IBM Storage Defender

Simplify data resilience across your storage state

Highlights

Helps achieve data resilience and compliance standards across your entire storage estate

Provides AI-enabled early threat detection with layered sensors for hardware, file systems, and backups

Delivers safe, fast recovery with trusted copies, pre-recovery scans, and clean room orchestration

Organizations today face increasingly severe threats to their information supply chains. With cyberattacks growing in frequency and severity, cybercriminals are becoming more sophisticated in their techniques. According to the IBM® X-Force® Threat Intelligence Index 2024 report [1], there has been a 71% year-over-year increase in the volume of attacks using valid credentials. Malware deployment was the most common action by cyberattackers, accounting for 43% of all reported incidents, with 20% of these involving ransomware cases. In addition to these threats, IT organizations must contend with natural disasters, system failures, human errors, and sabotage—events that can result in substantial financial losses and erode customer trust if sensitive data is compromised.

IBM Storage Defender is a purpose-built solution designed from the ground up to help organizations reduce the risk of data loss, mitigate financial impact, and ensure seamless business continuity in the face of cyberattacks or unforeseen catastrophic events. It achieves this by delivering advanced capabilities for data resilience, regulatory compliance, early threat detection, and fast, secure recovery, spanning on-premises, cloud, and edge environments. These robust capabilities are delivered through an integrated SaaS-based management platform that simplifies operations and enhances efficiency, providing the ability to quickly assess where an estate stands and identify areas for improvement, which is crucial for strengthening the overall data security posture.

Data resilience and compliance

Storage Defender provides advanced data resilience capabilities for primary systems like IBM FlashSystem® and Dell PowerMax, as well as backup and archive storage. It also integrates with IBM Storage Protect to ensure continuity for existing customers by maintaining the same robust backup and archive capabilities they rely on, while introducing enhanced features for improved data resilience. With unmatched coverage spanning all storage tiers across on-premises and hybrid cloud environments, it stands out as a key differentiator.

Features such as immutable snapshots, air gap protection, role-based access control, and encryption, integrated seamlessly across IBM and non-IBM storage offerings, enable organizations to confidently address security, business continuity, and regulatory compliance challenges. To reduce complexity and costs, Storage Defender introduces a flexible credit-based licensing model, "Resource Units" (RUs), enabling you to choose only the features your enterprise needs.

Easy-to-use policies for backup, remote replication, and secure data retention can be configured to automate the entire data protection process for sensitive data across a wide variety of workloads. The most relevant features are outlined in the table below.

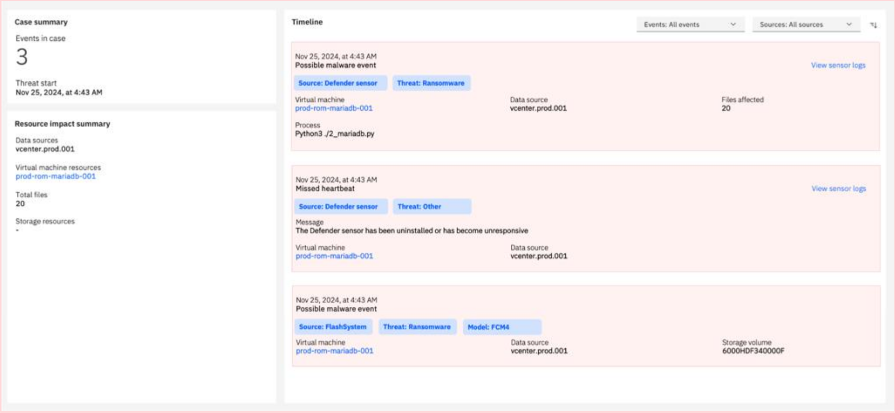
Source Type	Protected Workload
Hypervisors	VMware, Microsoft Hyper-V, Nutanix AHV, RHeV, and Oracle VM
Containers	Red Hat Open Shift, Kubernetes, and VMware Tanzu
Cloud Virtual Machines	Amazon EC2, Azure VM, and Google Cloud
Enterprise Databases	IBM Db2, Oracle, Oracle RAC, SAP, SAP HANA, Microsoft SQL Server, Sybase, Sybase IQ, Informix, and InterSystems
Modern Databases	MongoDB, Hive, HBase, Cassandra, Couchbase, MySQL, PostgreSQL, Datastax, and CockroachDB
Applications	Microsoft Exchange, Microsoft Active Directory, Microsoft SharePoint, and Lotus Domino
Cloud Applications	Microsoft Exchange Online, Microsoft 365, Microsoft Dynamics 365, Salesforce, Google Workspace, Azure File Storage, Azure Blob Storage, Azure VM, and Microsoft Entra ID
Physical Servers	Microsoft, Linux, AIX®, and Solaris
Primary Storage	Over 500 storage systems, including IBM Storage FlashSystem, Dell PowerMax, and Pure FlashArray
File Systems	IBM Storage Scale, Pure FlashBlade, Dell EMC Isilon, NetApp, and Hadoop

Early threat detection

Storage Defender leverages five layers of advanced AI-driven threat detection that analyze data patterns and identify anomalies across all storage tiers. This multi-layered approach ensures potential threats are detected and contained early, regardless of their location. By mitigating risks at every level, Defender reduces the risk of data breaches and downtime, safeguarding critical data and ensuring operational continuity. The table below outlines the locations where threat detection is applied and how it operates across these tiers.

