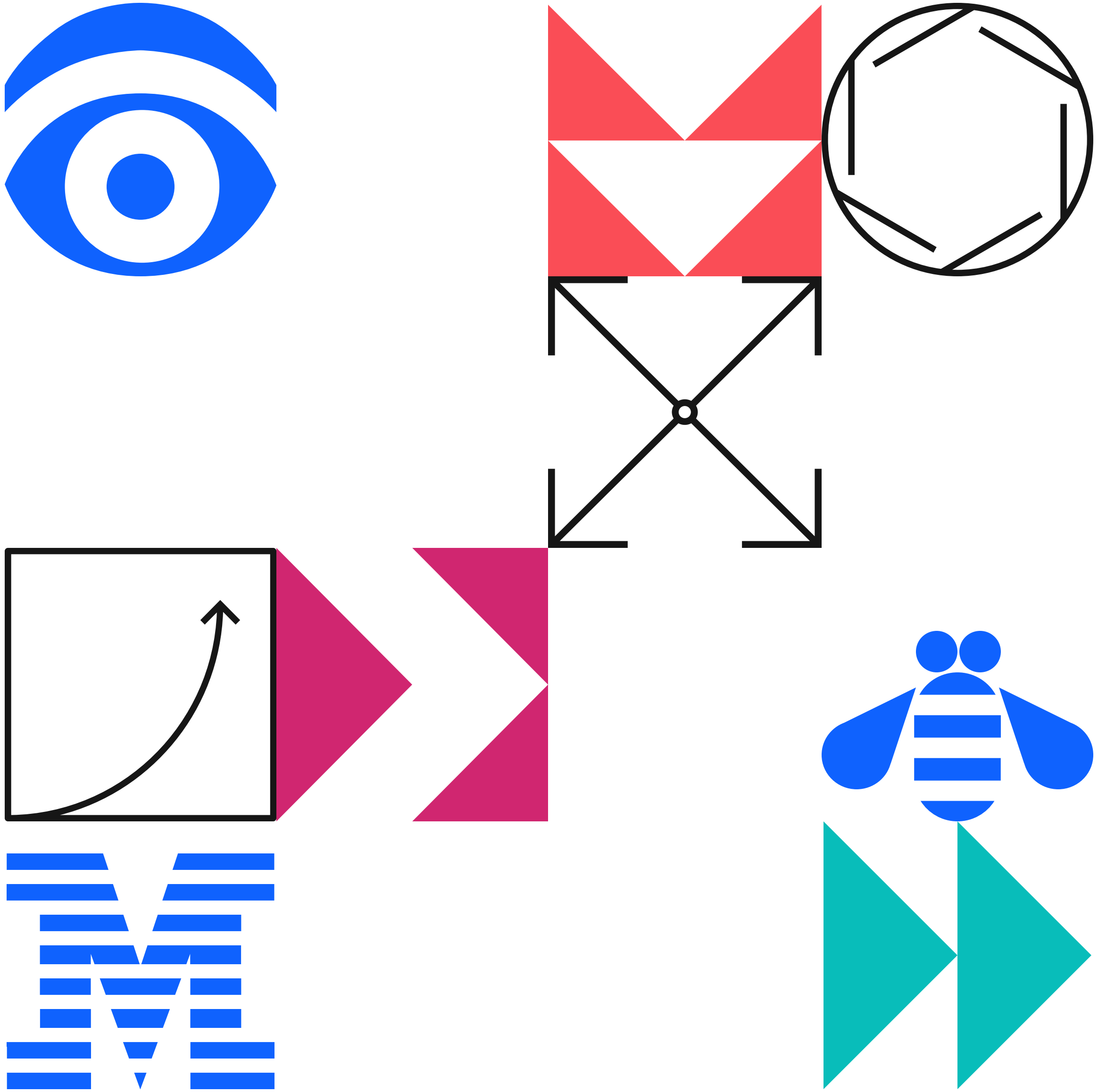
IBM **Storage Defender**
Data Resiliency Service



Colin Dawson

Senior Technical Staff Member &
IBM Storage Defender Development Architect

Disclaimer

This information is provided on an "AS IS" basis without warranty of any kind, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Some jurisdictions do not allow disclaimers of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

This information is provided for information purposes only as a high-level overview of possible future products. PRODUCT SPECIFICATIONS, ANNOUNCE DATES, AND OTHER INFORMATION CONTAINED HEREIN ARE SUBJECT TO CHANGE AND WITHDRAWAL WITHOUT NOTICE.

IBM's statements regarding its plans, directions, and intent are subject to change or withdrawal without notice at IBM's sole discretion. Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision. The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.

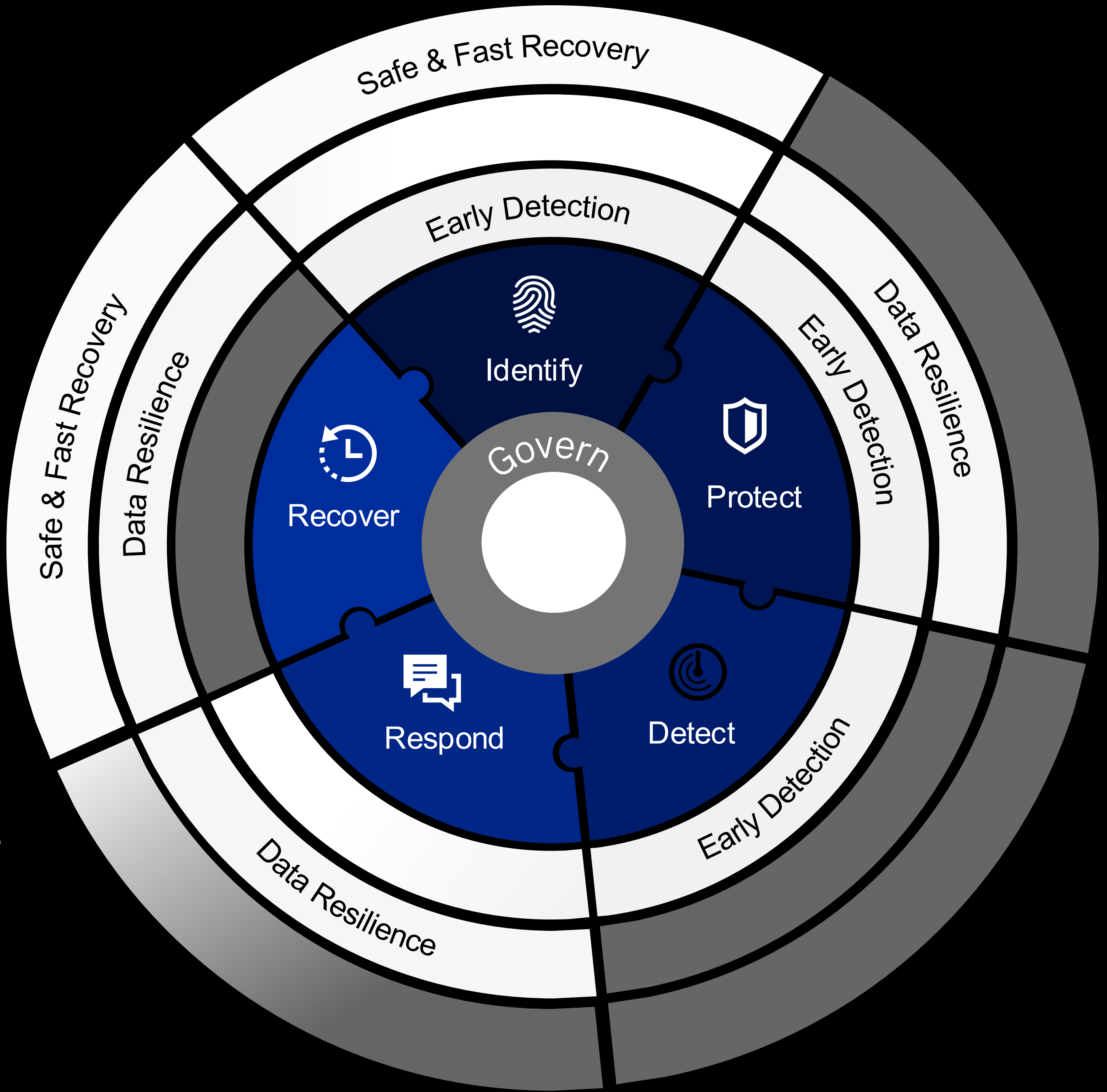
IBM reserves the right to change product specifications and offerings at any time without notice. This publication could include technical inaccuracies or typographical errors. References herein to IBM products and services do not imply that IBM intends to make them available in all countries.

What is Cyber Storage?

Early Threat Detection helps detect and prevent attacks in your environment

Data Resilience & Compliance ensures your data is being backed up

Safe & Fast Recovery can then restore your business as quickly as possible



What is IBM doing?

Bringing together capabilities from both storage and backup systems.

