

IBM Storage Protect for Cloud Azure

Unlock unparalleled data protection and compliance in Microsoft Azure



Highlights

Safeguard data with automated backups up to 4 times a day

Gain encrypted backup and simple search-based restore

Minimize data loss with rapid, granular, easier recovery

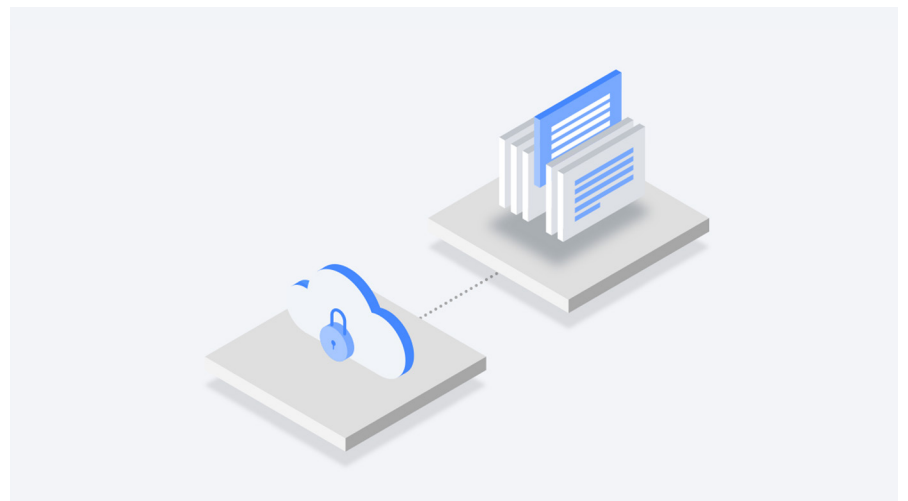
Improve compliance with infinite retention, data control and visibility

The explosive growth of ransomware attacks and other cyberthreats today has forced IT leaders to reevaluate their data protection and disaster recovery strategies.

As software as a service (SaaS), platform as a service (PaaS) and infrastructure as a service (IaaS) applications such as Microsoft 365, Salesforce and Microsoft Azure become ever more entrenched in businesses, they expand to contain more and more data, much of it business critical.

Simultaneously, IT organizations have required more aggressive recovery point objectives (RPOs) and recovery time objectives (RTOs). Organizations also face increasingly stringent regulatory requirements.

IBM® Storage Protect for Cloud Azure is designed to address the critical data protection and compliance needs of organizations in the Azure cloud environment. With its advanced capabilities and seamless integration, this solution helps keep your data secure, recoverable and compliant.





With automated backup, encrypted data, simple search-based restore, rapid granular recovery and enhanced compliance features, IBM Storage Protect for Cloud Azure offers a comprehensive set of capabilities to address your organization's data protection and compliance challenges.

Safeguard data with automated backups up to 4 times a day

Automated backups are essential for ensuring that critical data is always protected against cyberthreats, hardware failures, natural disasters and human errors. IBM Storage Protect for Cloud Azure automates the backup process through a simple and intuitive interface that lets IT teams easily configure backup policies, schedules and retention settings. This feature helps organizations back up data regularly without relying on manual processes that can be error-prone and time-consuming.

The solution also provides real-time status updates on backup operations, allowing IT teams to monitor progress and make sure backups are completed on time.

Gain encrypted backup and simple search-based restore

Encryption is a fundamental security measure that helps organizations protect their critical data against cyberthreats. Using the encrypted backup data capabilities of IBM Storage Protect for Cloud Azure, organizations can protect their backup data from unauthorized access, theft and corruption. It provides a security-rich network connection between the backup and recovery environment and the Azure platform to protect data.

IBM Storage Protect for Cloud Azure encrypts all backup data both in transit and at rest, using a unique encryption key that is generated for each backup job so that even if one key is compromised, the other backups can remain secure. This way, even if backup data falls into the wrong hands, it can't be accessed without the proper decryption key.

