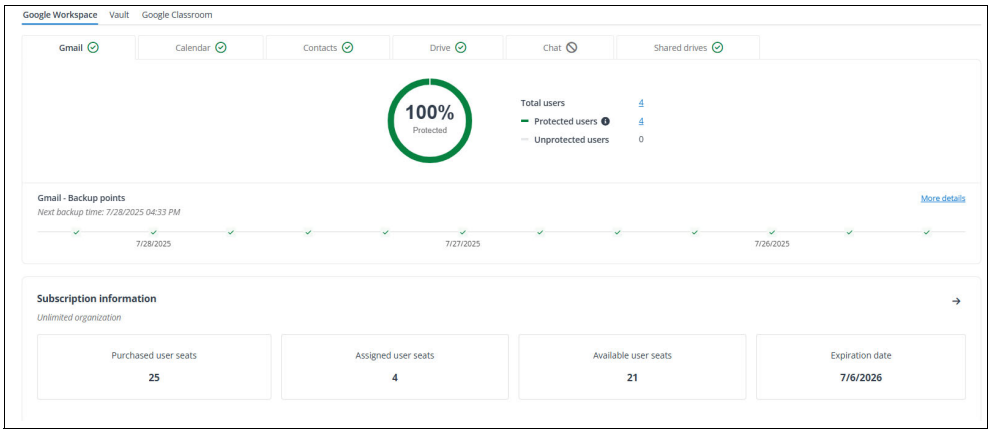


Figure 2-9 SP4C Google Workspace status panel

3

Integration Into SIEM Solutions

Security Information and Event Management (SIEM) are cybersecurity solutions that aggregate and analyzes log and event data from various sources within an organization's IT infrastructure. This centralized approach enables real-time monitoring, threat detection, incident response, and compliance reporting.

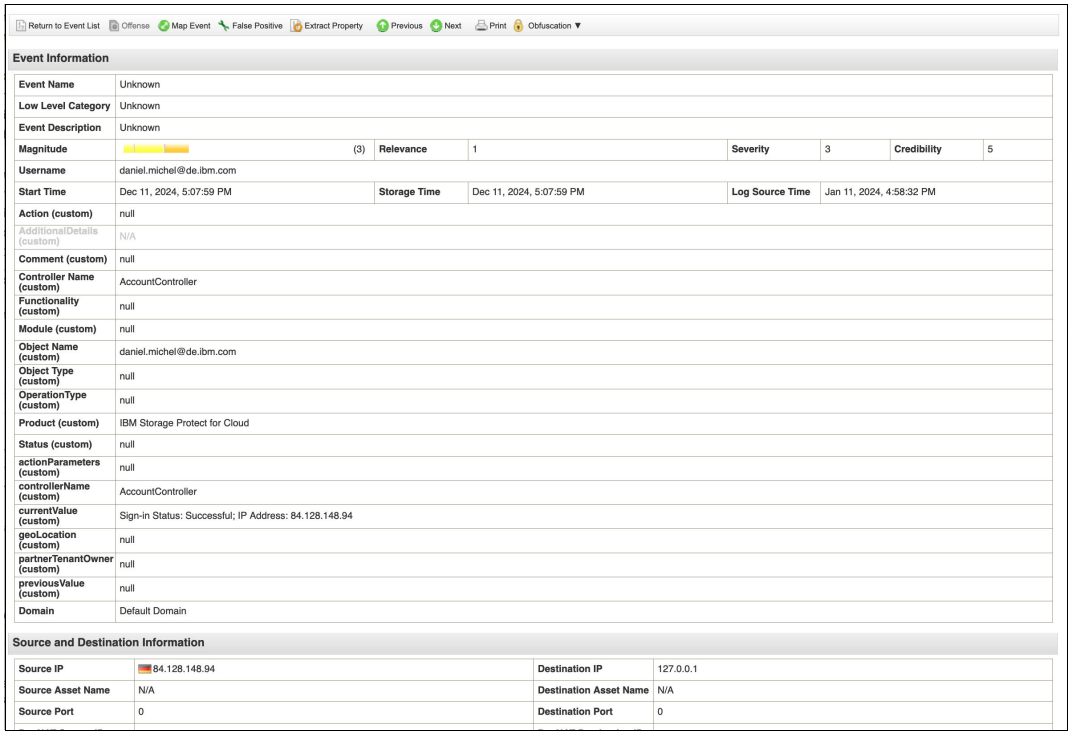
This chapter describes the following:

3.1 Introduction

As more customers are using SIEM solutions to monitor both on-premises products as well as Cloud service activities, integrating the IBM Storage Protect for Cloud platform with SIEM systems becomes crucial. This chapter describes the integration of IBM Storage Protect for Cloud with the two most widely used SIEM solutions: QRadar and Splunk.

