IBM Storage Defender Data Protect

A data resilience solution to accelerate and simplify data backup and recovery

Highlights

Enhances multi-layered protection for enterprise applications

Provides fast and safe recovery to reduce downtime

Offers data protection for a wide range of workloads

Allows end-to-end data resiliency as part of IBM Storage Defender

The average cost of a data breach continues to climb each year, with 2024 reaching an all-time high of USD 4.88million.[1] Protecting your data and recovering from an attack quickly and safely has become critical for business continuity. IBM Storage Defender Data Protect is a comprehensive solution that keeps your data safe and available, safeguarding against cyber threats such as ransomware, exfiltration and insider attacks. It offers policy-based protection across a wide range of cloud-native and on-premises data sources. Defender Data Protect is part of IBM Storage Defender.

IBM Storage Defender accelerates alert detection through several integrated mechanisms. By deploying in-line data corruption detection directly on primary storage arrays, it can promptly identify and signal anomalies as soon as corrupted data is written, minimizing exposure to potential data loss or attack. Agent-based anomaly detection within VMware virtual machines enables real-time monitoring of performance metrics and behaviors, flagging any deviations that might indicate a security event or operational issue. Additionally, anomaly detection in backup data scrutinizes both backup contents and behaviors for unexpected changes, providing a further layer of early warning after data leaves primary production systems. Finally, by scanning backups and data sets within isolated scan environments or clean rooms, the solution can safely identify malware or ransomware signatures without risk to production data, ensuring rapid and secure incident response. These multilayered detection strategies enable organizations to detect and respond to threats or corruption significantly faster than traditional, siloed monitoring approaches.

Multi-layered protection for enterprise applications
Designed on zero-trust principles, Defender Data Protect secures your enterprise data across a broad set of IT infrastructures–virtual and physical servers, traditional and containerized applications, databases, NAS, and SaaS workloads. This combination of security protocols, including immutability, WORM, data encryption framework, multifactor authentication, and granular role-based access control, helps to stop unauthorized applications and bad actors from modifying or deleting your data.

Fast and safe recovery to reduce downtime
The solution features near-zero recovery point objectives (RPOs) and near-instant recovery time objectives (RTOs) to meet business service-level agreements (SLAs). With the IBM Storage Defender unified control plane, you can quickly search and recover data on any Defender Data Protect cluster, located anywhere in the world. Defender Data Protect can help reduce downtime by instantly mass restoring any number of virtual machines (VMs), large volume of unstructured data, and any size Oracle database to any point in time, helping to reduce your data protection costs.

Data protection for a wide range of workloads
IBM Storage Defender Data Protect offers a robust set of capabilities for data protection and recovery across a wide range of workloads as detailed in the following table.

Protected Workloads	– Hypervisors: VMware vSphere (6.5 and later), Microsoft Hyper-V (2022, 2019, 2016, 2012 R2), Nutanix AHV, and RHeV – Kubernetes-based data and application state – Cloud: AWS EC2, Azure VM, and Google Compute – Physical: Windows, Linux (RHEL, CentOS, OEL, Debian, Ubuntu), AIX (7.x), and Solaris – Enterprise Databases: Oracle (11g R2, 12c), Oracle RAC and Microsoft SQL (2008 or later), SAP Oracle, SAP HANA, SAP Sybase ASE, SAP MS SQL, Sybase IQ, IBM DB2 LUW, Sybase ASE – Modern Databases: MongoDB with CDP, Hive, Hbase, Cassandra, CouchbaseDB, MySQL Enterprise Commercial Edition – Cloud-native Databases: AWS RDS, AWS Aurora, CockroachDB – Applications: MS Exchange (2010 SP3 or later), MSFT Active Directory, Microsoft 365 (Exchange Online, SharePoint Online, OneDrive, Teams, Groups), SalesForce (SFDC), and SAP HANA – Primary storage: IBM FlashSystem and IBM SAN Volume Controller, Pure FlashArray, HPE Nimble and Cisco Hyperflex – NAS: Pure FlashBlade, NetApp, Isilon, IBM Storage Scale, Google EFS, Elastifile, and generic solutions

Recovery Level	– Instant mass restore – Granular recovery of files, folders, and objects – Volume recovery – VMDK recovery – Instant volume mounts – Instant restores of VMs – Cyber recovery – 12 hour RPO
Ransomware Detection	– Immutable backups, DataLock (WORM), encryption, RBAC, Cyber vaulting – Machine learning-based anomaly detection – Rapid recovery at scale
Long-Term Archival	– Public cloud infrastructure, S3 and NFS compatible devices
Global Search	– Global actionable search – Automated global indexing – Wildcard searches for any VM, file, or object on the platform
Global Management and Access Control	– Storage Defender control plane – Multi-cluster single sign-on – Multi-factor authentication – Multi-cluster dashboard
Machine-Drive Recommendation	– Clean recovery point – Proactive system wellness – Capacity prediction – What-if analysis – Performance balancing – Support automation
Capacity Optimization	– Global variable-length sliding-widow deduplication – Compression
Integration and Automation	– API-first architecture – OpenAPI standard – RESTful API – Python SDK – PowerShell Module – VMware vRealize (vRA/vRO) – VMware vCloud Director (vCD) – ServiceNow – Ansible
Security	– TOTP, Restricted Shell Access – Software-defined AES-256, FIPS 140-2 compliant encryption of data in flight and at rest

End-to-end data resiliency as part of IBM Storage Defender
IBM Storage Defender Data Protect is part of IBM Storage Defender that integrates the strengths of our existing data protection products with innovative features that safeguard mission-critical workloads. This unified approach enables you to consume our data resilience software offerings as a single, centrally managed solution. Automation further accelerates the safe recovery of your mission-critical workloads.

Business benefits
Storage Defender Data Protect helps simplify and modernize your backup and recovery infrastructure with its multi-layered protection for enterprise applications and its fast and safe recovery capabilities. Defender Data Protect is part of IBM Storage Defender, a solution that helps monitor, protect, detect, and recover your data across primary and secondary storage. With IBM Storage Defender, you can enhance and better integrate your data protection and data security solutions while helping reduce the complexity and cost of your data storage management.

Why IBM?
IBM offers a comprehensive portfolio of hardware, software and services to help organizations cost effectively address their IT infrastructure needs. These include robust data storage solutions to enable always-on, trustworthy storage and help expedite disaster recovery. Because business needs shift, IBM solutions emphasize interoperability and the integration of new use cases or approaches, from analytics to multisite backup to near-instant recovery.

To learn more about IBM Storage Defender Data Protect, contact your IBM representative or IBM Business Partner, or visit ibm.com/products/storage-defender.

1. X-Force 2025 Threat Intelligence Index, May 2025, IBM

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
August 2025