- Ensures fastest recovery of critical workloads
- Implements a layer approach to data management to minimize data loss
- Leveraging guarantees and sustainable solutions

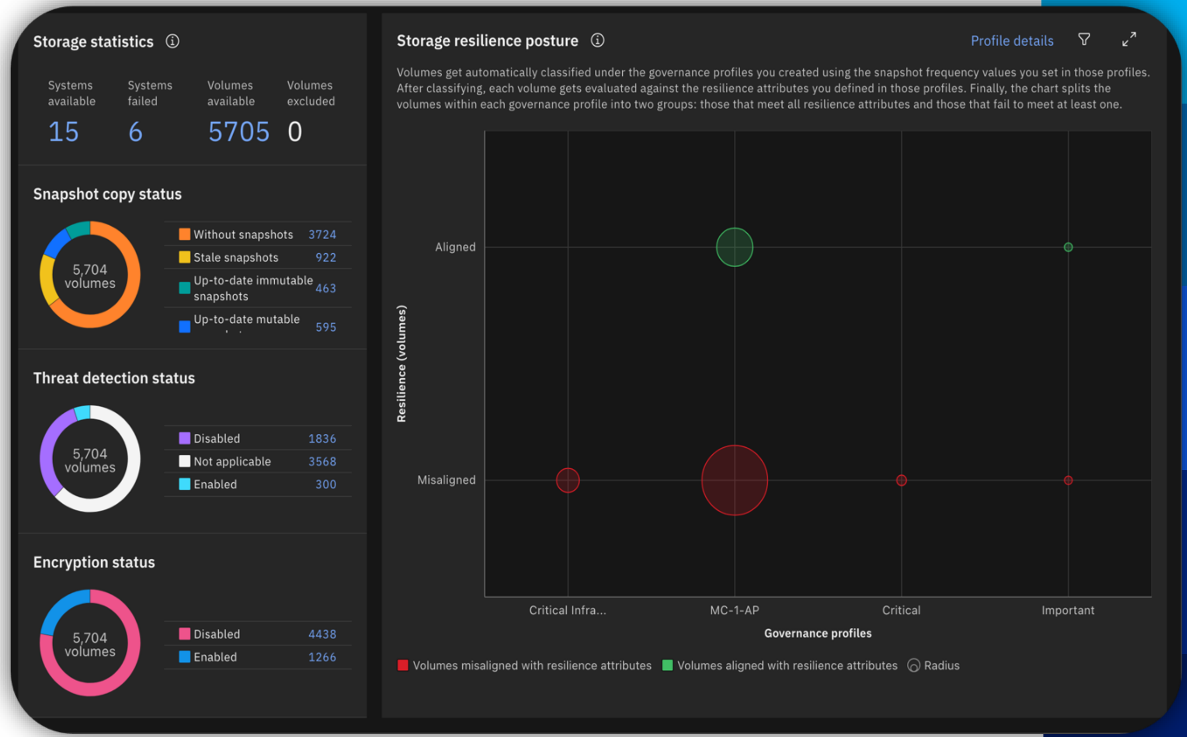
Integrating with IBM Security to provide end-to-end solutions from a single vendor

- Leverage market leading solutions in an integrated model
- Validate copies and mounted data in a clean room environment

Shifting detection left. Implementing layers of scanning to detect threats early.

- Multiple layers of anomaly and malware detection to reduce dormant threats
- Potentially detect malware and corruption before SOC
- Identify clean “safe” copies based on detected anomalies

IBM **Storage Defender** - Data Resiliency Service



Storage statistics ⓘ

Systems available	Systems failed	Volumes available	Volumes excluded
15	6	5705	0

Snapshot copy status

5,704 volumes

Without snapshots	3724
Stale snapshots	922
Up-to-date immutable snapshots	463
Up-to-date mutable	595

Threat detection status

5,704 volumes

Disabled	1836
Not applicable	3568
Enabled	300

Encryption status

5,704 volumes

Disabled	4438
Enabled	1266

Storage resilience posture ⓘ

Volumes get automatically classified under the governance profiles you created using the snapshot frequency values you set in those profiles. After classifying, each volume gets evaluated against the resilience attributes you defined in those profiles. Finally, the chart splits the volumes within each governance profile into two groups: those that meet all resilience attributes and those that fail to meet at least one.

Dashboard

- Data recoverability across workloads
- Actionable insights on meeting recovery and resiliency standards

IBM and 3rd party data platforms

- IBM FlashSystem, Dell PowerMax, and Pure
- IBM Defender Data Protect, Storage Protect

Alert on Risks or Red Flags

- Alerts on risks to meeting compliance
- Detect threats early through deployable anomaly detection agents

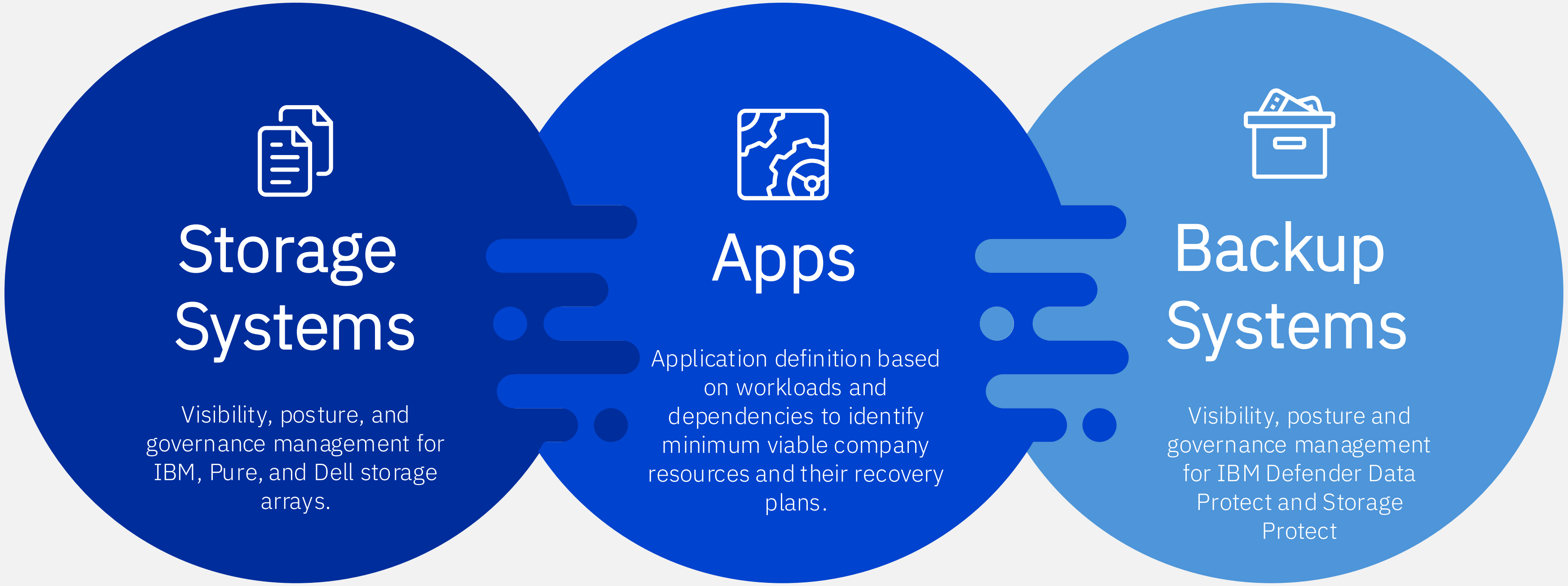
Policy Automation

- Define applications and recovery groups that map to minimum viable company that spans disparate infra and workloads
- Fix governance, SLA, and compliance discrepancies at scale

Drive Policy and Application Consistency

- Highlight configuration inconsistencies
- Application aware policies covering software snapshots, hardware snapshots, backups, tape and cloud tiered data

IBM Storage Defender – Data Resiliency Service



Storage Systems

Visibility, posture, and governance management for IBM, Pure, and Dell storage arrays.