3.2 Integration with QRadar

QRadar is a SIEM solution developed by IBM. It's designed to help organizations to detect, investigate, and respond to cybersecurity threats in real time. The following support page describes the required steps to integrate IBM Storage Protect for Cloud with QRadar by creating a Log Source and a Log Source Type:
https://www.ibm.com/support/pages/node/7178240


Return to Event List | Offense | Map Event | False Positive | Extract Property | Previous | Next | Print | Obfuscation ▼

Event Information

Event Name	Unknown						
Low Level Category	Unknown						
Event Description	Unknown						
Magnitude	(3)	Relevance	1	Severity	3	Credibility	5
Username	daniel.michel@de.ibm.com						
Start Time	Dec 11, 2024, 5:07:59 PM	Storage Time	Dec 11, 2024, 5:07:59 PM	Log Source Time	Jan 11, 2024, 4:58:32 PM		
Action (custom)	null						
AdditionalDetails (custom)	N/A						
Comment (custom)	null						
Controller Name (custom)	AccountController						
Functionality (custom)	null						
Module (custom)	null						
Object Name (custom)	daniel.michel@de.ibm.com						
Object Type (custom)	null						
OperationType (custom)	null						
Product (custom)	IBM Storage Protect for Cloud						
Status (custom)	null						
actionParameters (custom)	null						
controllerName (custom)	AccountController						
currentValue (custom)	Sign-in Status: Successful; IP Address: 84.128.148.94						
geoLocation (custom)	null						
partnerTenantOwner (custom)	null						
previousValue (custom)	null						
Domain	Default Domain						

Source and Destination Information

Source IP	84.128.148.94	Destination IP	127.0.0.1
Source Asset Name	N/A	Destination Asset Name	N/A
Source Port	0	Destination Port	0

Figure 3-1 Event information panel in QRadar

3.3 Integration with Splunk

Splunk is a powerful platform for searching, monitoring, and analyzing machine-generated data in real time. This support page describes the required steps to integrate IBM Storage Protect for Cloud with Splunk by building and configuring a custom Splunk add-on:
https://www.ibm.com/support/pages/node/7174823

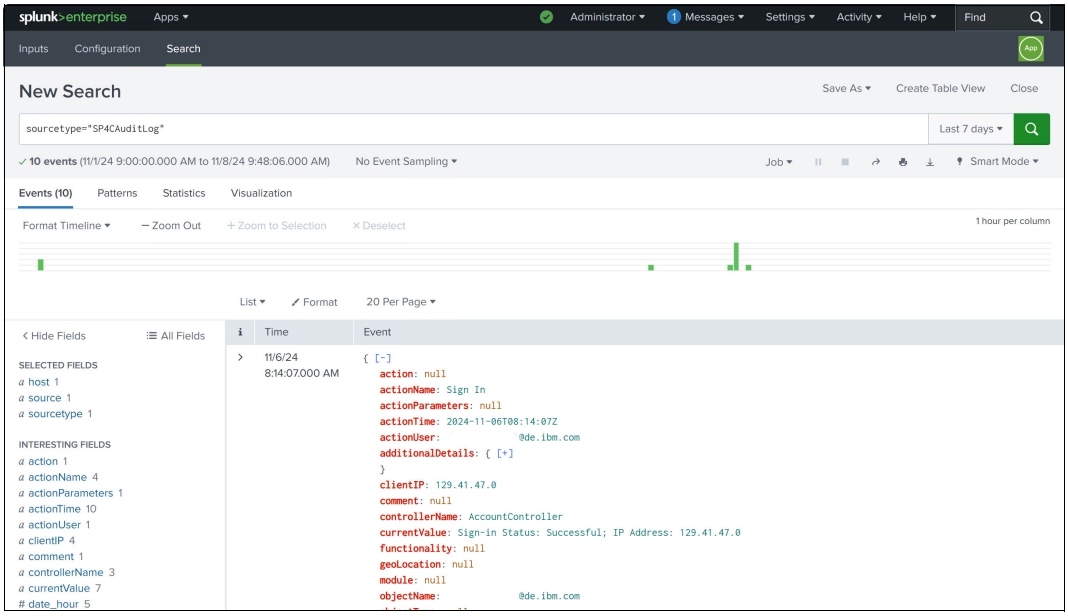


Figure 3-2 Audit events search in Splunk

3.4 Supported audit events

Admins of SIEM solutions like Splunk and QRadar need to know what security events or logs are being sent by IBM Storage Protect for Cloud so that they can create rules to ensure that all critical attack indicators are captured. The list of currently supported IBM Storage Protect for Cloud audit events for each workload can be downloaded at the following link: https://downloads.sp4c.storage-defender.ibm.com/SP4C_audit_events.xlsx

4

IBM Storage Protect for Cloud Partners

This chapter provides and overview and information about IBM Storage Protect for Cloud and how it is designed for the ease of use by Managed Service Providers (MSPs). This chapter highlights key features such as centralized management through the Partner Portal, role-based access control, comprehensive reporting and monitoring tools, standardized storage profiles, API integration, and built-in security measures. The solution enables MSPs to efficiently manage and protect customer data across various cloud platforms with scalability, automation, and flexibility.

