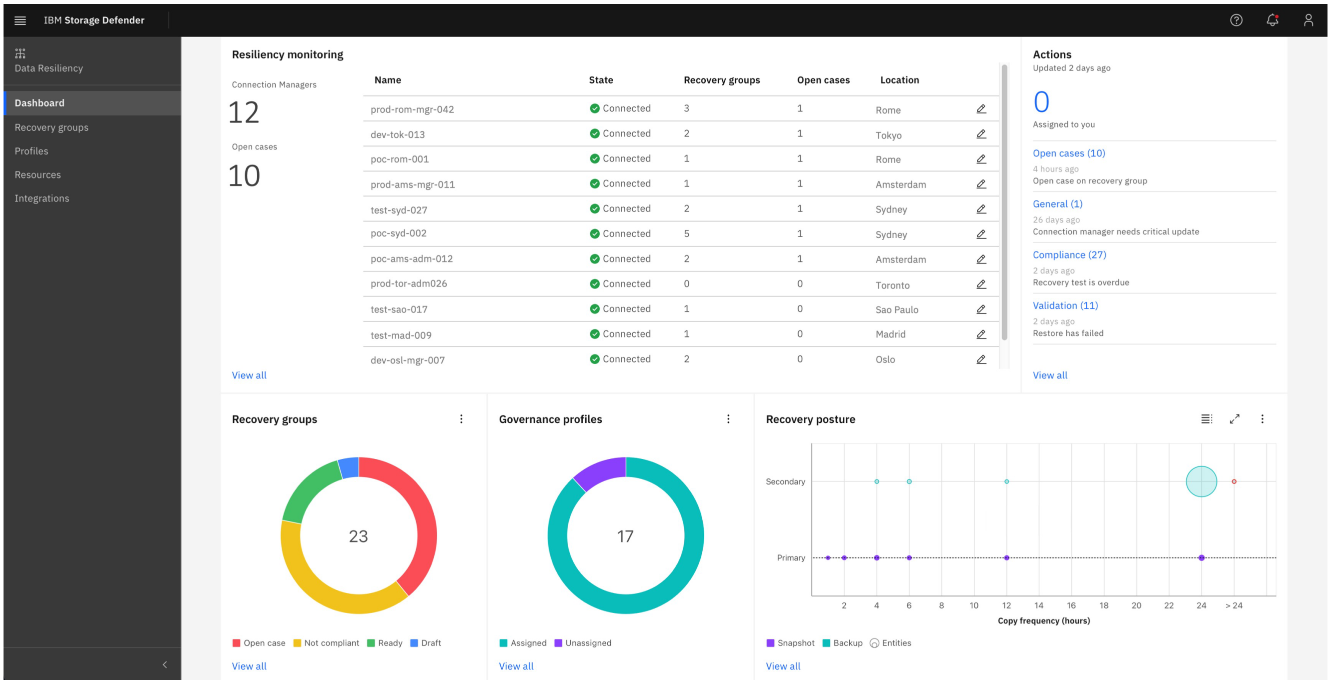
IBM Storage Defender

End-to-end Data Resilience and Compliance across primary and secondary workloads supported with Early Threat Detection and Safe & Fast Recovery.
IBM Storage Defender brings together the capabilities that enterprises need to go beyond data protection to real data resilience. Lower costs with increased operational efficiency, simple licensing, and integrations that preserve existing investments. IBM Storage Defender helps detect threats such as ransomware by leveraging intelligent AI from IBM and its ecosystem partners. These tools help organizations identify the safest recovery points as well as integrate with existing security operations tools and processes so that they can optimize recovery plans and restore critical operations sooner.

Mitigating Risk with a Holistic View: Improves enterprise security by offering governance views to monitor compliance goals. IBM Storage Defender optimizes bringing the right teams together to focus on protection objectives and execute critical recovery plans.
Flexible Licensing Preserves Investment: IBM Storage Defender uses Resource Units to offer flexibility, allowing clients to add or change capabilities over time and only pay for what's used.
Comprehensive Data Resiliency for Modern Workloads: IBM Storage Defender helps detect cyber incidents earlier and accelerates recovery. It supports faster recovery from immutable copies, initiates instant mass restore, and strengthens protection with replication, tiering, archiving, and tape. It supports both modern and traditional workloads on-prem and in the cloud.



