

IBM Storage Protect

Overview

IBM Storage Protect has been in the market for decades (it is still referred to by its initial branding, Tivoli Storage Manager or "TSM," by many customers). In March 2023, it was re-branded from IBM Spectrum Protect, as a part of the company's efforts to streamline and simplify its portfolio branding, and as a step towards its ultimate architectural vision of delivering a set of data services unified by a common control plane, deployable on any underlying infrastructure.

Usage

IBM Storage Protect software is typically used in enterprise environments that require physical file servers and enterprise applications (e.g., IBM DB2) to be protected. Protection of containerized and virtualized environments as well as modern applications requires additional software (either third-party, IBM Storage Protect for Virtualized Environments, IBM Storage Protect Plus, formerly IBM Spectrum Plus, or IBM Storage Protect for Cloud, which is formerly IBM Spectrum Protect Online Services and utilizes AvePoint technology to protect software-as-a-service applications). IBM Storage Protect Plus and Storage Protect for Cloud are covered separately in The Futurum Group's Data Protection Software and Backup-as-a-Service research.

- Characteristics
 - Performance
 - Depends on hardware (network connections, etc.).
 - Supports parallel data transfers.
 - Availability – Highly available environments are supported with specific configurations and failover software.
 - Replication – policy-driven incremental, scheduled or client-specific multi-site replication.
 - Supports bare metal restores.

Highlights

- Enterprise backup and recovery software with extensive features
- Protects block, NAS, and file storage, as well as applications and databases
- Large selection of targets for protected data
- Federated metadata catalog from multiple Storage Protect instances
- Incremental forever backup technology
- Compression and deduplication
- Node replication for disaster recovery (DR)
- Regulatory compliance and encryption support
- OEM relationship with Cohesity (DataProtect for VMs, Helios global SaaS control plane)
- Component of IBM Storage Defender

- Use Cases/Implementations
 - Backup and granular, operational recovery
 - Disaster recovery (DR)
 - Replication
 - DR testing, documentation, automation, and orchestration
 - Recovery from malware/ransomware
 - Data lifecycle management
 - Tiering to cloud and tape
 - Monitoring and analytics
- System Environments
 - Supported sources:
 - Multiple applications including HCL Domino, Microsoft SharePoint, Exchange, Active Directory, SAP, SAP HANA, SAP Oracle, SAP DB2, Oracle, Informix, Microsoft SQL Server, Sybase, IBM DB2.
 - Operating systems – Major UNIX (AIX, HP-UX, Solaris), multiple Linux, Windows, MacOS.
 - Virtual environments, via Storage Protect for Virtual Environments, including Microsoft Hyper-V and VMware ESXi.
 - Data from S3 client applications can be directly copied to an IBM Storage Protect repository.
 - Supports common data repository for direct backup and Instant Access Restore of Storage Protect Plus (previous Spectrum Protect Plus) and Storage Protect for Cloud (previously Spectrum Protect Plus Online Services) backups.
- Deployment and Administration
 - Installation wizard provides deployment simplicity.
 - IBM Storage Protect Operations Center can manage backups and systems, as can third-party software such as VMware vSphere Client.
 - IBM Blueprints provide reference designs for various configurations.
 - Automated, policy- and SLA-based jobs.
 - Self-service portal for ad hoc file restores.

Key Capabilities

Architecture and Deployment

IBM Storage Protect is installed on backup servers. Multiple sites can be managed, and catalog data (metadata in the content repository) is federated across sites. The architecture is highly scalable to manage billions of objects per backup server.

Stand-alone, IBM Storage Protect supports physical environments and enterprise applications such as IBM DB2. It can be installed in conjunction with IBM Storage Protect for Virtual

Environments to support virtual environments, and with IBM Storage Protect for Cloud to support SaaS applications including Microsoft 365 and Salesforce. Additionally, data can be backed up directly from IBM Storage Protect Plus to IBM Storage Protect.

Effective March 2023, IBM also has an OEM agreement and collaboration with Cohesity for Cohesity's DataProtect data protection solution and Helios SaaS data management offering. The collaboration will result in the first iteration of IBM Storage Defender, which is slated for general availability in the second quarter of 2023. Storage Defender is a long-term go-to-market play for IBM that will tie in a collection of IBM and partner products and capabilities under a new, IBM-developed management plane. In addition to IBM Storage Protect and Cohesity DataProtect, IBM has called out that IBM Storage FlashSystem with Safeguarded Copy, as well as a solution for container protection, will also be incorporated into the solution at its launch. Moving forward, Storage Defender will tie in further collaboration with a variety of players in the cyber-resilience landscape, in areas such as data scanning and classification. The ecosystem-supported approach will be an important theme in IBM's portfolio development and go-to-market strategies for data management and protection, moving forward.

Administration and Management

IBM Storage Protect backups can be managed by the IBM Storage Protect Operations Center, VMware vSphere Client, or third-party software (REST APIs are supported). This reduces the dedicated expertise required by administrators. For example, applications integrated with Storage Protect enable coherent data protection and management control through the application administration. Along a similar vein, IBM offers Storage Protect Blueprints to reduce the deployment time and expertise around configuration that is required. Cloutility software available from IBM partner Auwau enables multi-tenancy, on-boarding and billing for Storage Protect.

Data Cataloging, Search and Analytics

IBM Storage Protect includes a searchable, federated metadata catalog that facilitates granular recovery, compliance, and ransomware analytics.

Backup Processes

Storage Protect can protect source data from block storage systems, file servers, network-attached storage (NAS) systems (including support for the Network Data Management Protocol), applications, databases and data stored in the cloud. Via Storage Protect for Virtual Environments, it also supports VMware ESXi and Microsoft Hyper-V sources.