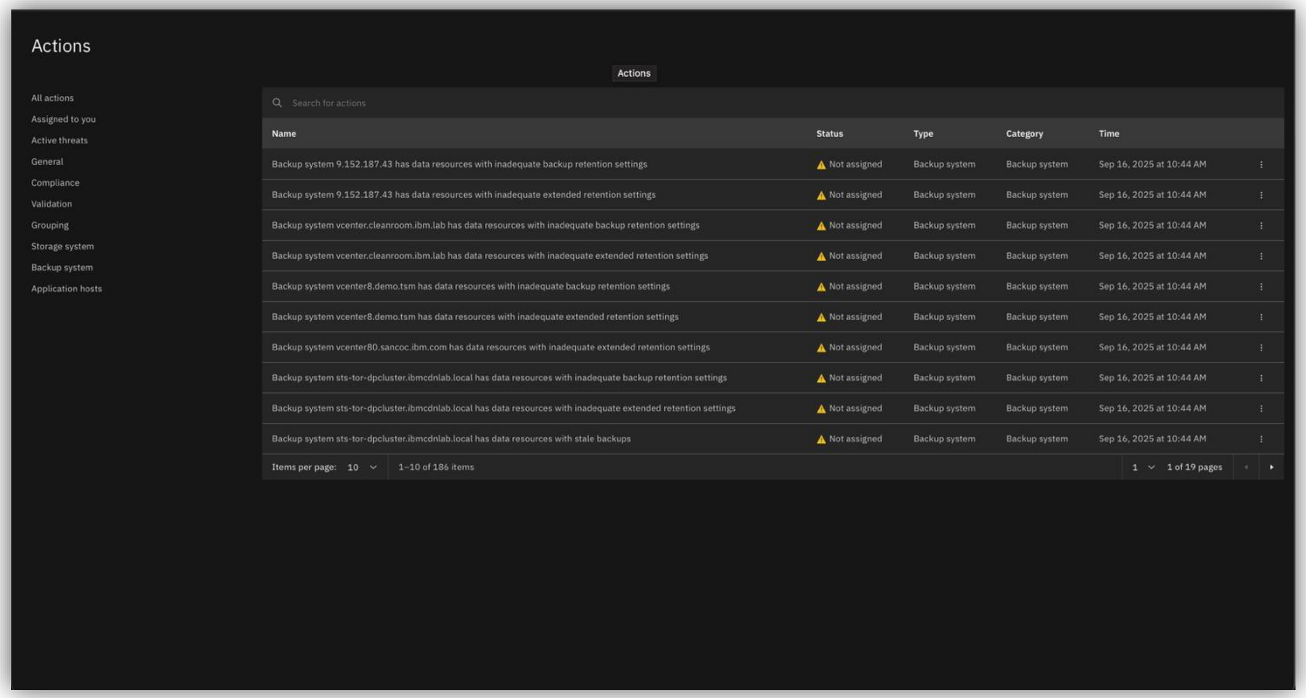
Apps

Application definition based on workloads and dependencies to identify minimum viable company resources and their recovery plans.

Backup Systems

Visibility, posture and governance management for IBM Defender Data Protect and Storage Protect

Take Actions with DRS



Name	Status	Type	Category	Time
Backup system 9.152.187.43 has data resources with inadequate backup retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system 9.152.187.43 has data resources with inadequate extended retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system vcenter.cleanroom.ibm.lab has data resources with inadequate backup retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system vcenter.cleanroom.ibm.lab has data resources with inadequate extended retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system vcenter8.demo.tsm has data resources with inadequate backup retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system vcenter8.demo.tsm has data resources with inadequate extended retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system vcenter80.sancoc.ibm.com has data resources with inadequate extended retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system sts-tor-dpcluster.ibmcdnlab.local has data resources with inadequate backup retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system sts-tor-dpcluster.ibmcdnlab.local has data resources with inadequate extended retention settings	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM
Backup system sts-tor-dpcluster.ibmcdnlab.local has data resources with stale backups	⚠ Not assigned	Backup system	Backup system	Sep 16, 2025 at 10:44 AM

Items per page: 10 1–10 of 186 items 1 1 of 19 pages

DRS streamlines incident and misconfiguration handling by aligning recovery point policies with governance requirements, ensuring compliance and data protection. Additionally, it provides task assignment and workflow management features, allowing teams to coordinate and remediate issues efficiently while maintaining operational resilience.

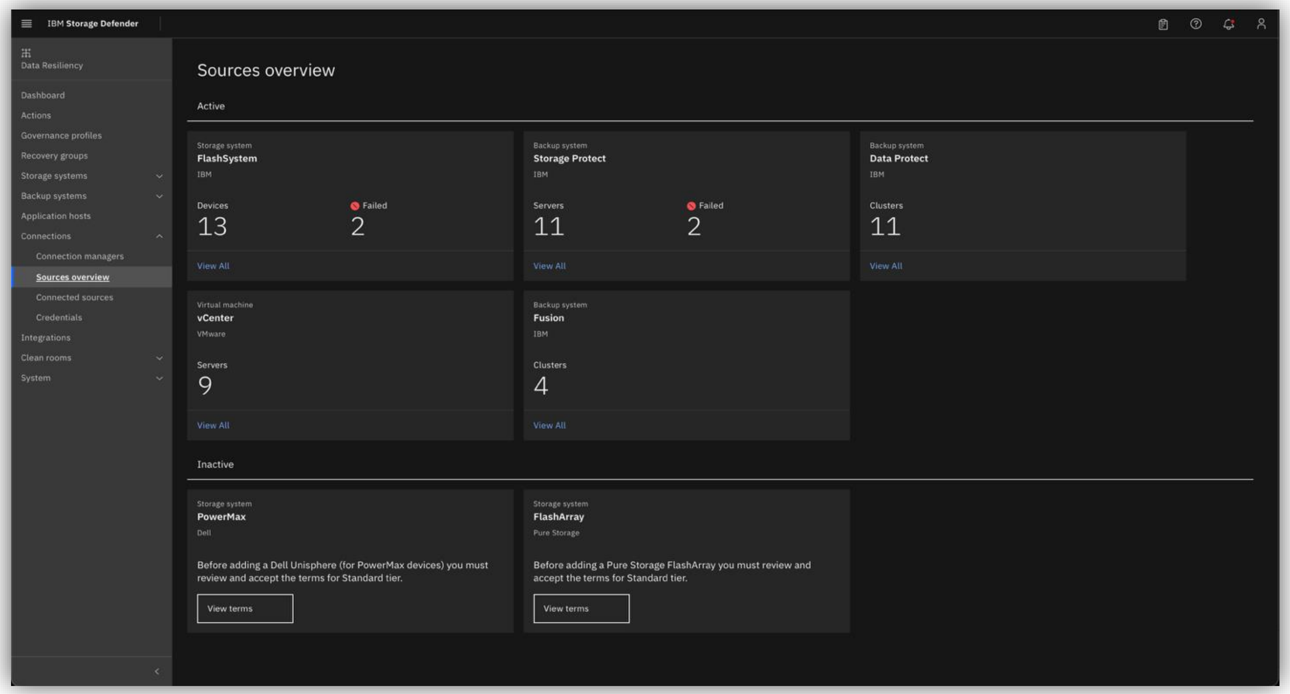
Today

- **Define governance policies** for your storage and backup systems that follow enterprise goals as well as industry frameworks or policies.
- Proactively **test your recovery points** and ensure they are ready for recovery when needed.
- Respond to anomalies and threats with **granularity.**

Vision

- Drive additional actions for both **proactive and reactive operations.**
- Map actions to ensure **regulatory and compliance** use cases are met.
- Enhance and **prioritize actions** with AI insights and intelligence.

Bridge Silos with DRS



Sources overview

Active

Storage system
FlashSystem
IBM
Devices 13
Failed 2
View All

Backup system
Storage Protect
IBM
Servers 11
Failed 2
View All

Backup system
Data Protect
IBM
Clusters 11
View All

Virtual machine
vCenter
VMware
Servers 9
View All

Backup system
Fusion
IBM
Clusters 4
View All

Inactive

Storage system
PowerMax
Dell
Before adding a Dell Unisphere (for PowerMax devices) you must review and accept the terms for Standard tier.
View terms

Storage system
FlashArray
Pure Storage
Before adding a Pure Storage FlashArray you must review and accept the terms for Standard tier.
View terms

DRS bridges storage and backup silos by providing an end-to-end view across enterprise storage systems and platforms. It unifies fragmented environments into a single pane of visibility, enabling teams to monitor, manage, and optimize storage and backup resources, governance, and resiliency holistically. This integrated approach improves efficiency, reduces complexity, and ensures data resilience across the entire infrastructure.

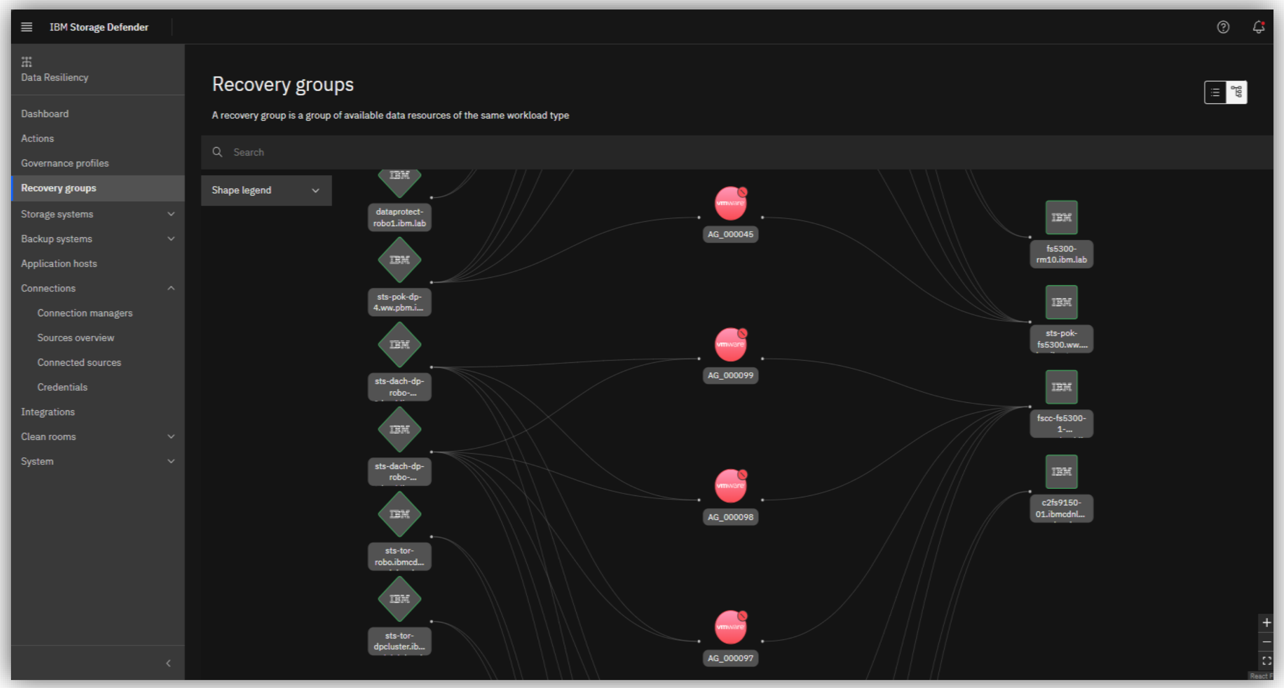
Today

- **Reduce gaps** between security, storage, and backup systems.
- Connect different sources from multiple vendors like **IBM, Dell, and Pure.**
- Recover efficiently from the latest**, clean recovery points** available to you from across the enterprise.