Resiliency monitoring

Connection Managers
12

Open cases
10

Name	State	Recovery groups	Open cases	Location
prod-rom-mgr-042	✓ Connected	3	1	Rome
dev-tok-013	✓ Connected	2	1	Tokyo
poc-rom-001	✓ Connected	1	1	Rome
prod-ams-mgr-011	✓ Connected	1	1	Amsterdam
test-syd-027	✓ Connected	2	1	Sydney
poc-syd-002	✓ Connected	5	1	Sydney
poc-ams-adm-012	✓ Connected	2	1	Amsterdam
prod-tor-adm026	✓ Connected	0	0	Toronto
test-sao-017	✓ Connected	1	0	Sao Paulo
test-mad-009	✓ Connected	1	0	Madrid
dev-osl-mgr-007	✓ Connected	2	0	Oslo

View all

Actions
Updated 2 days ago

0
Assigned to you

Open cases (10)
4 hours ago
Open case on recovery group

General (1)
26 days ago
Connection manager needs critical update

Compliance (27)
2 days ago
Recovery test is overdue

Validation (11)
2 days ago
Restore has failed

View all

IBM Storage Defender

Why IBM Storage Defender?

Protecting and ensuring the availability of your data is essential to building operational resilience. Corporate data must be safeguarded, not just from cyber-attacks, but from dangers that include human error, hardware failure, sabotage, and natural disasters.

How: Organizations need to deploy trusted data protection, threat detection, and rapid recovery software with the widest range of capabilities, retention options, and automated management of hot, warm, and cold data. Critical to this is early threat detection so that threats can be identified and resolved before data is impacted, rapid response so that business operations are not disrupted, and that the solution integrates with SecOps tools and processes in placet.

What: IBM Storage Defender provides capabilities that enable early detection, rapid recovery, and SecOps integration with multiple layers of data resilience – data protection, data immutability, and data isolation.
IBM has brought together these capabilities across an organization's primary and secondary storage systems to enable end-to-end data resilience for all workloads and applications.

Threat Detection:

- In-line data corruption detection
- Malware scanning
- AI refines and improves threat detection
- Continuous checking of backups as the universe of known threats expands

Data Immutability:

- Immutable snapshots
- Immutable targets: cold storage / object storage
- WORM – Write-Once Read-Many
- NERN – Non-Erasable Non-Rewritable

Data Protection:

- Data protection across multiple layers and workloads including:
- Hardware snapshots
- Copy data management
- Data backup and recovery
- Short and long-term retention
- All on-premises and cloud environments

Data Isolation:

- Multiple layers of data isolation
- Logical, physical, and air-gapped
- Cold storage / object storage
- Data vaults
- Isolated infrastructures
- Clean rooms

IBM Storage Defender

IBM Storage Defender: Capabilities

IBM Storage Defender is a highly customizable solution where you can leverage various components or tools.