In this chapter:

4.1 Overview

IBM Storage Protect for Cloud Partners is a multi-tenant, cloud-native data protection solution designed specifically for Managed Service Providers (MSPs). It enables partners to deliver secure, scalable, and automated backup and recovery services to their clients for a wide range of enterprise Cloud workloads such as Microsoft 365, Salesforce, Microsoft Dynamics 365, Google Workspace and various Microsoft Azure services.

It's built on the IBM Storage Protect for Cloud platform with added enhancements specifically for MSP use cases. IBM Storage Protect for Cloud Partners offers flexible billing models, tenant and administrative isolation, delegated administration and support for white-labeling. IBM Storage Protect for Cloud Partners comes with a centralized web-based UI, the Partner Portal.

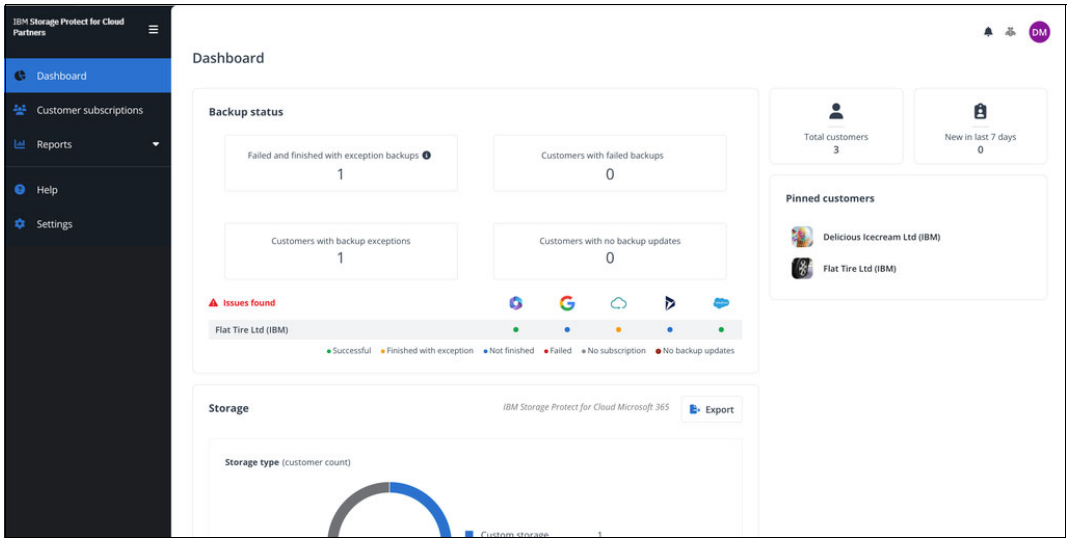


Figure 4-1 IBM Storage Protect for Cloud Partners dashboard

4.2 Key Features

4.2.1 Centralized management

In the Partner Portal, the Customer subscription page displays general account and service information. It's possible to sort, filter, and search for customers. MSPs can also perform administrative tasks for their customers. New customers can be invited to IBM Storage Protect for Cloud by clicking Onboard new customer.

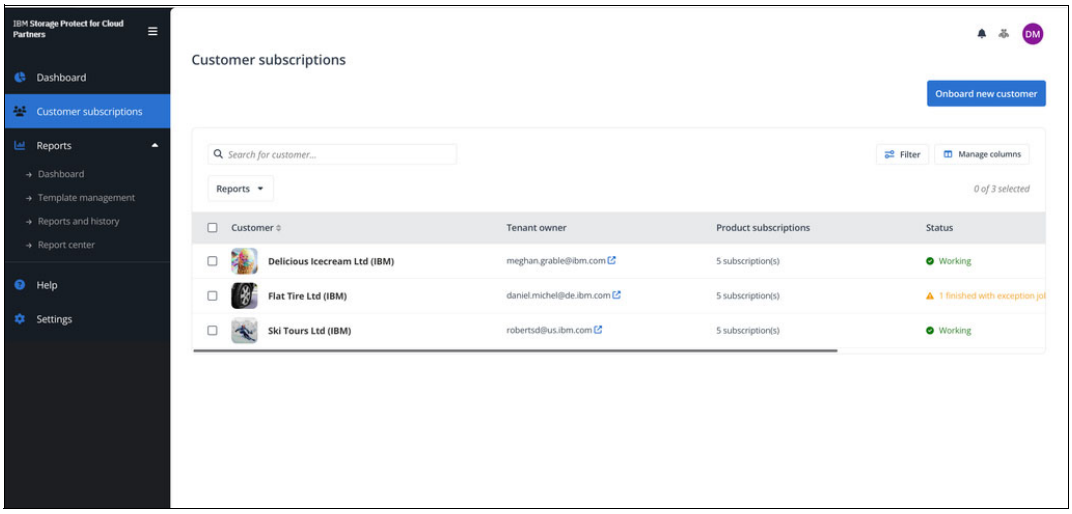


Figure 4-2 IBM Storage Protect for Cloud Partners Customer Subscriptions panel

Services can be added for an existing customer by selecting the customer and clicking Add service.