Vision

- Bring in additional sources for **primary storage**
- Bring in additional sources for **backup storage**
- Support additional **workloads**

Visualize with DRS



Recovery groups

A recovery group is a group of available data resources of the same workload type

DRS visualizes connected sources enabling users to see relationships, groupings, and dependencies across their environment. By mapping these connections, it highlights coverage gaps and strengthens visibility into protection and resiliency posture. This holistic view helps organizations identify risks, optimize defenses, and ensure comprehensive resilience across their systems.

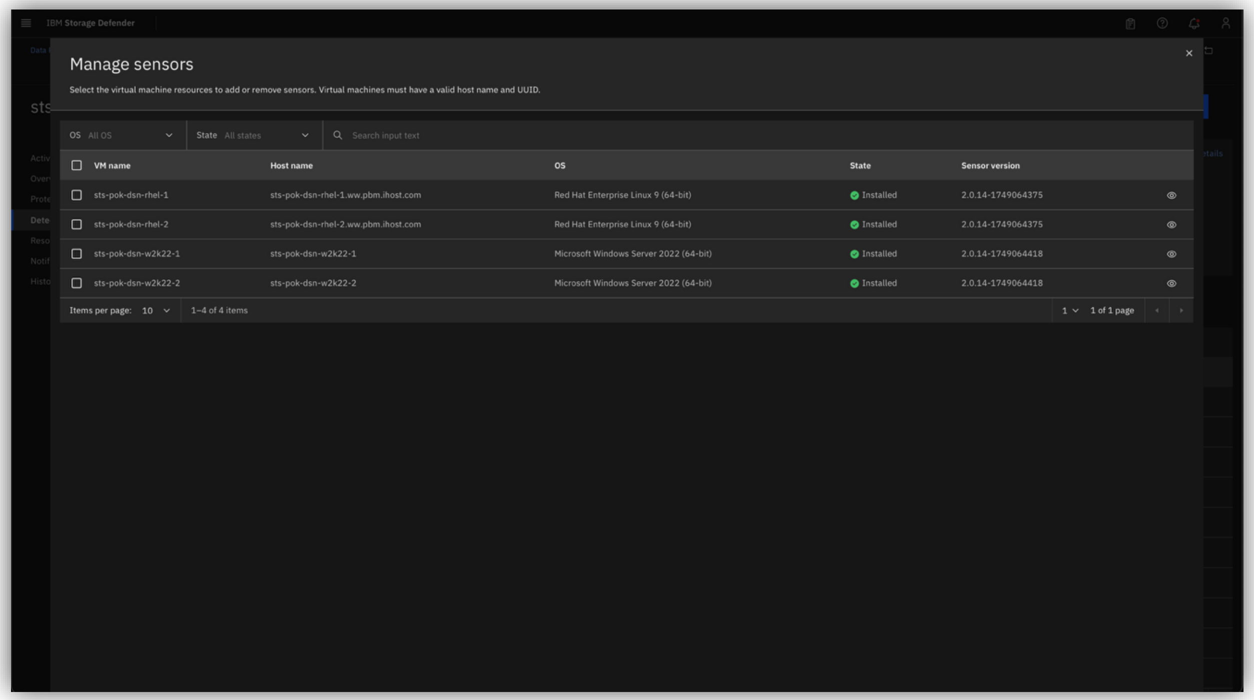
Today

- Highlight **protection gaps** across the environment.
- Automatically **group and map relationships** between common resources across primary storage, backup and virtual machines.
- Optimize copies by identifying objects and copies that have been over or under provisioned.

Vision

- Visualize **additional objects** like vCenters, volumes, datastores…
- Visualize **additional relationships** like replication and HA.
- Visualize **topology and connections** of systems and sources

Deploy Sensors with DRS



Manage sensors

Select the virtual machine resources to add or remove sensors. Virtual machines must have a valid host name and UUID.

OS: All OS | State: All states | Search input text

☐	VM name	Host name	OS	State	Sensor version
☐	sts-pok-dsn-rhel-1	sts-pok-dsn-rhel-1.ww.pbm.ihost.com	Red Hat Enterprise Linux 9 (64-bit)	✓ Installed	2.0.14-1749064375
☐	sts-pok-dsn-rhel-2	sts-pok-dsn-rhel-2.ww.pbm.ihost.com	Red Hat Enterprise Linux 9 (64-bit)	✓ Installed	2.0.14-1749064375
☐	sts-pok-dsn-w2k22-1	sts-pok-dsn-w2k22-1	Microsoft Windows Server 2022 (64-bit)	✓ Installed	2.0.14-1749064418
☐	sts-pok-dsn-w2k22-2	sts-pok-dsn-w2k22-2	Microsoft Windows Server 2022 (64-bit)	✓ Installed	2.0.14-1749064418

Items per page: 10 | 1–4 of 4 items | 1 | 1 of 1 page

DRS enables the deployment of lightweight sensors within VMware virtual machines to continuously monitor memory and file systems. Leveraging AI and ML, these sensors detect anomalies that may indicate corruption or emerging threats and generate real-time alerts to help teams investigate and respond quickly. This proactive approach enhances threat detection and safeguards the integrity of virtualized environments.

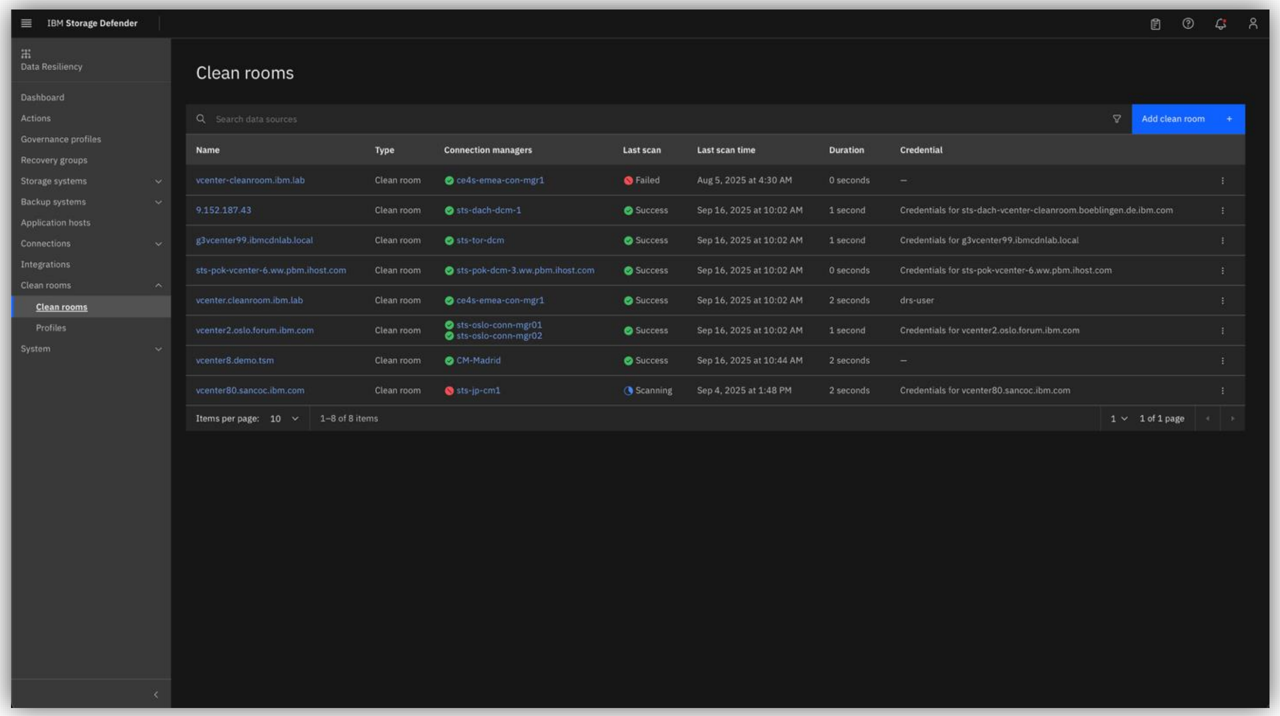
Today

- Ability to **deploy anomaly sensors** at the edge, directly into VMs.
- **Detect anomalous changes** within individual VMs leveraging AI and ML.
- Support for **Linux** and **Windows VMs.**

Vision

- Deploy Sensors across a **broader set of VMware Operating Systems**
- Deploy Defender sensors on **more platforms and file systems** like Power, Fusion, and Scale file systems.
- **Exfiltration sensors** to detect patterns that are related to data exfiltration.