Data loss can be a significant challenge for organizations that rely on native workload backup because in some cases, the backup may not exist, leading to disruption in business operations and possible financial losses. With the solution's search-based restore feature, IT teams can search and browse through all backups to locate specific files or objects. It supports full-text search, file name search and metadata-based search, making it easier for IT teams to locate the desired data quickly. Once the data is located, it can be restored with just a few clicks, minimizing downtime and promoting business continuity.



Minimize data loss with rapid, granular, easier recovery

IBM Storage Protect for Cloud Azure provides on-demand, granular recovery of Microsoft Azure Active Directory, Azure Virtual Machines and Azure Blob Storage. Data loss can occur due to various reasons such as cyberthreats, hardware failures, natural disasters or human errors. With the solution's rapid recovery capability, IT teams can recover lost data quickly and efficiently without having to restore an entire virtual machine or storage account.

Improve compliance with infinite retention, data control and visibility

IBM Storage Protect for Cloud Azure provides a comprehensive data control, visibility and control capability that helps organizations improve compliance with infinite retention. Data retention is an essential aspect of data management, particularly for organizations that need to comply with regulatory requirements such as GDPR, HIPAA and PCI-DSS.

With the solution's infinite retention capability, organizations can retain backup data infinitely to manage compliance with regulatory requirements. The infinite retention capability in IBM Storage Protect for Cloud Azure offers flexible retention policies that allow organizations to retain backup data for as long as they need to.

Additionally, IBM Storage Protect for Cloud Azure offers real-time status updates on backup operations, allowing IT teams to monitor progress and ensure that backups are completed on time. It also provides detailed reporting capabilities that enable IT teams to analyze backup data trends and make informed decisions about their data management strategy.

Furthermore, the solution's visibility and control capabilities enable IT teams to monitor their backup environment's security posture and make changes as needed. The solution provides access controls, multifactor authentication and other security measures that help protect backup data against cyberthreats.

The infinite retention, visibility and data control capabilities of IBM Storage Protect for Cloud Azure provide organizations with a comprehensive set of tools to manage their backup and recovery operations efficiently. With flexible retention policies, real-time status updates, detailed reporting capabilities and advanced security measures, IT teams can manage compliance with regulatory requirements while managing their data more effectively.

Conclusion

IBM Storage Protect for Cloud Azure is a powerful data protection solution that enables organizations to safeguard their critical data in the cloud. The solution offers a comprehensive set of features such as automated backups, encrypted backup data, simple search-based restore, rapid recovery and infinite retention capabilities. These features help organizations minimize data loss and downtime while managing compliance with regulatory requirements. IBM Storage Protect for Cloud Azure is a strong choice for businesses that need a reliable and efficient way to protect their data in the Microsoft Azure platform, minimize risk and ensure business continuity.

Why IBM?

IBM offers a vast portfolio of hardware, software and services, including industry-leading data storage products and solutions. Innovative technology, open standards, excellent performance and a broad portfolio of proven storage offerings—all provided by IBM, a recognized industry leader—are just a few of the reasons to consider IBM Storage Protect for Cloud.

For more information

To learn more about IBM Storage Protect for Cloud, contact your IBM representative or IBM Business Partner, or visit ibm.com/products/storage-protect-for-cloud.

© Copyright IBM Corporation 2023

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
July 2023

IBM and the IBM logo and are trademarks or registered trademarks of International Business Machines Corporation, in the United States and/or other countries. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on ibm.com/trademark.

Microsoft is a trademark of Microsoft Corporation in the United States, other countries, or both.

This document is current as of the initial date of publication and may be changed by IBM at any time. Not all offerings are available in every country in which IBM operates.

It is the user's responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs. THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT.

Statement of Good Security Practices: No IT system or product should be considered completely secure, and no single product, service or security measure can be completely effective in preventing improper use or access. IBM does not warrant that any systems, products or services are immune from, or will make your enterprise immune from, the malicious or illegal conduct of any party.

The client is responsible for ensuring compliance with all applicable laws and regulations. IBM does not provide legal advice nor represent or warrant that its services or products will ensure that the client is compliant with any law or regulation.

