

Holisztikus védelem, jövőálló módon

Arrow IBM Modernization Workshop
2026.04.14.

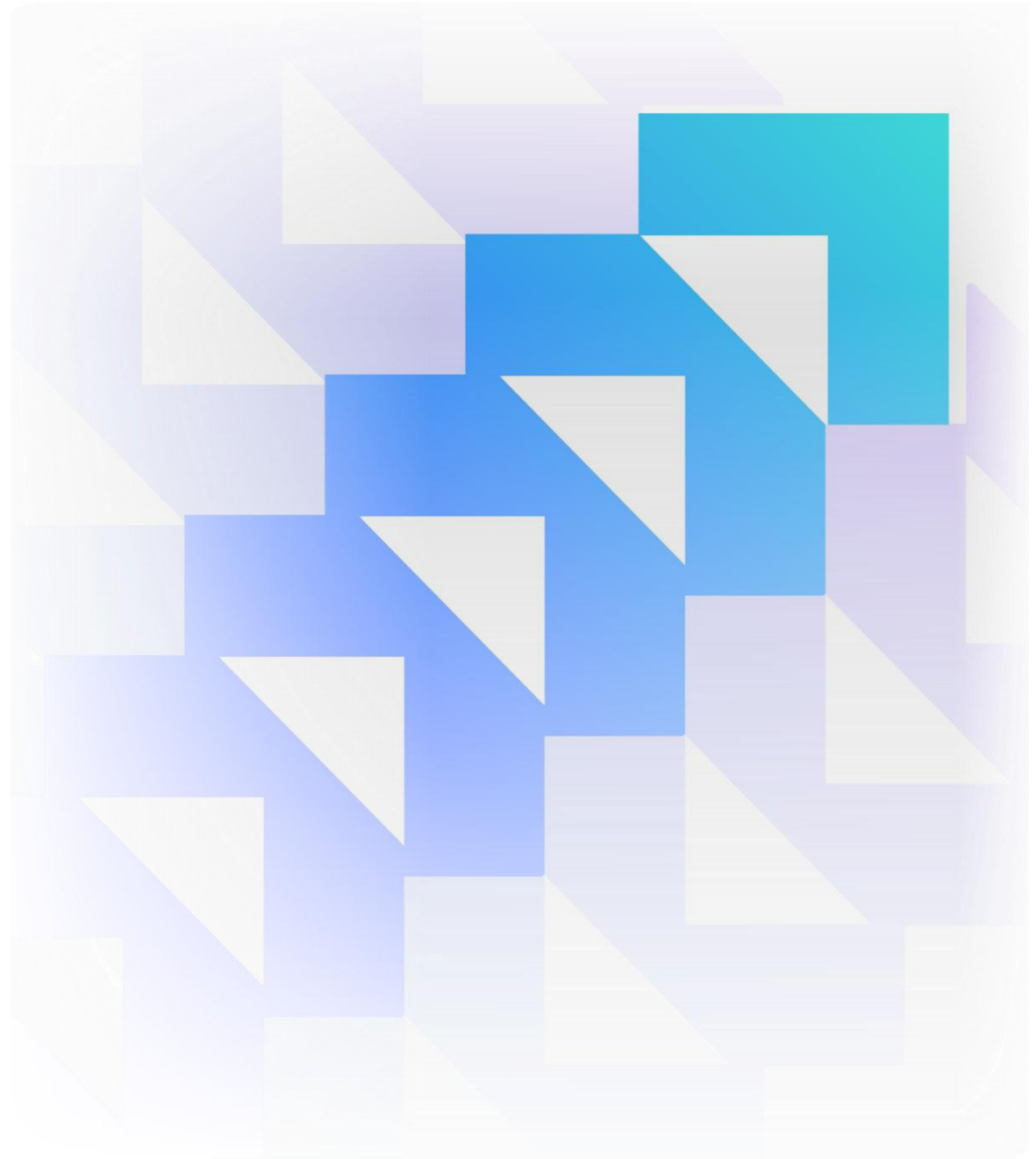
Gergely Ferenc

IBM HW Presales & BDM

Arrow ECS Kft.