Leverage Clean Rooms with DRS



Clean rooms

Name	Type	Connection managers	Last scan	Last scan time	Duration	Credential
vcenter-cleanroom.ibm.lab	Clean room	ce4s-emea-con-mgr1	Failed	Aug 5, 2025 at 4:30 AM	0 seconds	–
9.152.187.43	Clean room	sts-dach-dcm-1	Success	Sep 16, 2025 at 10:02 AM	1 second	Credentials for sts-dach-vcenter-cleanroom.boeblingen.de.ibm.com
g3vcenter99.ibmcdnlab.local	Clean room	sts-tor-dcm	Success	Sep 16, 2025 at 10:02 AM	1 second	Credentials for g3vcenter99.ibmcdnlab.local
sts-pok-vcenter-6.ww.pbm.ihost.com	Clean room	sts-pok-dcm-3.ww.pbm.ihost.com	Success	Sep 16, 2025 at 10:02 AM	0 seconds	Credentials for sts-pok-vcenter-6.ww.pbm.ihost.com
vcenter.cleanroom.ibm.lab	Clean room	ce4s-emea-con-mgr1	Success	Sep 16, 2025 at 10:02 AM	2 seconds	drs-user
vcenter2.oslo.forum.ibm.com	Clean room	sts-oslo-conn-mgr01 sts-oslo-conn-mgr02	Success	Sep 16, 2025 at 10:02 AM	1 second	Credentials for vcenter2.oslo.forum.ibm.com
vcenter8.demo.tsm	Clean room	CM-Madrid	Success	Sep 16, 2025 at 10:44 AM	2 seconds	–
vcenter80.sancoc.ibm.com	Clean room	sts-jp-cm1	Scanning	Sep 4, 2025 at 1:48 PM	2 seconds	Credentials for vcenter80.sancoc.ibm.com

Items per page: 10 | 1–8 of 8 items | 1 | 1 of 1 page

DRS allows organizations to define and connect an isolated recovery environment, or clean room, to safely restore data for analysis and forensics. By leveraging this controlled environment, teams can investigate threats, validate data integrity, and perform recovery testing without risking the spread of malware or corruption. This approach strengthens security and ensures a trusted path to resilient recovery.

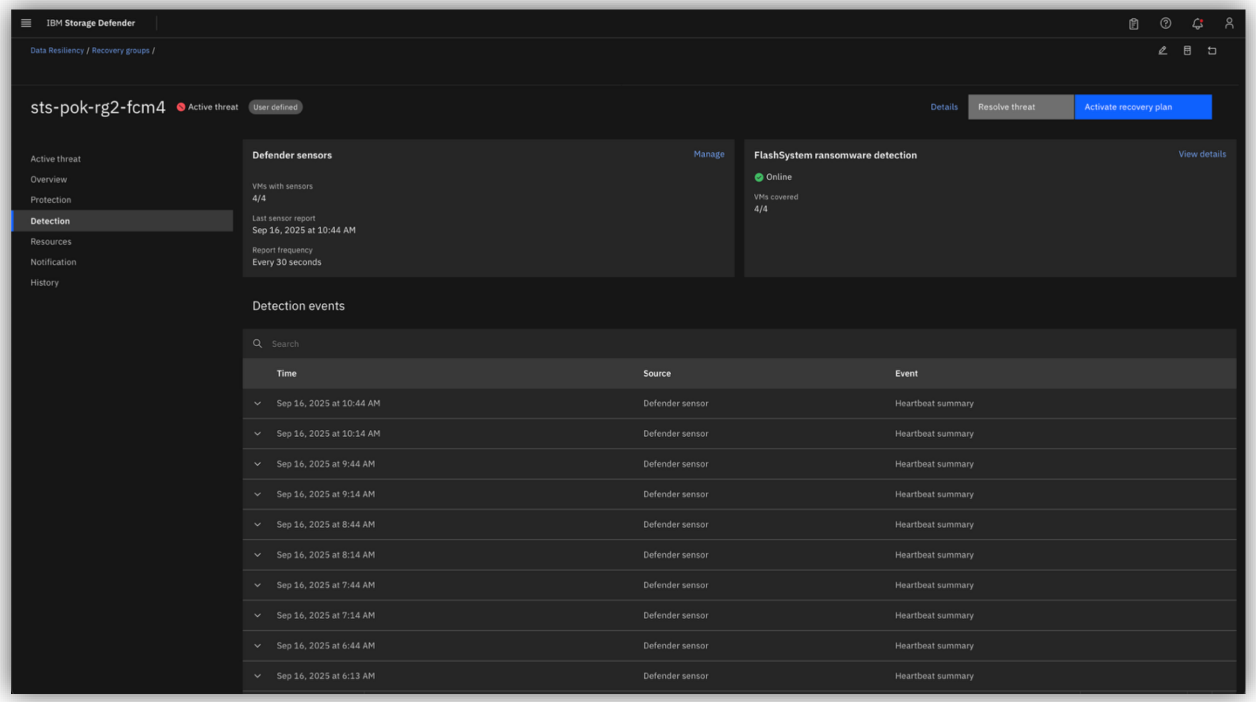
Today

- Deploy isolated environments for **validation of workloads** in an air-gaped, safe space.
- Leverage automation platforms like ansible to **facilitate complex testing** and return-to-production workflows.
- **Re-use existing security tools** like AV scanners to scan data in IRE.

Vision

- Deploy Isolated Scan Environments leveraging Index Engines – Cyber Sense to **scan workloads agnostically**.
- **Automate scanning and validation** of workloads across the storage estate.
- Enable **bring-your-own-scanner** for ISEs.

Aggregate Alerts with DRS



sts-pok-rg2-fcm4

Defender sensors

VMs with sensors
4/4

Last sensor report
Sep 16, 2025 at 10:44 AM

Report frequency
Every 30 seconds

FlashSystem ransomware detection

● Online

VMs covered
4/4

Detection events

Time	Source	Event
Sep 16, 2025 at 10:44 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 10:14 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 9:44 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 9:14 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 8:44 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 8:14 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 7:44 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 7:14 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 6:44 AM	Defender sensor	Heartbeat summary
Sep 16, 2025 at 6:13 AM	Defender sensor	Heartbeat summary

DRS centralizes alert management by ingesting alerts from multiple sources, including its deployed sensors and real-time threat detection within primary storage arrays. By consolidating these signals into a single view, it streamlines analysis, improves decision-making, and accelerates response actions. This unified approach enhances visibility and ensures faster, more effective threat mitigation across the environment.

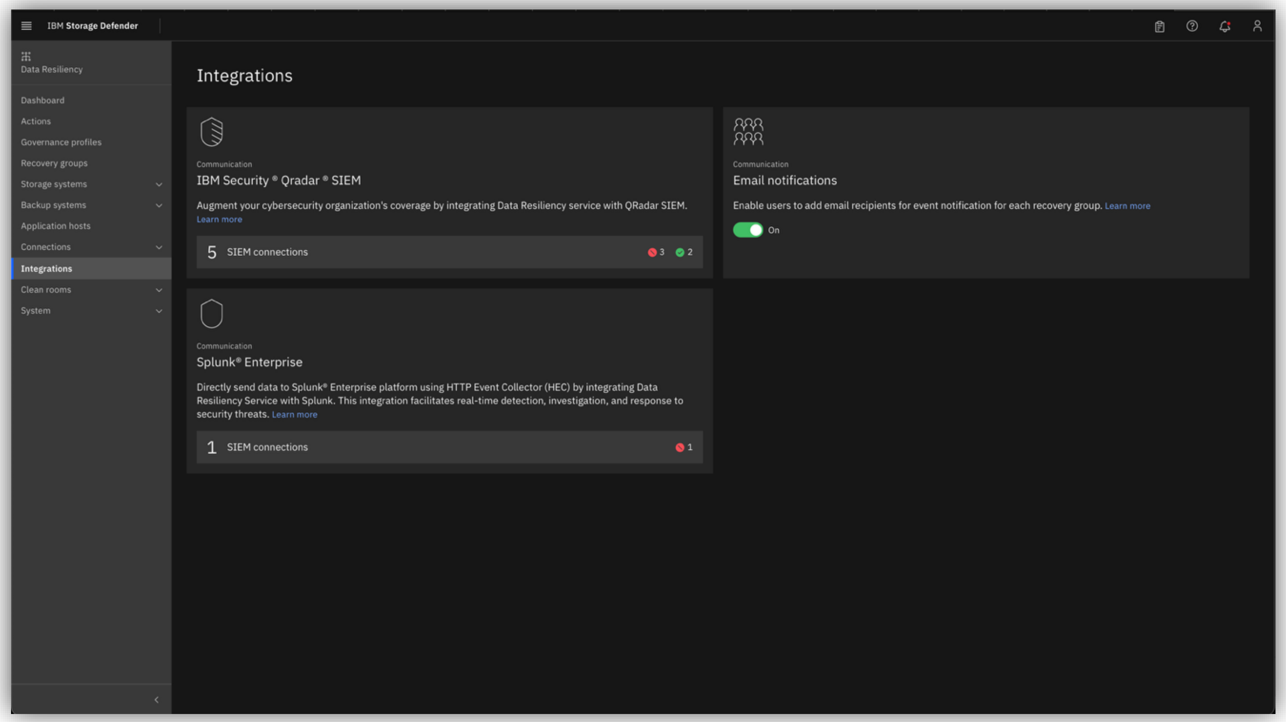
Today

- Ingest alerts from multiple sources to **identify threats at a wider scope**.
- Deployed Defender Sensors and FCM Anomaly detection work hand-in-hand to **detect anomalies and threats** in the environment.
- Leverage different technologies along different points in the data path to **detect threats with more fidelity.**

Vision

- Ingest alerts from **more sources** like Defender Data Protect and Defender Sentinel.
- Ingest **security bulletins** for most up to data date on threats and attack patterns.
- **Reduce false positives**, define **blast radius**, and create **threat timelines** to assist with response.