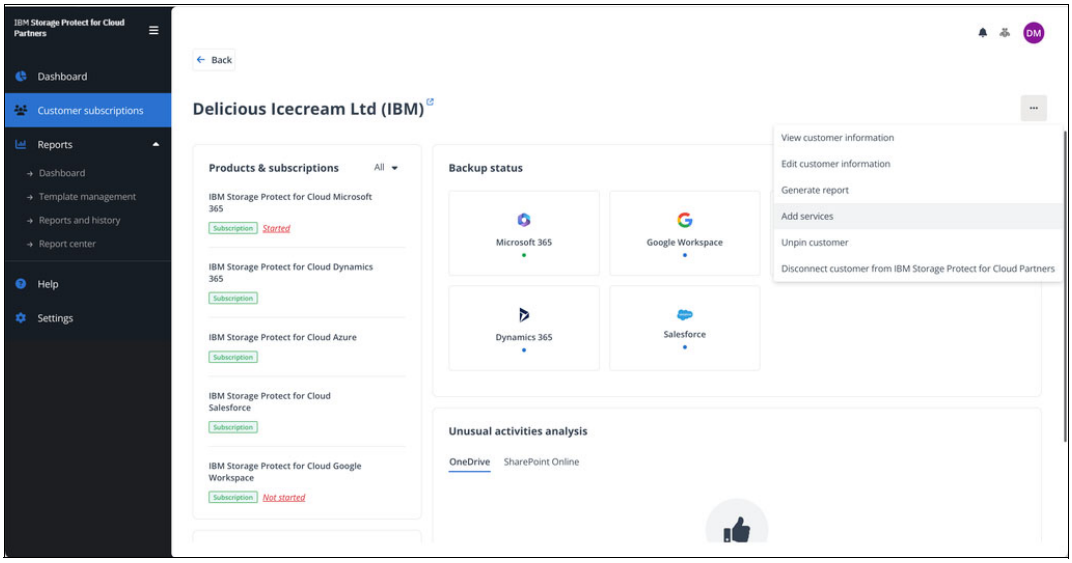


Figure 4-3 IBM Storage Protect for Cloud Partners Subscribed Customer details panel

Similarly, existing subscriptions can be modified by selecting the customer's subscription and clicking Edit subscription.

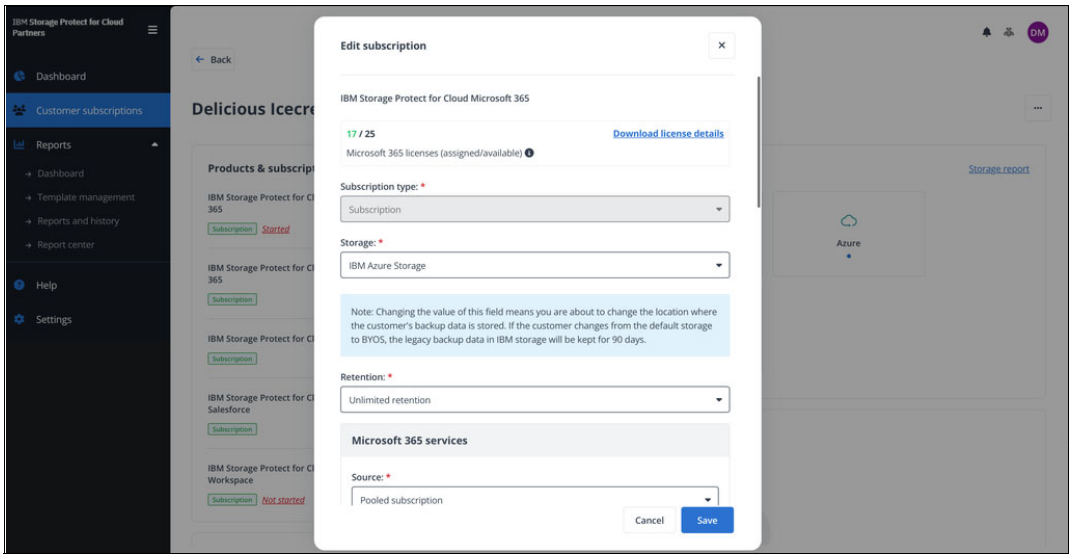


Figure 4-4 IBM Storage Protect for Cloud Partners Edit Subscriptions dialog

4.2.2 Role-Based Access

In the Partner Portal, MSPs have the flexibility to either create local user accounts or to configure a Partner App Profile for Microsoft 365 so that users and groups from Microsoft Entra ID can be added as IBM Storage Protect for Cloud Partners users for Single Sign-On (SSO) experience. With Role-Based Access Control (RBAC), MSPs have full control *who can do what* in the Partner Portal as well as in the managed customer's backup and recovery environments. Managed customers can be organized by using Customer Groups.