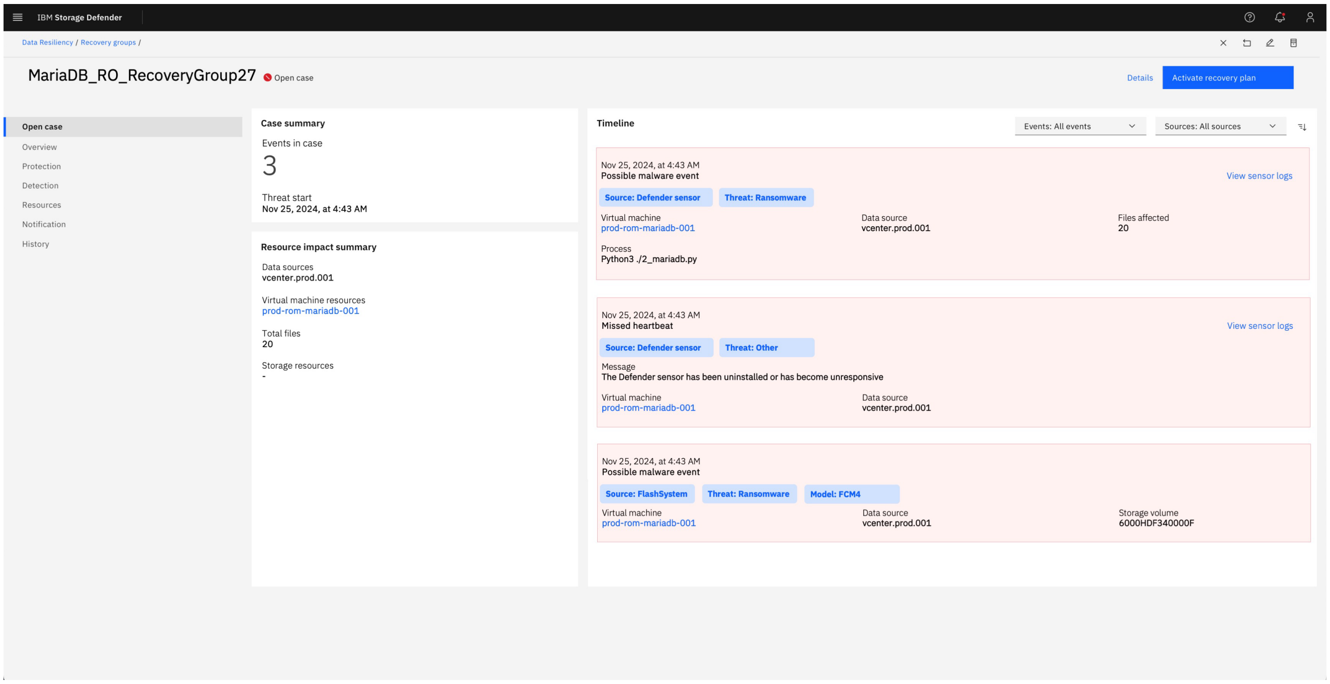
Capabilities:

- Scan immutable snapshots for anomalies
- Create backups and copies of data
- Protect containerized environments
- Archive your data for long term retention
- Protect your data with immutable targets i.e. tape, cloud, flash...
- Virtalize your storage to modernize and consolidate
- Manage your copies i.e. immutable snapshots

Target Audience

Healthcare

In addition to meeting rising care expectations while lowering the costs of care delivery through faster, more efficiently sharing data that connects patients, medical professionals, labs, and other providers, the healthcare industry is under constant attack from cyber threats. In 2021, and for the 11th consecutive year, healthcare had the highest industry average cost related to data breaches, increasing almost 30% from an average total cost of $7.13 million in 2020 to $9.23 million.