Ferenc.Gergely@arrow.com,

+36 30 121 8007

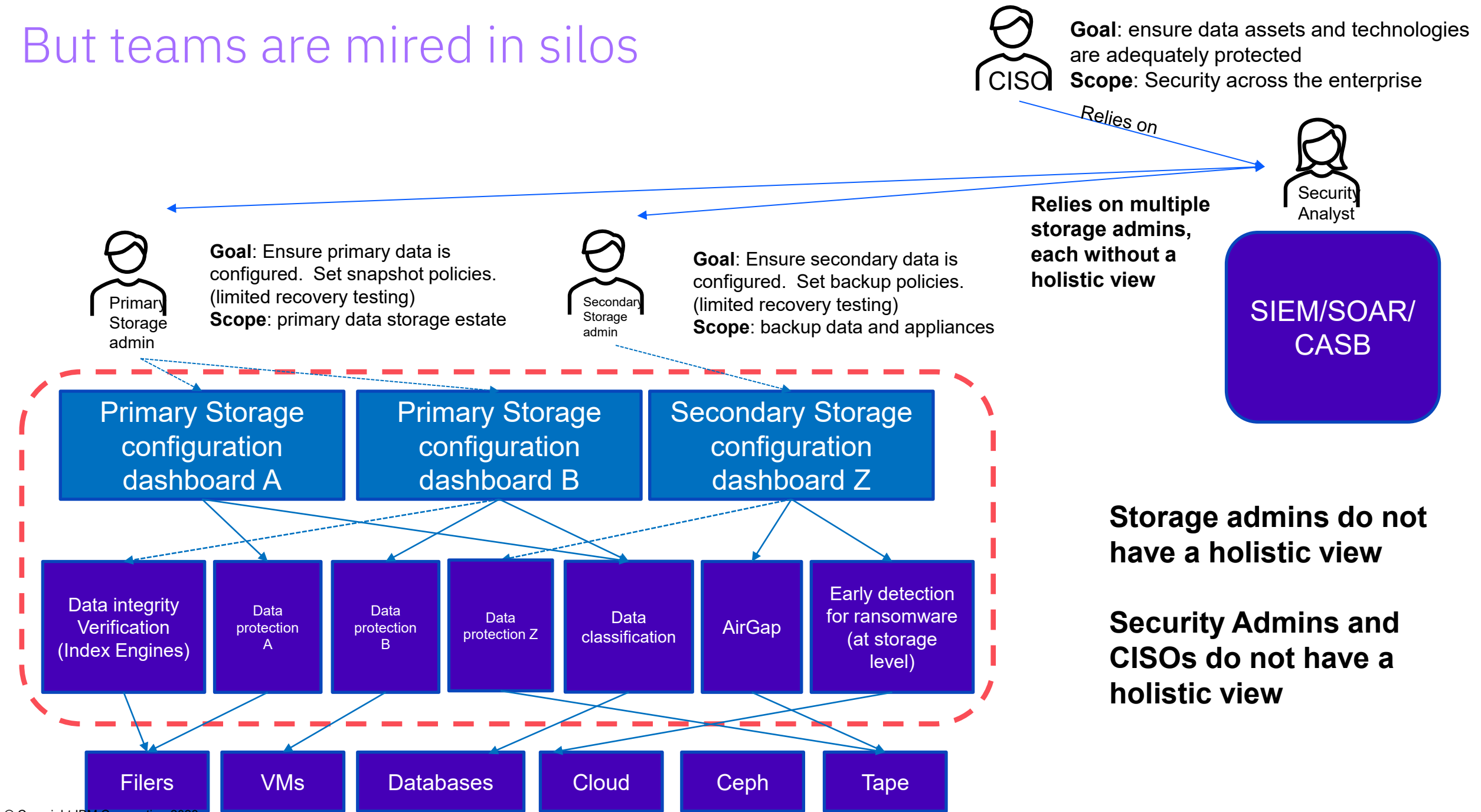


Paradigm shift: Need for Cyber Recovery

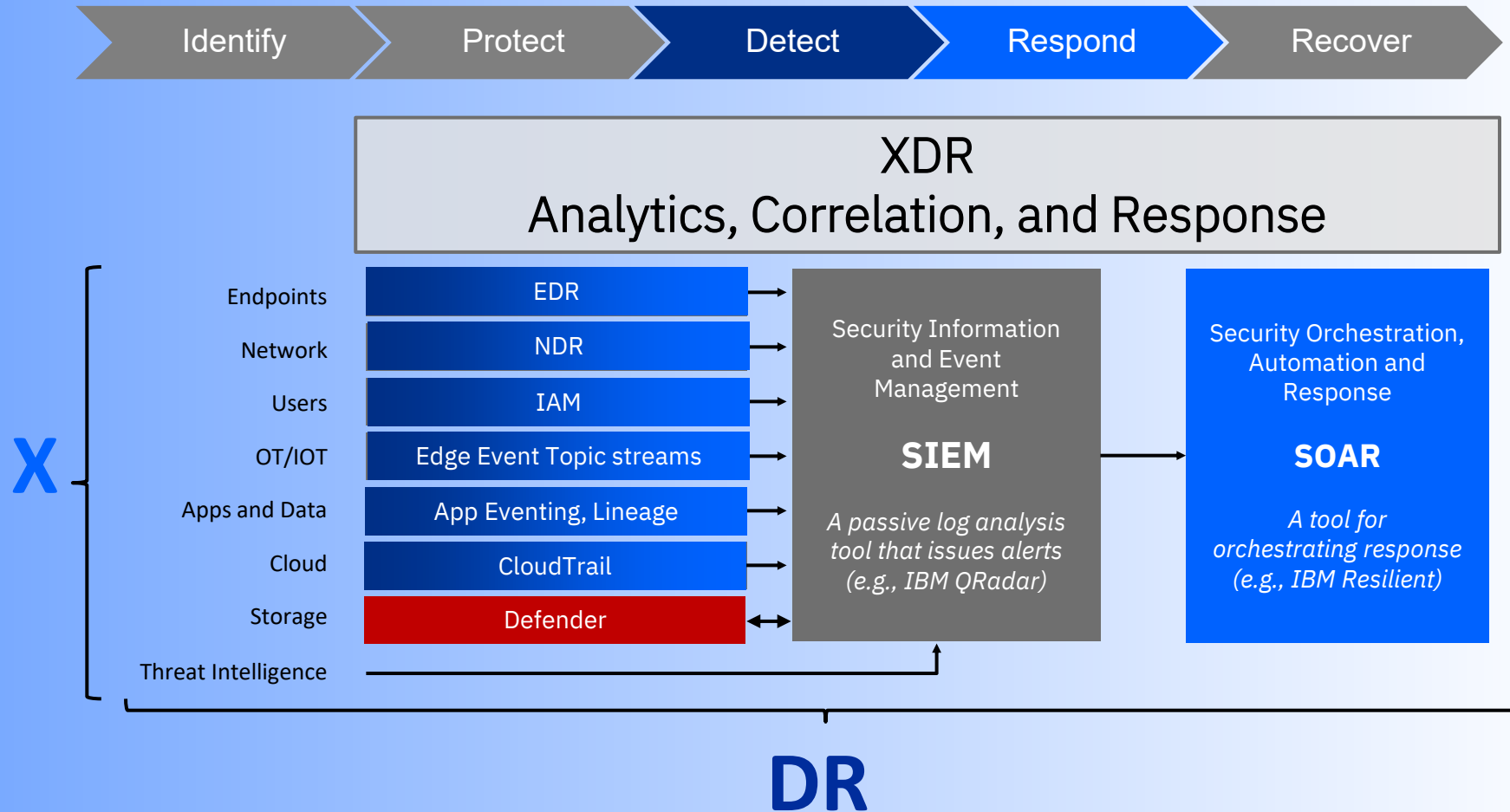
Cyber Recovery is fundamentally different from traditional recovery

Category	Traditional Recovery	Cyber Recovery	
Nature of impact	Random e.g. natural disasters	Targeted engineered for maximum impact	Need Early Detection
Scope of impact	Local / Regional	Global affects all connected systems	
Backup repository affected	Not typical	Yes 17% success in attacking backup	
Recovery point	Known	Unknown need most recent uninfected copy	Need Safe Recovery
Mitigation objective	RPO/RTO	RPO/RTO + Safe Recovery	
Duration of impact	Hours to Days	Days to Weeks	
Relative probability of occurrence	Low	High	

But teams are mired in silos



SecOps integration – adding Data layer to XDR



Extended Detection and Response (XDR)

“Security threat detection and incident response tool that natively integrates multiple security products into a cohesive security operations system that unifies all licensed components.”