Figure 4-5 IBM Storage Protect for Cloud Partners Customer groups panel

MSPs can create Custom Roles on the Roles page. Custom Roles are assigned specific system permissions and specific customers groups, so the users with different roles can only perform certain actions and manage certain customers in the Partner Portal.

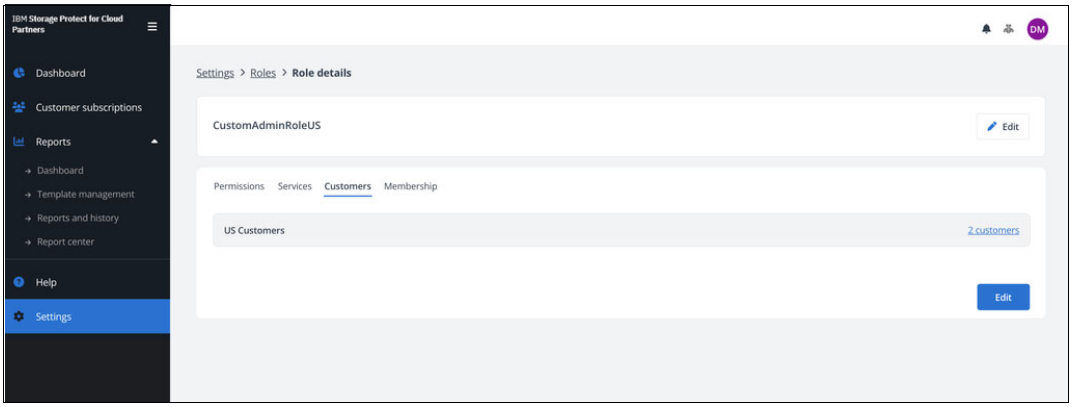


Figure 4-6 IBM Storage Protect for Cloud Partners Role details panel

4.2.3 Reporting

The Partner Portal provides comprehensive reporting capabilities that help MSPs to increase their operational efficiency. Unified dashboards provide a single view of backup and storage activities across multiple customers, platforms, and locations. MSPs can quickly identify issues, such as failed backups or capacity limits, without checking individual systems. MSPs can also easily understand the status of the customer subscriptions (license usage, expiration dates, etc.). This reduces the time and effort needed for manual data collection and monitoring.

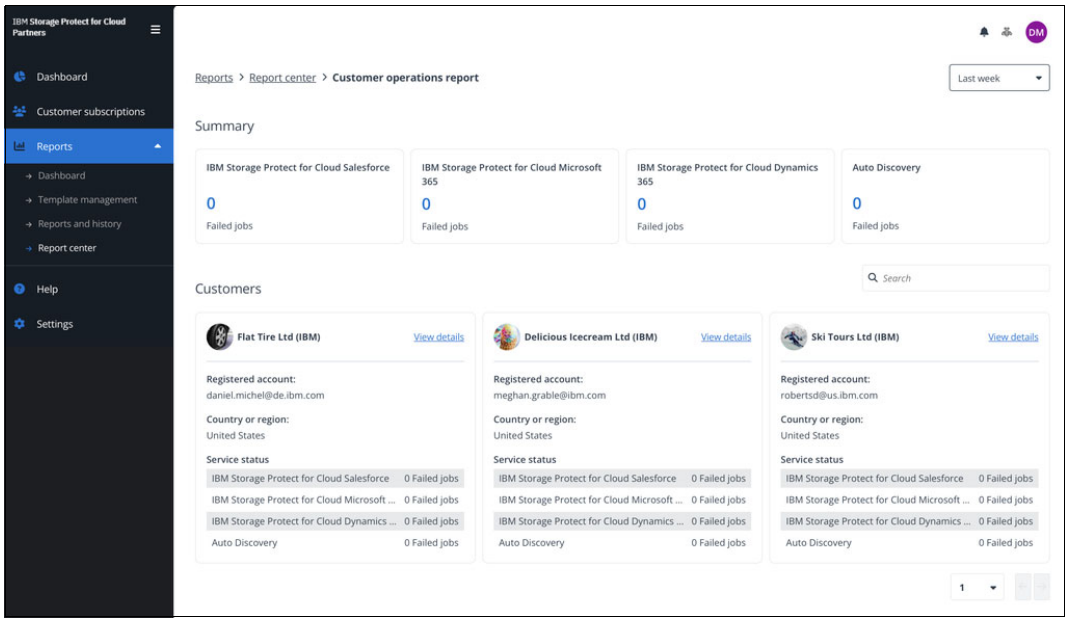


Figure 4-7 IBM Storage Protect for Cloud Partners Reports panel

The report generation engine can automatically generate and distribute reports on a daily, weekly, or monthly basis. MSPs can customize the reports to tailor them to their needs. This cuts down on operational expenses and it improves consistency in communication.