MariaDB_RO_RecoveryGroup27 Open case

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

Financial Services

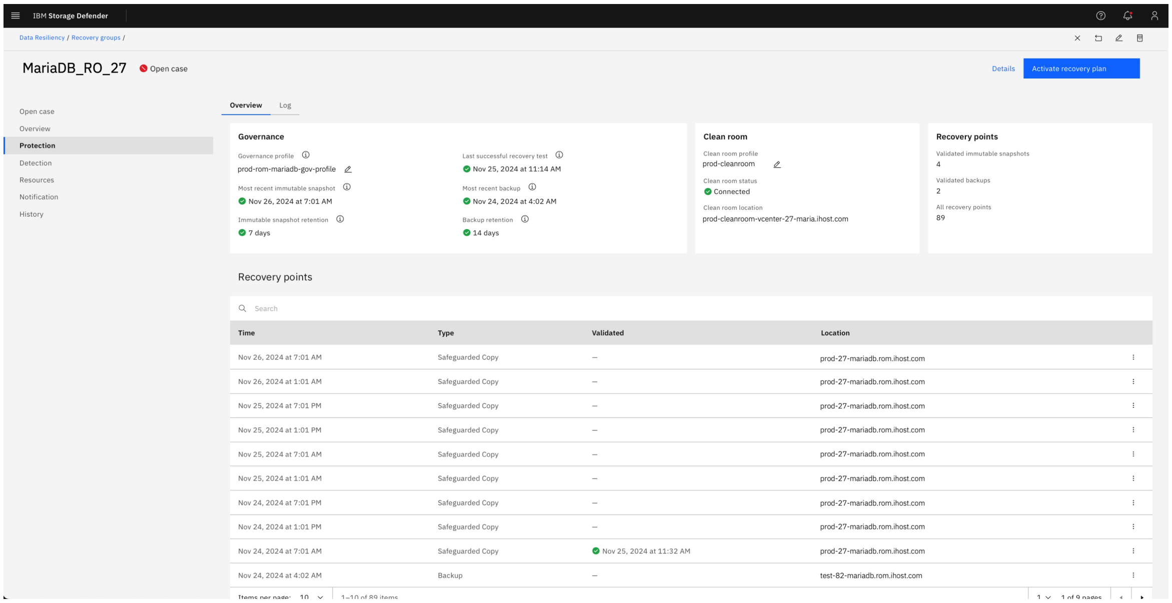
While trying to leverage data insights to find cross-sell and upsell opportunities to grow their businesses and deliver data faster to stakeholders, these organizations are entrusted by their clients with a high degree of sensitive personal information concerning wealth, income, and taxation. As evidenced by three financial services firms being fined by the Securities and Exchange Commission (SEC) in August of 2021 for failing to adequately safeguard PII to meet regulatory compliance demands but are also very attractive targets for cyber thieves. Financial Services trails only healthcare in terms of the highest average cost of a data breach in 2021 at $5.7M.

Government

Governments at all levels must manage and protect their citizens' information. Increasing access to public services, digitizing citizen interactions and the efficient use of tax dollars and government resources are all ways that government leaders and portfolio owners are evaluated. The efficient use and fast delivery of data is paramount to meeting these objectives while ensuring citizen information is protected from compromise. In fact, the average cost of a data breach rose 79% from 2020 to 2021, something that government IT leaders cannot afford to ignore.

Distribution and Logistics

While trying to leverage data insights to optimize inventory, find cross-sell and deliver a more personalized shopper experience, these organizations store a high volume of transactional data, purchase history, credit card information and loyalty programs re entrusted by their clients with a high degree of sensitive personal information concerning wealth, income and taxation. With more and more services and transactions delivered digitally, data needs to be accessible in a fast and efficient manner to support trusted, on the fly decision making to improve customer interactions, both internally and with external trading partners across supply chains without compromising security.



MariaDB_RO_27

Governance

Governance profile: prod-rom-mariadb-gov-profile

Last successful recovery test: Nov 25, 2024 at 11:14 AM

Most recent immutable snapshot: Nov 26, 2024 at 7:01 AM

Most recent backup: Nov 24, 2024 at 4:02 AM

Immutable snapshot retention: 7 days

Backup retention: 14 days

Clean room

Clean room profile: prod-cleanroom

Clean room status: Connected

Clean room location: prod-cleanroom-vcenter-27-maria.ihost.com

Recovery points

Validated immutable snapshots: 4

Validated backups: 2

All recovery points: 89

Recovery points

Time	Type	Validated	Location
Nov 26, 2024 at 7:01 AM	Safeguarded Copy	–	prod-27-mariadb.rom.ihost.com
Nov 26, 2024 at 1:01 AM	Safeguarded Copy	–	prod-27-mariadb.rom.ihost.com
Nov 25, 2024 at 7:01 PM	Safeguarded Copy	–	prod-27-mariadb.rom.ihost.com
Nov 25, 2024 at 1:01 PM	Safeguarded Copy	–	prod-27-mariadb.rom.ihost.com
Nov 25, 2024 at 7:01 AM	Safeguarded Copy	–	prod-27-mariadb.rom.ihost.com
Nov 25, 2024 at 1:01 AM	Safeguarded Copy	–	prod-27-mariadb.rom.ihost.com
Nov 24, 2024 at 7:01 PM	Safeguarded Copy	–	prod-27-mariadb.rom.ihost.com
Nov 24, 2024 at 1:01 PM	Safeguarded Copy	–	prod-27-mariadb.rom.ihost.com
Nov 24, 2024 at 7:01 AM	Safeguarded Copy	✓ Nov 25, 2024 at 11:32 AM	prod-27-mariadb.rom.ihost.com
Nov 24, 2024 at 4:02 AM	Backup	–	test-82-mariadb.rom.ihost.com