A variety of storage infrastructure types including flash, spinning disk, tape, on-premises object stores and public clouds are supported as storage targets. Protected data is stored in what IBM calls container storage pools (not to be confused with Docker-style containers). Storage pools and

replicate copies can reside on a variety of storage systems including NAS systems, block storage, virtual tape libraries (VTLs), object storage, public clouds, and tape devices. Another instance of Storage Protect on a server can also be a protection target.

IBM Storage Protect container storage pools enable external cloud and object storage without additional hardware or gateways on popular cloud environments such as IBM Cloud, IBM Cloud Object Storage, Amazon Simple Storage Service (Amazon S3), Google Cloud Storage, Microsoft Azure Blob storage, and other validated S3 object storage services.

According to IBM, Storage Protect can ingest up to 100 TB of new and changed data per day. The product uses an incremental forever backup technology to only store changed data, reducing network bandwidth and backend storage requirements.

As data grows, IBM Storage Protect backups can be augmented with advanced agents and snapshots that can reduce backup and restore times for large applications and virtual machines. For example, the IBM Storage Protect High Speed Data Transfer option, which uses patented IBM Fast, Adaptive and Secure Protocol (IBM FASP®) technology to transfer data faster than TCP over high-latency or high-loss networks.

Recovery and Replication

Backups are important but restores are essential. IBM Storage Protect enables fast, flexible restores from primary and remote recovery sites. Individual items, databases, storage volumes, complex systems, and entire data centers can be recovered. Granular recoveries are further facilitated by the ability to copy, browse, and recover from storage snapshots. Additionally, Storage Protect provides near-instant access to backup data for Microsoft Windows and Linux Intel-based servers and Windows workstations. Restores can occur from an alternate backup server if the primary backup server is unavailable.

Backup information also be replicated between multiple IBM Storage Protect servers at different sites, either on-premises or hosted in the cloud. IBM Storage Protect Extended Edition includes policy-driven remote replication, which can significantly reduce storage space requirements at primary backup sites.

Simplified disaster-recovery audits, recovery simulators and guided recovery from disasters provide assurance that systems can be recovered as expected. Self-service recovery is available (e.g., for application owners).

Data Efficiency

Incremental forever-based backups, software-based compression and deduplication, and policy-based data lifecycle management, including tiering to on- or off-premises object storage (e.g., support for AWS S3 Intelligent Tiering) all support data efficiency.

Encryption and Immutability

IBM Storage Protect supports immutability, including IBM Storage Scale as WORM file volumes, and immutable storage on IBM Cloud Object Storage and IBM Cloud Object Storage System for cloud storage pools.

Software-based encryption for data in-flight, and for data stored in IBM Storage Protect storage pools, is supported. External, hardware-based encryption (e.g., for tape) is also supported.

Access Control

Role-based access control (RBAC) and multi-factor authentication (MFA) are supported, as is two-key authorization for administrator commands. Two key authorization for administrator commands offers tighter security and requires dual authorization to prevent data loss. Additionally, firewall access may be set up, and secure network-based communications is supported via the TLS and SSL protocols.

Front-end anomaly detection monitors data flow and deduplication patterns for suspicious activity. After client backup sessions, statistics are analyzed for signs of ransomware infection. If signs are present, administrators are notified, and warning message is displayed in the Operations Center.

Data Vaulting

Data can be migrated to tape storage solutions, and IBM Storage Protect has built-in integration to the cloud.

Significant Announcements

- 2023
 - March:
 - Re-branding from IBM Spectrum Protect
 - Announcement of OEM relationship with Cohesity
 - [Launch of IBM Storage Defender](#)
 - Launch of IBM Storage Protect 8.1.18

Futurum Group EvalScale – Data Protection Software

The Futurum Group product review methodology “EvalScale” assesses each product within a specific technology area. The evaluation of each product is based on its capabilities, with capabilities for each technology segment grouped into distinct categories. For the Data Protection Software EvalScale products are evaluated based on the following 4 criteria categories:

- Protection Environment
- Advanced Capabilities
- Cyber Resiliency
- Ability to Execute

The full Data Protection EvalScale can be found [here](#).

The Futurum Group Opinion and Outlook for IBM Storage Protect Plus

IBM Storage Protect has a long history with customers, to the point where it is still referred to as TSM by many of them. It is entrenched especially in enterprise-scale environments requiring protection of physical infrastructure and traditional applications. The specialized training historically required for TSM has been substantially reduced via the addition of IBM Storage Protect Operations Center, which delivers visibility and ease of use to backup administrators. This answers many earlier criticisms. Adding a self-service portal has also been important for customers, as it enables backup administrators to meet the needs of lines of business more effectively.

Looking ahead, the announcement of IBM Storage Defender portends a portfolio and go-to-market roadmap that is increasingly complemented by other IBM Storage products, as well as by third-party software. For example, IBM has struggled to gain traction from a data protection standpoint in VM environments with Storage Plus for Virtual Machines, and with Storage Protect Plus. Cohesity will fill this niche. Additionally, larger-scale data management and cyber-resiliency capabilities will be added, both through partnership and through tie-ins with IBM software capabilities such as IBM QRadar.

Copyright 2023 The Futurum Group, LLC. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or stored in a database or retrieval system for any purpose without the express written consent of The Futurum Group Inc. The information contained in this document is subject to change without notice. The Futurum Group assumes no responsibility for errors or omissions. The Futurum Group makes no expressed or implied warranties in this document relating to the use or operation of the products described herein. In no event shall The Futurum Group be liable for any indirect, special, inconsequential or incidental damages arising out of or associated with any aspect of this publication, even if advised of the possibility of such damages.