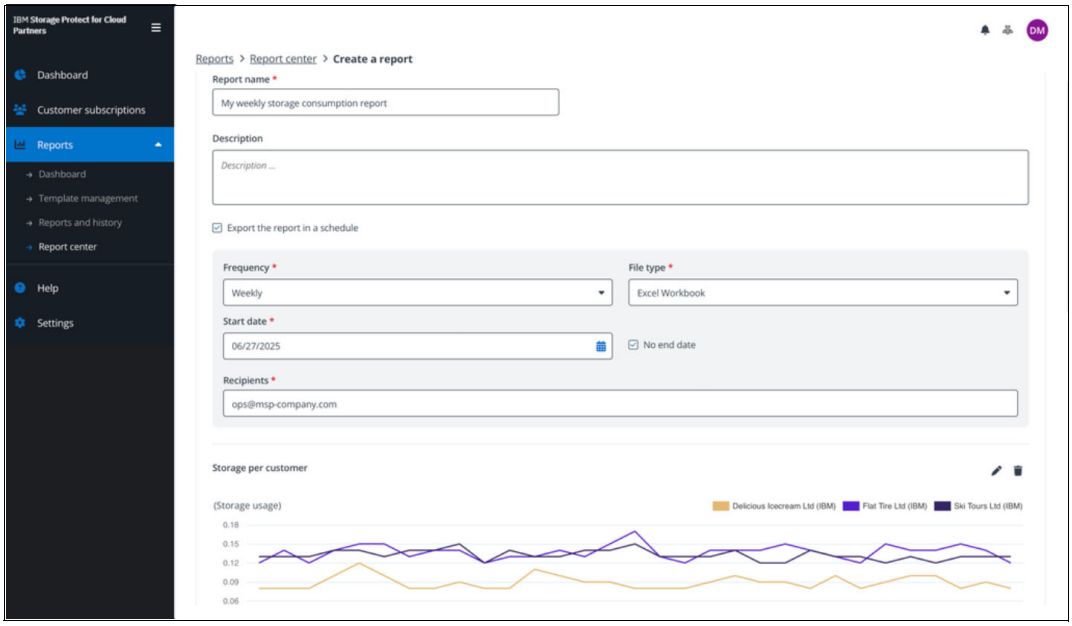


Figure 4-8 IBM Storage Protect for Cloud Partners Report center creation dialog

4.2.4 Monitoring

The Partner Portal is a *single pane of glass*. It allows MSPs to monitor the backup environments of all customers from one central place. It provides details about the data protection jobs, storage consumption, and system health. Alerts are automatically triggered and sent via email.

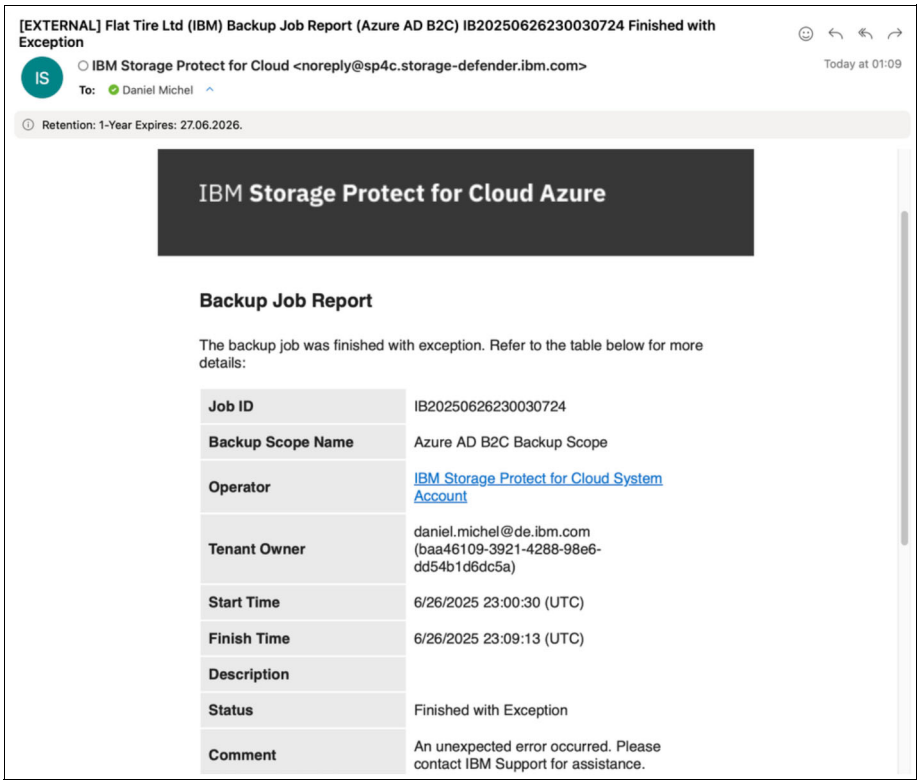


Figure 4-9 Backup Job Report Email example

4.2.5 Storage

Storage profiles allow MSPs in IBM Storage Protect for Cloud Partners to standardize storage across multiple customers. Instead of configuring storage settings individually for each customer, MSPs can assign a storage profile that contains pre-defined configurations. IBM Storage Protect for Cloud Partners has built-in support for many popular Cloud storage providers.