Items per page: 10 | 1–10 of 89 items | 1 | 1 of 9 pages

IBM Storage Defender

Experience true resilience with IBM Storage Defender

Defender Essentials has the capabilities needed for true data resilience
Gain the benefits of the following:

- Enhanced security: Multilayered AI threat detection together with Immutable snapshots
- Improved performance: Streamlined recovery workflows and reduced RTO/RPO
- Simplified management: Centralized resiliency control with Storage Insights Pro
- Cost-effective: Leverage existing infrastructure and reduce operational overhead
- Compliance: Monitor policy requirements and threats in one place

Save your enterprise lost revenue and time when ransomware attacks

Modern Data Storage Challenges: A Growing Concern

- Data Volumes: The exponential growth of data requires scalable and efficient storage solutions.
- Sophisticated Threat Actors: Cybercriminals are using advanced tactics to breach systems and compromise sensitive data.
- Complexity: Managing multiple data sources, hybrid environments, and compliance requirements adds to operational difficulty.
- Regulations: Stringent legal and compliance requirements demand organizations to implement robust data protection strategies.
- Punitive Fines & Legal Jeopardy: Failing to comply with regulations can result in hefty fines and legal consequences.
- Response Coordination: In the event of a security incident, swift and effective response coordination is crucial.
- Business Continuity and Recovery: Ensuring that operations can continue despite disruptions is essential for organizational resilience.

How can your data storage survive this?

IBM Storage Defender provide an integrated approach to data protection, leveraging AI, automation, and proactive threat detection to safeguard critical data assets. By addressing these challenges, organizations can enhance security, ensure compliance, and maintain business continuity in an ever-evolving digital world.

Here’s what you get with Defender Essentials

Data Resilience Service Portal

The Data Resilience Service portal serves as a central solution for managing users and permissions. It integrates connection managers, offering multi-site visibility, and aggregates threats while dispatching alerts. The portal triggers proactive SGC on affected arrays and initiates recovery group restores to quickly bring systems back online.

IBM Storage Defender

Connection Manager

The Connection Manager integrates on-site resources with a service that proxies command and control for the solution. It supports VMware, physical, or other hypervisor deployments via OVA or ISO installer. Only metadata is sent to the SaaS portal, while all backup data stays local.

Defender Sensors

Defender Sensors install on critical RedHat, SUSE, and Ubuntu VMware workloads. They provide near real-time file system threat monitoring with minimal resource usage (under 5%), augmenting array-based ransomware detection with additional detection layers.

Clean Room

The Clean Room provides a safe, isolated location for recoveries, testing, and validation. It is designed to prevent malware escape and isolation to avoid infection during recovery or production processes.

Integration that extends value: IBM Storage Defender

Value of defend your data with IBM

- Enhanced visibility and control
- Leverage existing infrastructure
- Centralized data resiliency management
- Automated and coordinated threat response
- Bring Security, Storage, and IT Ops together to speed attack incident response

Automated SGC on detection

Multiple Layers of Alerts

Alerts are monitored across several layers. A missed heartbeat from the Defender Sensor or storage (via SI Pro) opens a case and raises suspicion.

Malware Detection - FlashSystem and SI Pro

When malware is detected, IBM FlashSystem Ransomware Threat Detection and SI Pro send alerts to Defender. Defender then reaches out to the array and triggers a proactive Safeguarded Copy, quickly containing the damage.

Malware Detection - Defender Sensors

IBM Defender Sensors detect data corruption in the VM filesystem and raise alerts on Defender's open case screen.