Integrate with DRS



Integrations

Communication
IBM Security ® Qradar ® SIEM

Augment your cybersecurity organization's coverage by integrating Data Resiliency service with QRadar SIEM. Learn more

5 SIEM connections ● 3 ✓ 2

Communication
Email notifications

Enable users to add email recipients for event notification for each recovery group. Learn more

On

Communication
Splunk® Enterprise

Directly send data to Splunk® Enterprise platform using HTTP Event Collector (HEC) by integrating Data Resiliency Service with Splunk. This integration facilitates real-time detection, investigation, and response to security threats. Learn more

1 SIEM connections ● 1

DRS integrates with SIEM solutions to seamlessly feed alerts and events from its cyber resiliency platform into existing security operations workflows. By doing so, it enables security teams to detect potential threats faster, correlate them with broader enterprise events, and take timely action. This integration strengthens threat visibility and enhances overall security posture.

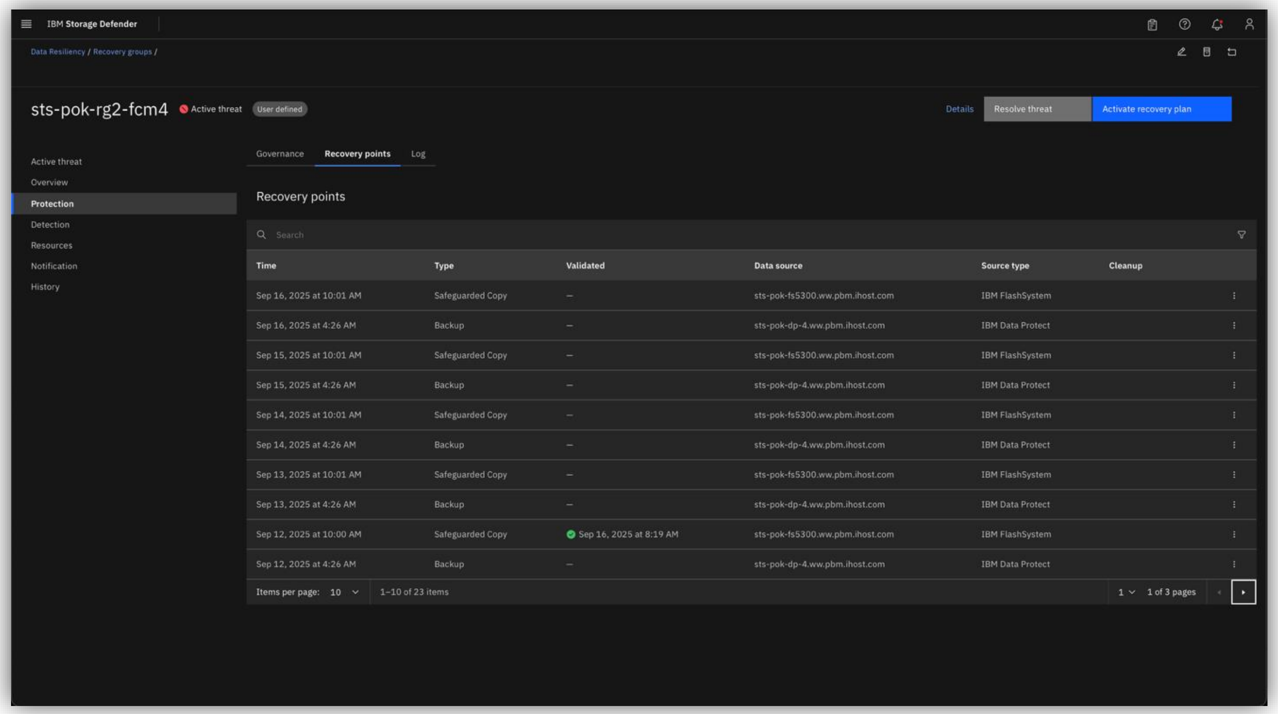
Today

- **Send logs and alerts to security teams** through integration of SIEM solutions including Qradar and Splunk.
- Receive enhanced alerting from IBM Storage Insights Pro for **aggregation** with other sensors.
- Integrate with your email provide to **alert users** and other personas about threats and other actions.

Vision

- Integrate with other platforms and applications like ServiceNow and add easier ways to integrate like **webhooks**.
- **Ingest data from SIEMs** and other security solutions to enhance Defender’s threat aggregation, threat timeline, and blast radius capabilities.
- Leverage more automation and application tools like **Ansible, Terraform, and Turbonomic**

Curate Recovery Points with DRS



Time	Type	Validated	Data source	Source type	Cleanup
Sep 16, 2025 at 10:01 AM	Safeguarded Copy	–	sts-pok-fs5300.ww.pbm.ihost.com	IBM FlashSystem	
Sep 16, 2025 at 4:26 AM	Backup	–	sts-pok-dp-4.ww.pbm.ihost.com	IBM Data Protect	
Sep 15, 2025 at 10:01 AM	Safeguarded Copy	–	sts-pok-fs5300.ww.pbm.ihost.com	IBM FlashSystem	
Sep 15, 2025 at 4:26 AM	Backup	–	sts-pok-dp-4.ww.pbm.ihost.com	IBM Data Protect	
Sep 14, 2025 at 10:01 AM	Safeguarded Copy	–	sts-pok-fs5300.ww.pbm.ihost.com	IBM FlashSystem	
Sep 14, 2025 at 4:26 AM	Backup	–	sts-pok-dp-4.ww.pbm.ihost.com	IBM Data Protect	
Sep 13, 2025 at 10:01 AM	Safeguarded Copy	–	sts-pok-fs5300.ww.pbm.ihost.com	IBM FlashSystem	
Sep 13, 2025 at 4:26 AM	Backup	–	sts-pok-dp-4.ww.pbm.ihost.com	IBM Data Protect	
Sep 12, 2025 at 10:00 AM	Safeguarded Copy	✓ Sep 16, 2025 at 8:19 AM	sts-pok-fs5300.ww.pbm.ihost.com	IBM FlashSystem	
Sep 12, 2025 at 4:26 AM	Backup	–	sts-pok-dp-4.ww.pbm.ihost.com	IBM Data Protect	

DRS curates recovery points by aggregating them from multiple systems, including both primary and backup storage across different vendors and platforms. This creates a single source of truth to identify the best possible recovery point, optimizing for stronger RPO and RTO. Additionally, it provides visibility into whether recovery points have been validated or scanned, ensuring confidence and integrity in data restoration.

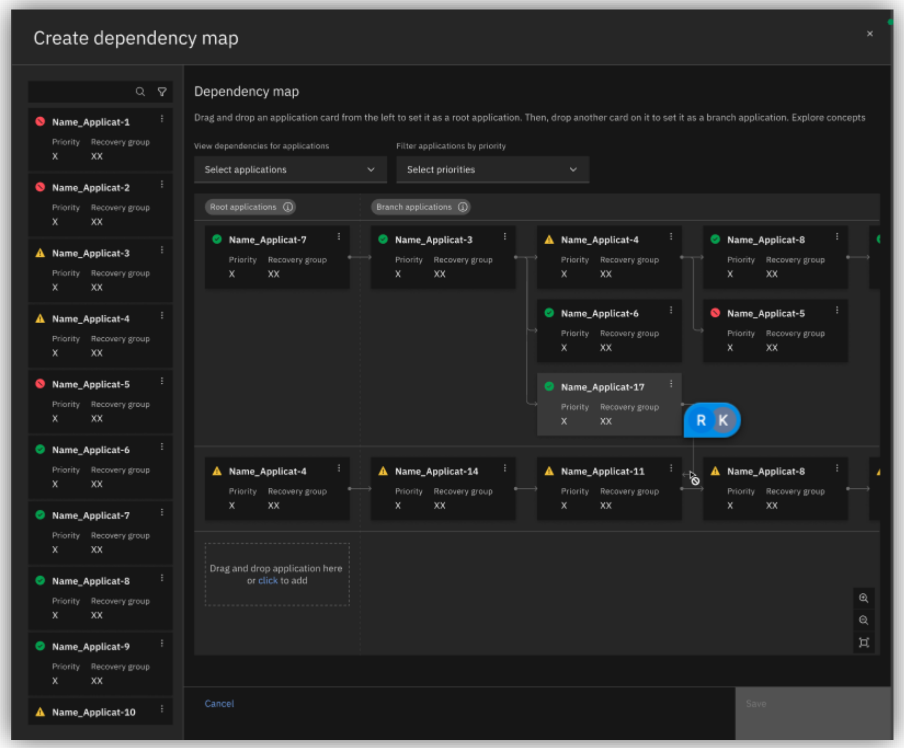
Today

- **Correlate** recovery points within Recovery Groups for a wide view of recovery points across the enterprise.
- Validate recovery points with **isolated recovery environments.**
- Mark validated recovery points as tested and valid for **response and planning**.