Tier	Threat Detection
Production Systems	AI-driven software sensors to detect anomalous operations at the file system level.
IBM FlashSystem	IBM FlashCore® modules to detect threats at block level through IBM Storage Insights Pro in less than 60 seconds [2].
Primary Storage	Application-aware anomaly scanning on immutable snapshots.
Backup Copies	Anomaly scanning whether in object storage, tape, or the cloud.
Clean Room Systems	AI-driven software sensors and malware scanners to detect suspicious objects before restoring them to production.

When an anomaly is detected, a case is automatically created, and a notification is sent to IBM QRadar® SIEM (Security Information and Event Management), Splunk, or any other supported SIEM solution. In addition, email alerts are sent to incident teams to start coordinated recovery actions. The solution also offers integration with IBM X-Force Threat Intelligence to stay informed about the latest threats and vulnerabilities, ensuring security teams have up-to-date information to assess the anomaly's context effectively. All open cases are presented in a comprehensive "Case summary" screen, which provides detailed information about the type of anomaly, affected virtual machines, and the storage resources impacted by the event. This information is crucial for initiating the next steps between infrastructure and security operations (SecOps) teams and deciding whether recovery plans should be implemented immediately.



Case summary

Events in case
3

Threat start
Nov 25, 2024, at 4:43 AM

Resource impact summary

Data sources
vcenter.prod.001

Virtual machine resources
prod-rom-mariadb-001

Total files
20

Storage resources
-

Timeline

Nov 25, 2024, at 4:43 AM
Possible malware event
Source: Defender sensor
Threat: Ransomware
Virtual machine
prod-rom-mariadb-001
Data source
vcenter.prod.001
Files affected
20
Process
Python3 ./2_mariadb.py

Nov 25, 2024, at 4:43 AM
Missed heartbeat
Source: Defender sensor
Threat: Other
Message
The Defender sensor has been uninstalled or has become unresponsive
Virtual machine
prod-rom-mariadb-001
Data source
vcenter.prod.001

Nov 25, 2024, at 4:43 AM
Possible malware event
Source: FlashSystem
Threat: Ransomware
Model: FCM4
Virtual machine
prod-rom-mariadb-001
Data source
vcenter.prod.001
Storage volume
6000HDF340000F

Figure 1. Case Summary Screen.

Safe and Fast Recovery

IBM Storage Defender provides robust management tools to efficiently control and organize data copies across all storage tiers within hybrid cloud environments. It identifies and displays the most recent trusted copy and its location, ensuring rapid availability for near-instant recovery. Built-in automation simplifies and accelerates the resumption of business operations, enabling organizations to meet recovery point (RPO) and recovery time objectives (RTO) required for regulatory compliance.

For added security, data managed by IBM Storage Defender is replicated to offsite recovery facilities. This enables fast and flexible restores from primary and remote sites, supporting the recovery of individual items, complex systems, and entire data centers, regardless of the scale of the disaster.

When combined with IBM FlashSystem, recovery times can be reduced even further, as IBM Storage Defender restores workloads directly from safeguarded copies. By transferring data through the SAN (Fibre Channel or iSCSI) rather than over the network, this approach minimizes the time required to resume critical business operations. In the event of a potential attack, IBM Storage Defender goes a step further by correlating the specific volume in IBM FlashSystem linked to the targeted virtual machine. It then proactively creates a Safeguarded Copy for offline investigation and recovery operations. This rapid, automated action significantly reduces the time between receiving an alert, containing the attack, and initiating recovery, ensuring minimal disruption when every second counts.

For safe recovery, workloads can be restored in an isolated “Clean Room” environment for analysis and validation before being returned to production systems. This verification confirms that the data is clean, and business operations can be confidently re-established.

Conclusion

IBM Storage Defender provides ultimate visibility across your data estate, serving as the foundation for building multiple lines of defense across all storage tiers. By combining advanced threat detection, robust data protection, and fast recovery capabilities, it supports operational resilience, enabling organizations to navigate unpredictable events with confidence and ensure the continuity of vital business operations.

Why IBM?

IBM offers a comprehensive portfolio of hardware, software, and services designed to help organizations efficiently address their IT infrastructure needs. This includes robust data resilience solutions that support rapid recovery from unexpected catastrophic events. As business requirements evolve, IBM solutions emphasize interoperability and seamless integration of emerging use cases, from advanced analytics to multisite backups and near-instant recovery operations.

For more information

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

1. X-Force Threat Intelligence Index 2024, IBM, February 2024.
2. IBM FlashCore Module Product Guide, IBM, 2024.

IBM Corporation
New Orchard Road
Armonk, NY 10504

Produced in the
United States of America
December 2024

This document is current as of the initial date of publication and may be changed by IBM at any time.

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.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.