# 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 2023 reaching an all-time high of USD 4.45 million.[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 high-performance, secure data backup and recovery solution to safeguard your data 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 Data Protect provides comprehensive data backup and recovery for a wide variety of workloads, supporting cloud-native, edge, and on-premises workloads at scale. It can help streamline your operations through integrated solutions, under a single management plane, spanning across workloads with a multilayered security architecture, API-first extensibility for turnkey backup and recovery, and immutable snapshots. Defender Data Protect provides near-instant recovery of databases and virtual machines. By using AI-powered anomaly detection, global search, and multi-cloud support for virtual air-gapping and data isolation, it simplifies and accelerates your backup and recovery operations. Combined with its robust global deduplication and data compression capabilities, Defender Data Protect can help you lower the total cost of ownership by minimizing overhead and helping you save on storage costs. Moreover, its cyber threat detection capabilities can identify threats early on to ensure your data copies are clean. In the event of a cyberattack or data corruption, you can rely on the mass instant restore capabilities within Defender Data Protect for a swift return to normal business operations.

**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 (5.5 and later), Microsoft Hyper-V (2019, 2016, 2012 R2), Nutanix AHV<br>– Kubernetes-based data and application state<br>– Cloud: AWS EC2, Azure VM, and Google Compute<br>– Physical: Windows, Linux (RHEL, CentOS, OEL, Debian, Ubuntu), AIX (7.x), and Solaris<br>– 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<br>– Modern Databases: MongoDB with CDP, Hive, Hbase, Cassandra, CouchbaseDB, MySQL Enterprise Commercial Edition<br>– Cloud-native Databases: AWS RDS, AWS Aurora, CockroachDB<br>– Applications: MS Exchange (2010 SP3 or later), MSFT Active Directory, Microsoft 365 (Exchange Online, SharePoint Online, OneDrive, Teams, Groups), SalesForce (SFDC), and SAP HANA<br>– Primary storage: IBM FlashSystem and IBM SAN Volume Controller, Pure FlashArray, HPE Nimble and Cisco Hyperflex<br>– NAS: Pure FlashBlade, NetApp, Isilon, IBM Storage Scale, Google EFS, Elastifile, and generic solutions |
| --- | --- |

| | |
|---|---|
| Recovery Level | – Instant mass restore<br>– Granular recovery of files, folders, and objects<br>– Volume recovery |
| Ransomware Detection | – Immutable backups,<br>  DataLock (WORM), encryption<br>– Machine learning-based anomaly detection<br>– Rapid recovery at scale |
| Long-Term Archival | – Public cloud infrastructure, S3 and<br>  NFS compatible devices |
| Global Search | – Global actionable search<br>– Automated global indexing<br>– Wildcard searches for any VM, file,<br>  or object on the platform |
| Global Management<br>and Access Control | – Storage Defender control plane<br>– Multi-cluster single sign-on<br>– Multi-factor authentication<br>– Multi-cluster dashboard |
| Machine-Drive<br>Recommendation | – Clean recovery point<br>– Proactive system wellness<br>– Capacity prediction<br>– What-if analysis<br>– Performance balancing<br>– Support automation |
| Capacity Optimization | – Global variable-length<br>  sliding-widow deduplication<br>– Compression |
| Integration and<br>Automation | – API-first architecture<br>– OpenAPI standard<br>– RESTful API<br>– Python SDK<br>– PowerShell Module<br>– VMware vRealize (vRA/vRO)<br>– ServiceNow<br>– Ansible |
| Security | – Software-defined AES-256, FIPS 140-2<br>  compliant encryption of data in flight and<br>  at rest (with FIPS 140-3 certification<br>  available soon) |

**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.

IBM Storage Defender also includes an AI-powered Trust Index that provides a score to indicate the relative trustworthiness of your data copies by combining signals from existing solutions and detection methodologies unique to Storage Defender developed by IBM Research. This capability leverages the knowledge and experience from across IBM to help our clients secure and rapidly recover their critical business information with ease.

**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. Cost of a Data Breach Report 2023, September 2023, IBM.

**IBM.**