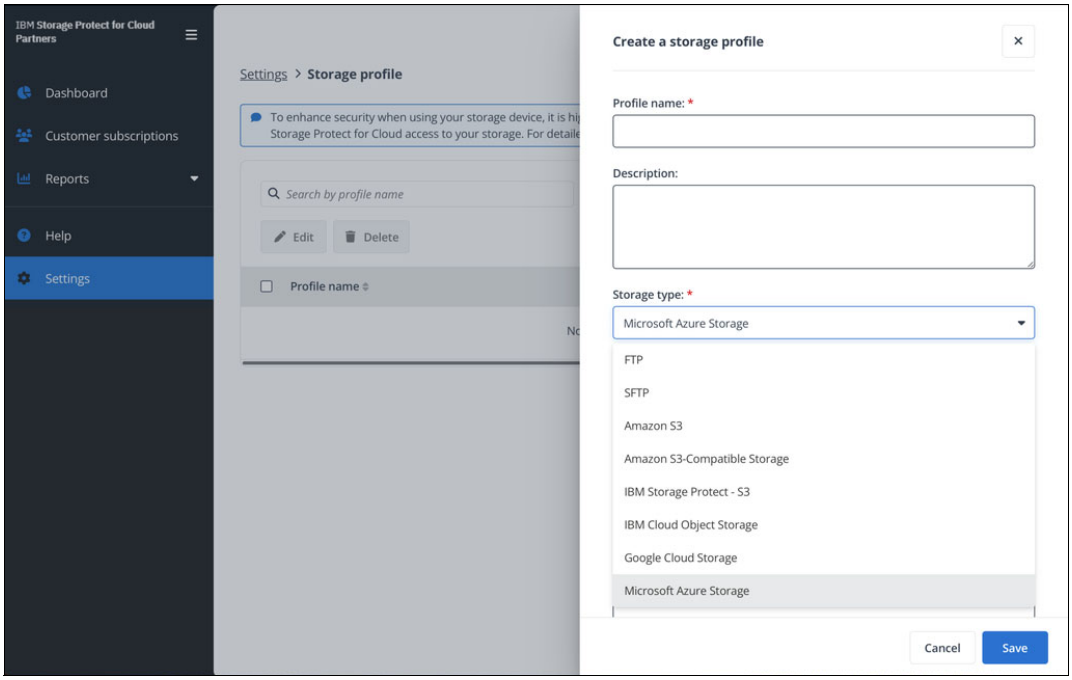


Figure 4-10 IBM Storage Protect for Cloud Partners Storage profile dialog

4.2.6 IBM Graph API

IBM Storage Protect for Cloud Partners comes with the IBM Graph API which streamlines partner operations. It provides a powerful and flexible interface that allows MSPs to programmatically interact with the data protection platform to manage customers, customer subscriptions, data protection jobs and protected data (IBM Storage Protect for Cloud Microsoft 365 only).

MSPs can go to Settings and then click Create App Registration on the API app registration page to create access credentials. The IBM Graph API supports both client secrets as well as certificates for authentication.