Vision

- Automatically **test recovery points** to validate them.
- **AI enhancements for prioritization** of scanning, validation, and restoration.
- Leverage **smart recovery plans** to identify best possible recovery path for workloads and applications.

Map Application Dependencies with DRS



Create dependency map

Dependency map

Drag and drop an application card from the left to set it as a root application. Then, drop another card on it to set it as a branch application. Explore concepts

View dependencies for applications: Select applications

Filter applications by priority: Select priorities

DRS provides rapid and actionable data resiliency insights across storage and backup systems, highlighting strengths, gaps, and potential risks. It delivers clear recommendations to address vulnerabilities, improve protection, and enhance recovery readiness. This visibility empowers organizations to proactively strengthen resiliency and ensure business continuity.

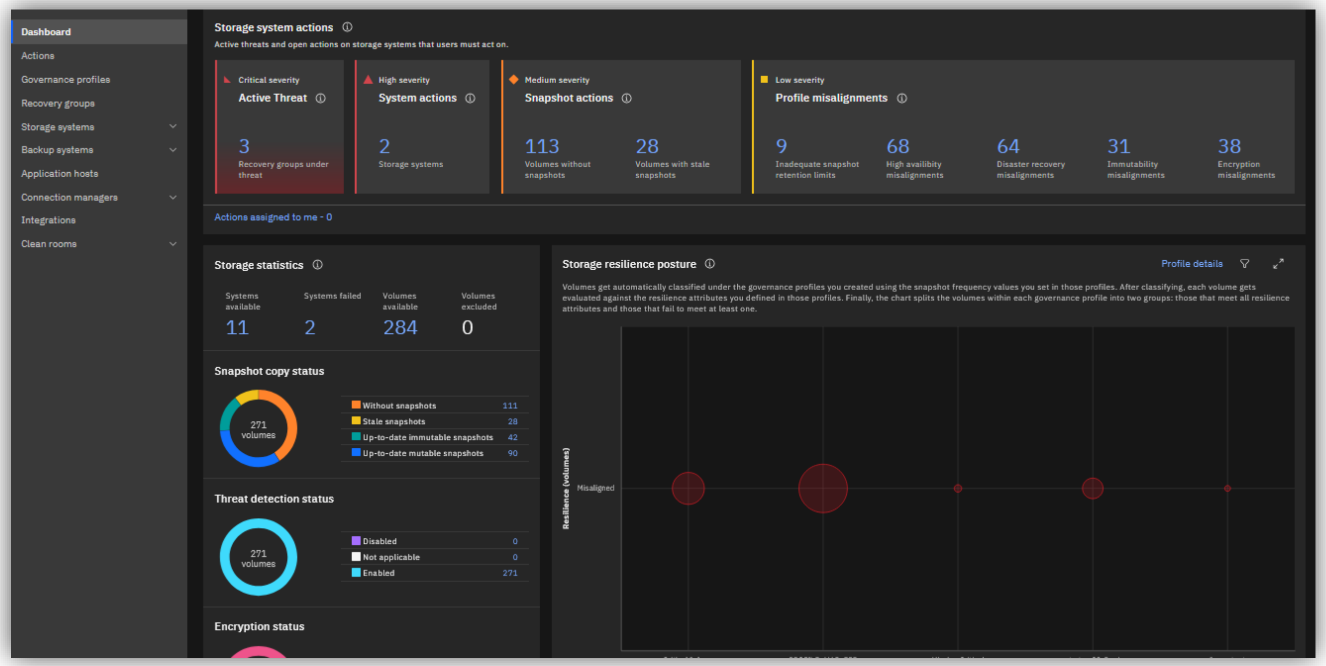
Today

- Bring together workloads that operate together, as an **Application**
- **Prioritise the recovery of workloads** within an Application, as well as the priority between Applications
- **Relate these Applications** to your business functions, and focus on bringing back your MINIMAL VIABLE COMPANY

Vision

- Downloadable **Recovery plans** that document applications, recovery points, and how to perform recovery. (support cyber event disconnect from internet)
- **Cached** recovery plans in data center (local) for ease of access and use for recovery.
- Offline recovery **automation** with recovery plans built using Ansible/Python. User provides input for which recovery point (timeframe) and recovery driven via automation.

Summarize with DRS



Storage system actions

Active threats and open actions on storage systems that users must act on.

Critical severity
Active Threat
3 Recovery groups under threat

High severity
System actions
2 Storage systems

Medium severity
Snapshot actions
113 Volumes without snapshots
28 Volumes with stale snapshots

Low severity
Profile misalignments
9 Inadequate snapshot retention limits
68 High availibity misalignments
64 Disaster recovery misalignments
31 Immutability misalignments
38 Encryption misalignments

Actions assigned to me - 0

Storage statistics

Systems available	Systems failed	Volumes available	Volumes excluded
11	2	284	0

Snapshot copy status

271 volumes

🟧 Without snapshots	111
🟨 Stale snapshots	28
🟩 Up-to-date immutable snapshots	42
🟦 Up-to-date mutable snapshots	90

Threat detection status

271 volumes

🟪 Disabled	0
⬜ Not applicable	0
🟦 Enabled	271

Encryption status

Storage resilience posture

Volumes get automatically classified under the governance profiles you created using the snapshot frequency values you set in those profiles. After classifying, each volume gets evaluated against the resilience attributes you defined in those profiles. Finally, the chart splits the volumes within each governance profile into two groups: those that meet all resilience attributes and those that fail to meet at least one.

DRS provides rapid and actionable data resiliency insights across storage and backup systems, highlighting strengths, gaps, and potential risks. It delivers clear recommendations to address vulnerabilities, improve protection, and enhance recovery readiness. This visibility empowers organizations to proactively strengthen resiliency and ensure business continuity.

Today

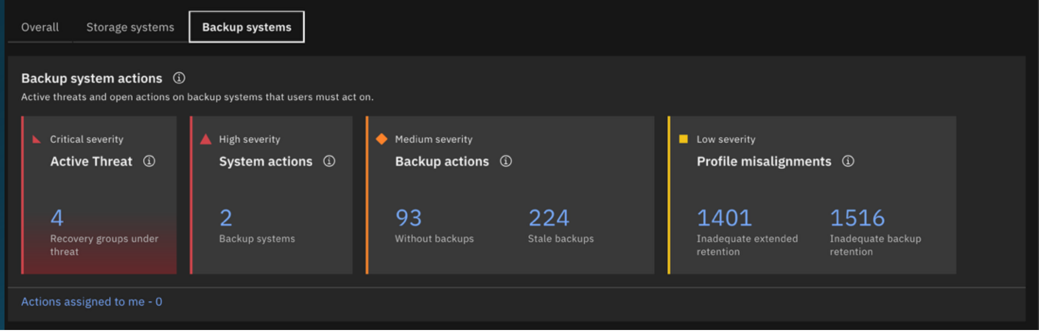
- Leverage targeted dashboards for the **CISO**, **primary systems** administrator, and **backup systems** administrators, delivered in 2Q25
- Quickly compare your storage environment against **industry best practices**.
- Visualize gaps and actions to im**prove or meet resiliency requirements** driven by the business or external policies.

Vision

- **Leverage AI and LLMs** to display data, drive actions, and summarize reports with granularity, on demand.
- Review **status of entire environment** across different sources, platforms, and sensors, in the cloud or on-premise
- **Customize view** based on persona, regulations, and needs.

Start your IBM **Storage Defender DRS** Trial

Gain **visibility to your storage environment** and gain valuable insights into its resiliency posture and governance metrics to meet business goals and regulations.



Overall | Storage systems | **Backup systems**

Backup system actions ⓘ

Active threats and open actions on backup systems that users must act on.

