

IBM Storage Defender

Simplify data resilience
for enterprise data storage



Highlights

Detects threats to your data

Accelerates business operations recovery

Integrates with SecOps tools and processes

Simplifies purchasing and licensing management

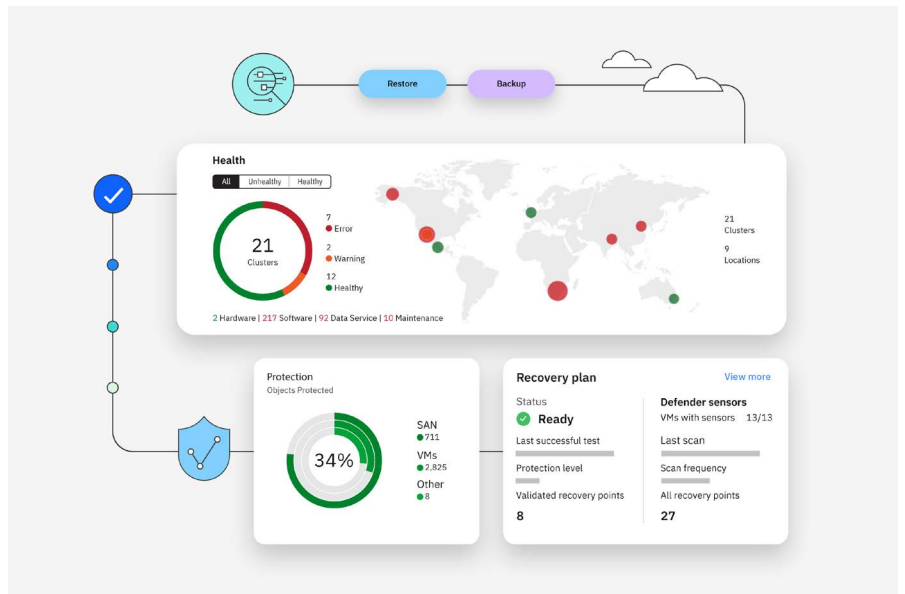
Business leaders today face a multitude of potential threats to their organizations' data. From data loss caused by hardware failure, user error or sabotage to ransomware, exfiltration and other destructive attacks, an organization's brand and customer relationships are at stake as these threats continue to proliferate. As of 2023, identifying and containing a data breach takes affected organizations an average of 73 days and costs USD 4.45 million, a 15% increase since 2020.¹

The IBM® Storage Defender application helps reduce your organization's data loss risks with advanced capabilities that can monitor, protect, detect, and recover data across your hybrid cloud storage infrastructure. It provides a simple, consolidated view of data protection and cyber resilience status with integration into your security dashboards. Storage Defender delivers its capabilities through an integrated SaaS-based management platform that's optimized for personas based on their specific roles across storage, backup and security operations (SecOps).

Detects threats to your data

Storage Defender is designed to use sensors across primary and secondary workloads to detect threats and anomalies from backup metadata, array snapshots and other relevant threat indicators. The application aggregates signals from all available sensors, whether signals originate from hardware IBM FlashCore® Module (FCM) or software-file system or backup-based detection. This proactive capability helps you detect and address an array of threats before they can impact your data. It now also includes new threat detection methodologies developed by IBM Research® specific to Storage Defender, as well as providing the ability to work in close coordination with IBM FlashSystem® to further improve threat detection, data protection and fast operations recovery.

Storage Defender can also detect anomalies in an SAP HANA database as data is written to primary or secondary storage so that, when creating copies of the data, it uses that knowledge to ensure that the data being copied is not compromised.



Accelerates business operations recovery

Storage Defender includes copy data management tools to manage and orchestrate application-integrated copies of data. It makes copies available as users need them—for almost instant data recovery or for data reuse—by cataloging and managing copy data across hybrid cloud infrastructures. Additional automation is built into the latest release of Storage Defender to further accelerate the safe recovery of your mission-critical workloads.

Furthermore, Storage Defender can detect an anomaly in your data by examining the changes in your databases, such as Oracle or SAP HANA. Storage Defender triggers an alert that allows you to initiate a recovery from the latest clean, immutable hardware snapshot. This information can be used to recover data safely because Storage Defender knows which copy is the latest clean copy, based on its awareness of the anomalies it has detected. Additionally, by using on-premises and cloud clean rooms, Storage Defender can provide a place to conduct safe additional validation of the data before restoring it to production.

Integrates with SecOps tools and processes

Storage Defender can integrate security tools that may already be in use in your organization. This integration allows you to build a bidirectional alert and response system between your SecOps and storage teams to establish a set of processes that can reduce the complexity and cost of managing data storage systems.

Also, by allowing Storage Defender to use actionable alerts to align infrastructure, data, and security teams, you can quickly isolate threats and initiate your recovery plans more rapidly.



Simplifies purchasing and licensing management

Storage Defender introduces the concept of resource units (RUs) that let you purchase and allocate the specific data resilience capabilities that meet your needs. This simplified software acquisition and licensing approach makes it easier to manage what previously might have been an array of software capabilities spread over several licensable software solutions.

Optional Storage Defender Components, licensable through Resource Units, include archive management, protection for EPIC and SAP HANA workloads, copy management and storage virtualization.

IBM Storage Defender provides multiple layers of data resilience and enables early detection of threats including risk from ransomware, disasters, sabotage, accidental deletion and other sources of disruption. It also allows rapid recovery across your hybrid cloud storage infrastructure while providing a simple, consolidated view of data protection and cyber resilience status integrated into security dashboards. Using RUs to deliver capabilities, you can streamline your software acquisition and license management by purchasing a single license that provides only the data resilience resources you need.

Why IBM?

IBM offers a broad 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 recovery from disasters. 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.

For more information

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

1. Cost of a Data Breach Report 2023, IBM, July 2023.

© Copyright IBM Corporation 2024

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
June 2024

© Copyright IBM Corporation 2024. IBM, the IBM logo, IBM FlashCore, IBM FlashSystem, and IBM Research 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.

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.