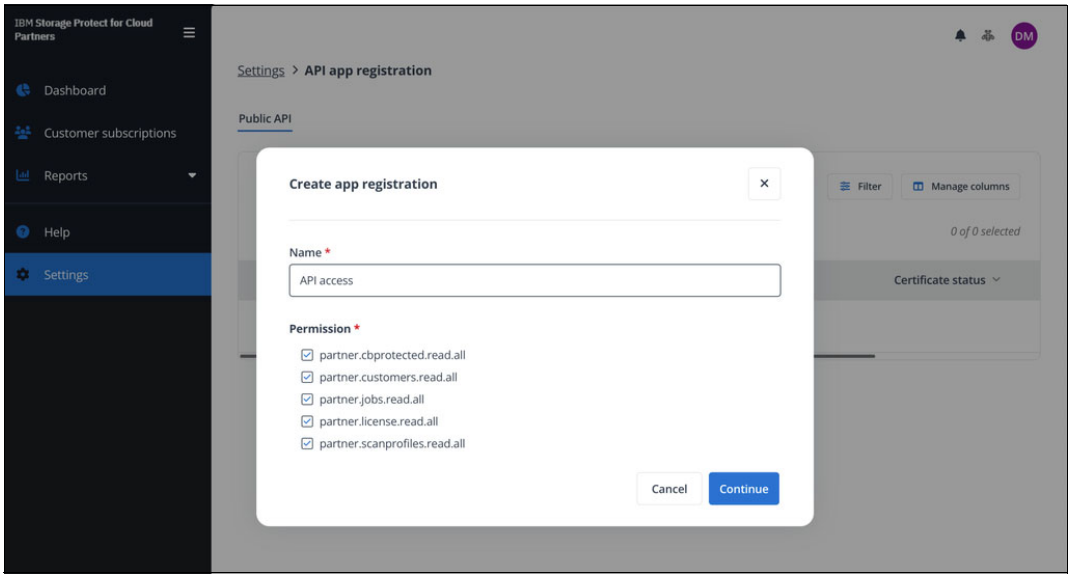


Figure 4-11 IBM Storage Protect for Cloud Partners API Registration dialog

4.2.7 Security

IBM Storage Protect for Cloud Partners provides security by design. It has built-in tenant isolation which means that each customer environment is logically isolated, but MSPs can monitor all customers from one central place. With Role-Based Access, authorized users can only see relevant data per their roles or assigned customers. All administrative tasks in the Partner Portal as well as in the customer's data protection environments are tracked for auditing and compliance.

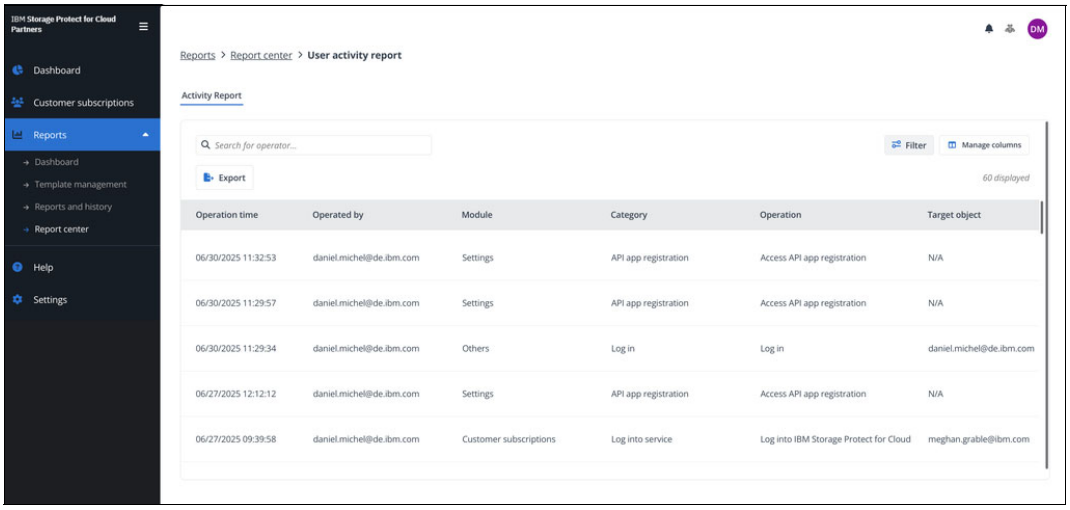


Figure 4-12 IBM Storage Protect for Cloud Partners User activity report panel

5

Conclusion

In today's digital landscape, the explosive rise of ransomware and targeted cyberattacks demands a transformative approach to data protection and recovery. As SaaS adoption accelerates and platforms like Microsoft 365 become indispensable for business operations, IT leaders face an urgent mandate: reevaluate outdated strategies and embrace resilient, cloud-ready solutions. Misplaced confidence in cloud-provider safeguards has led to costly assumptions, but the shared-responsibility model makes it clear—data protection is the organization's burden to bear.

To secure critical workloads and maintain business continuity, forward-thinking organizations must invest in third-party backup and recovery solutions that address the unique vulnerabilities of SaaS environments. IBM Storage Protect for Cloud rises to this challenge with enterprise-grade capabilities that deliver reliability, speed, and intelligent threat detection. In a world where data breaches carry increasingly devastating consequences, such proactive measures are not just recommended—they are essential.

Moreover, managed service providers are leveraging IBM Storage Protect for Cloud to offer data protection as a fully managed service. With multi-tenant architectures and centralized monitoring, MSPs can scale backup operations effortlessly, uphold strict SLAs, and provide expert oversight—freeing IT teams to focus on innovation rather than infrastructure. This partnership model transforms robust cloud data protection into an accessible, subscription-based service that aligns with modern consumption patterns and ensures resilience for businesses of all sizes.

In summary, the convergence of rising cyber threats, expanding SaaS usage, and the shared responsibility model makes robust cloud data protection indispensable. By embracing solutions like IBM Storage Protect for Cloud—either directly or through trusted MSP partners—organizations can achieve comprehensive backup, rapid recovery, and proactive threat monitoring across their critical workloads. This strategic alignment not only mitigates operational risks but also empowers businesses to innovate with confidence in a secure and resilient digital environment. Ultimately, proactive data protection with IBM Storage Protect for Cloud transforms potential vulnerabilities into strategic advantages, ensuring that tomorrow's growth is underpinned by unwavering continuity.

REDP-5759-00

ISBN

Printed in U.S.A.