Critical severity **Active Threat** ⓘ	High severity **System actions** ⓘ	Medium severity **Backup actions** ⓘ		Low severity **Profile misalignments** ⓘ	
4 Recovery groups under threat	2 Backup systems	93 Without backups	224 Stale backups	1401 Inadequate extended retention	1516 Inadequate backup retention

Actions assigned to me - 0

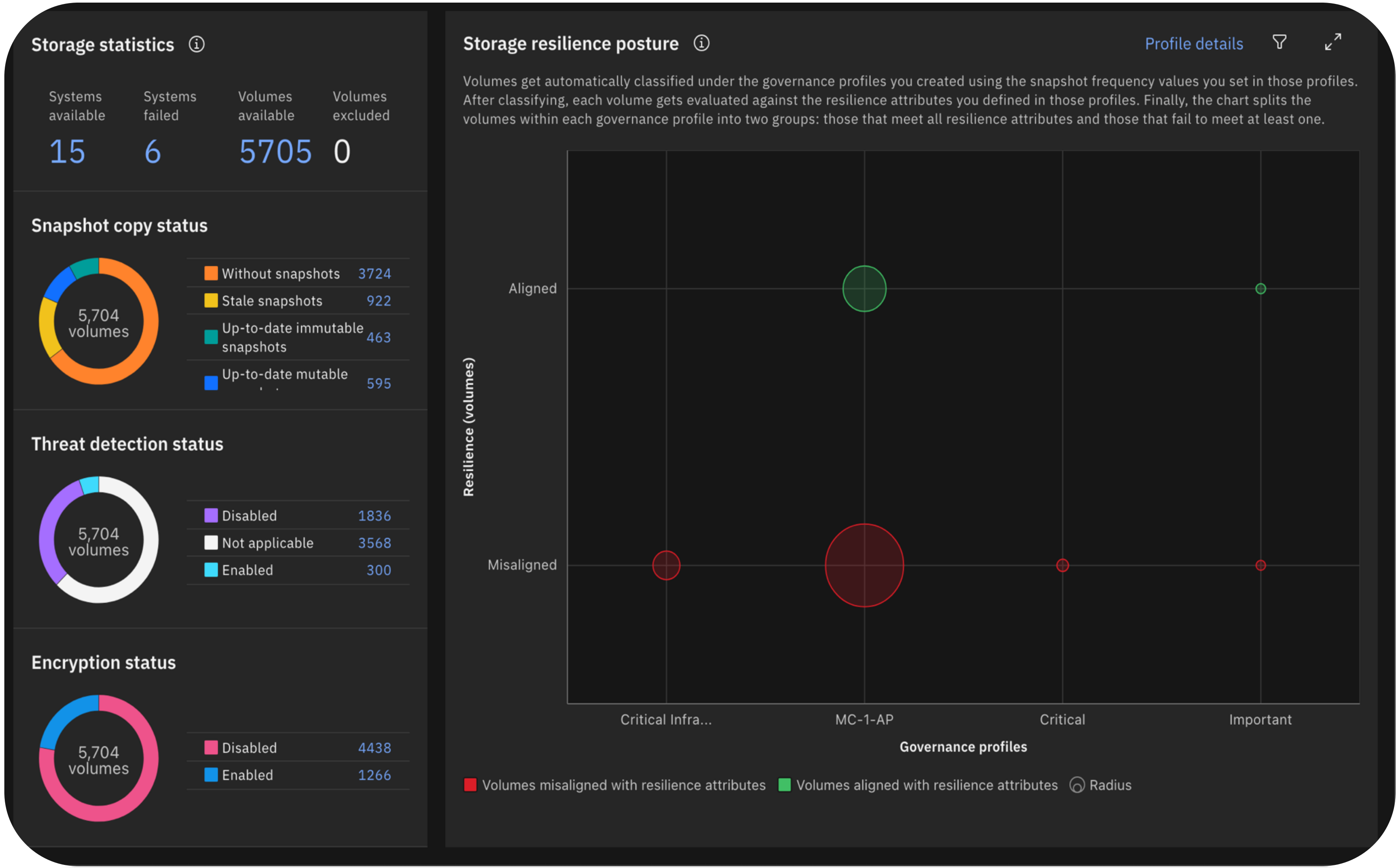
https://ibm.biz/DRSTRIAL

^ Start 60 Day Trial

Watch this short Demo to get a quick look at the solution!

Making the tool work for you

Take action and improve based on Defender's recommendations and findings. Visualize your storage and backup systems while gaining valuable insights about governance and posture.



Storage statistics ⓘ

Systems available	Systems failed	Volumes available	Volumes excluded
15	6	5705	0

Snapshot copy status

🟧 Without snapshots	3724
🟨 Stale snapshots	922
🟩 Up-to-date immutable snapshots	463
🟦 Up-to-date mutable	595

Threat detection status

🟪 Disabled	1836
⬜ Not applicable	3568
🟦 Enabled	300

Encryption status

🟥 Disabled	4438
🟦 Enabled	1266

Storage resilience posture ⓘ

Profile details

Volumes get automatically classified under the governance profiles you created using the snapshot frequency values you set in those profiles. After classifying, each volume gets evaluated against the resilience attributes you defined in those profiles. Finally, the chart splits the volumes within each governance profile into two groups: those that meet all resilience attributes and those that fail to meet at least one.

🟥 Volumes misaligned with resilience attributes 🟩 Volumes aligned with resilience attributes ○ Radius

Safe and fast recovery

Trusted copy identification, and clean room orchestration to test backups or snapshots prior to recovery.

AI-enabled early threat detection

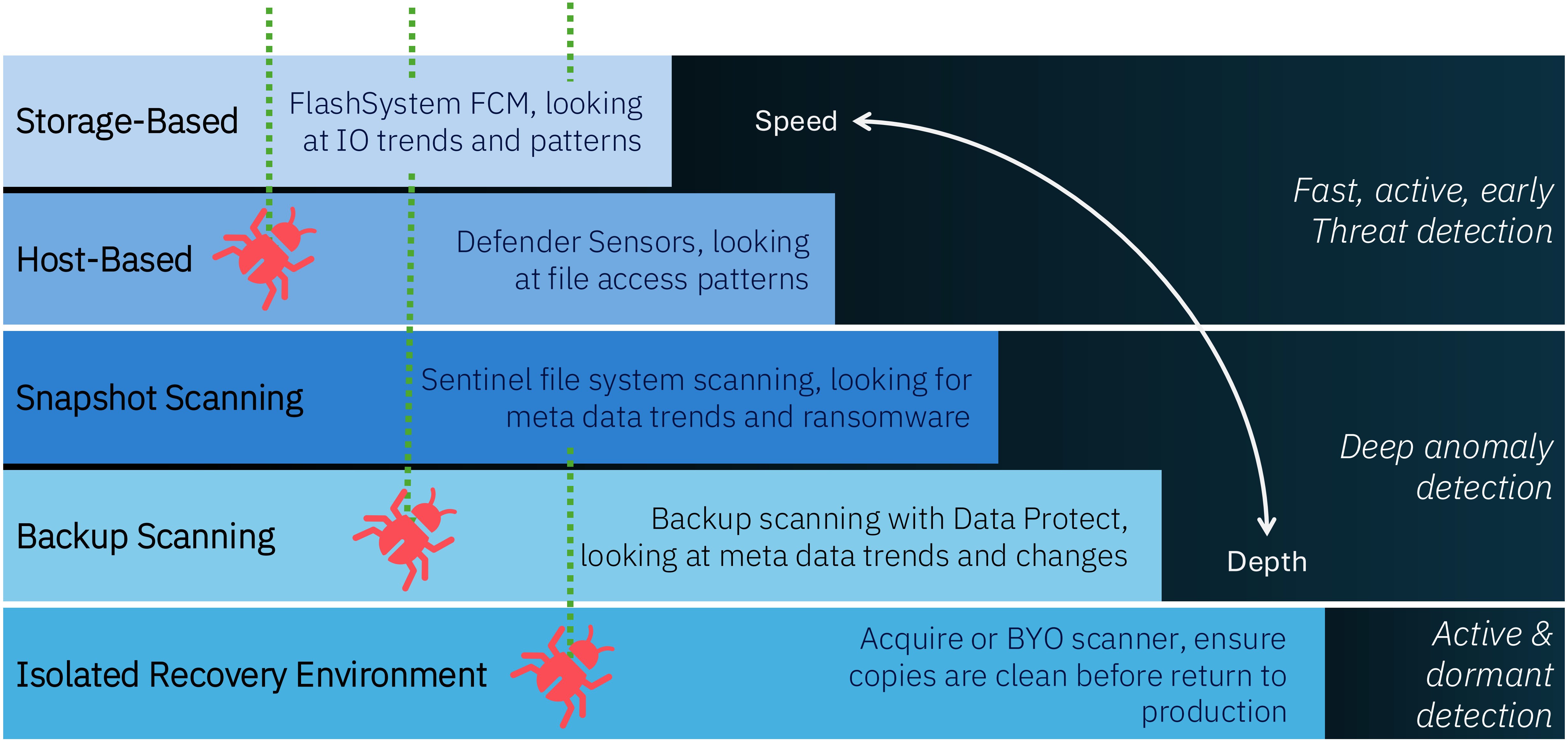
Layered sensors providing hardware, filesystem and backup-based detection that enables early response.

Data resiliency and compliance

Enables you to set the resiliency standard to meet compliance across your data storage estate.

Background

Multi Layered Ransomware Detection



Storage-Based

FlashSystem FCM, looking at IO trends and patterns

Host-Based

Defender Sensors, looking at file access patterns

Snapshot Scanning

Sentinel file system scanning, looking for meta data trends and ransomware

Backup Scanning

Backup scanning with Data Protect, looking at meta data trends and changes

Isolated Recovery Environment

Acquire or BYO scanner, ensure copies are clean before return to production

Speed

Depth

Fast, active, early Threat detection

Deep anomaly detection

Active & dormant detection