– Gartner

Key Value Props

- **Intelligent threat management workflows** produce high-quality incident context and prioritization. *Risks are to data, need context on data, not available in Endpoints or Network detection*
- **Federated data stitching** keeps multi-source and data scale problem under control. *Need to bring together all risks to data together for coordinated response with SOAR*
- **Automated Response playbooks** accelerate time and precision to remediate. *Proactive remediation*

Positioning

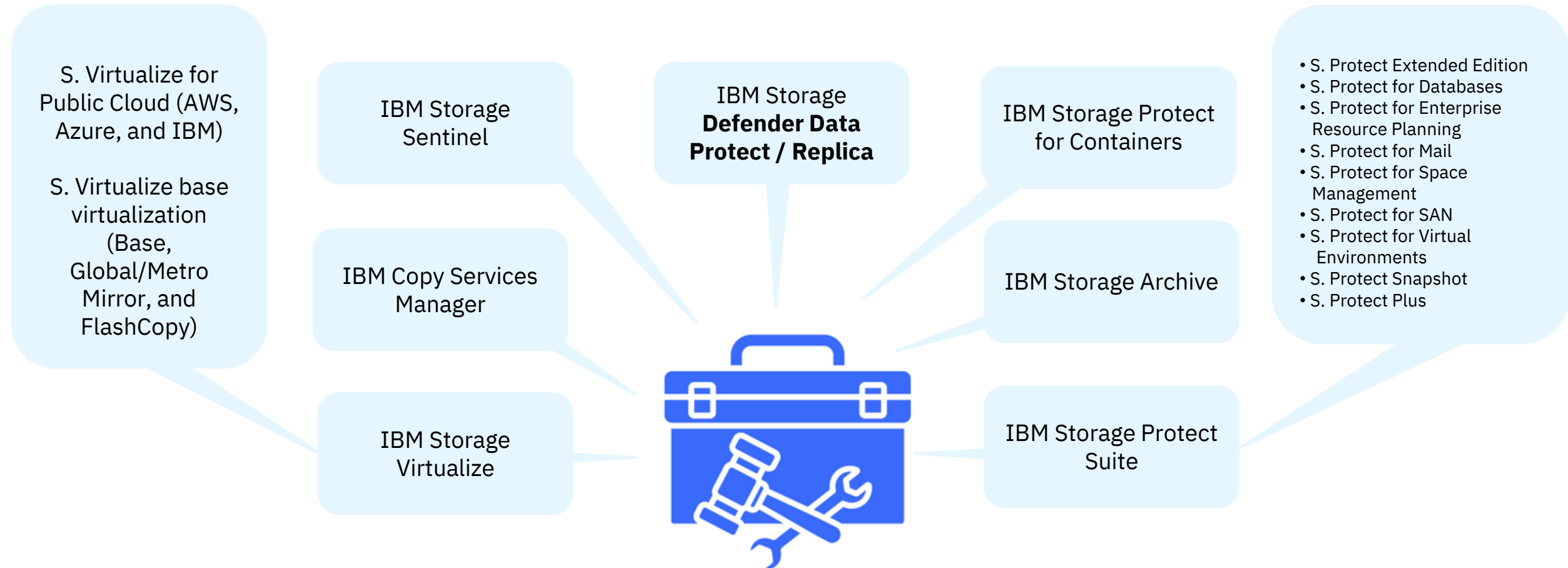
- **XDR is not enough** Does not have context on data, sensitivity, risks
- **Leverage XDR and SIEM threat management capabilities**
Coordinated investigation, response, eventing and detection.
- **Two way connection to SIEM, SOAR automation**
Data Services need to work in sync with SIEM and SOAR full duplex

Source: “Is Security Operations Ready for XDR?” Gartner. Nov 2021.

Original Content from April 2022 TT Study - Justin Youngblood, Sridhar Muppidi

IBM Storage Defender - Components

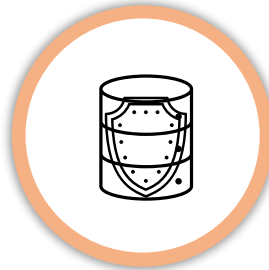
- Remember, IBM Storage Defender is a highly customizable solution where you can leverage various components or tools.
- These are the tools that are part of IBM Storage Defender:



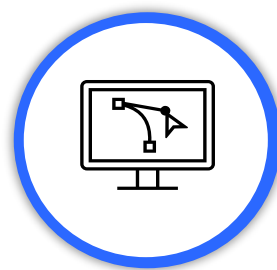
A complete solution that goes beyond Backup



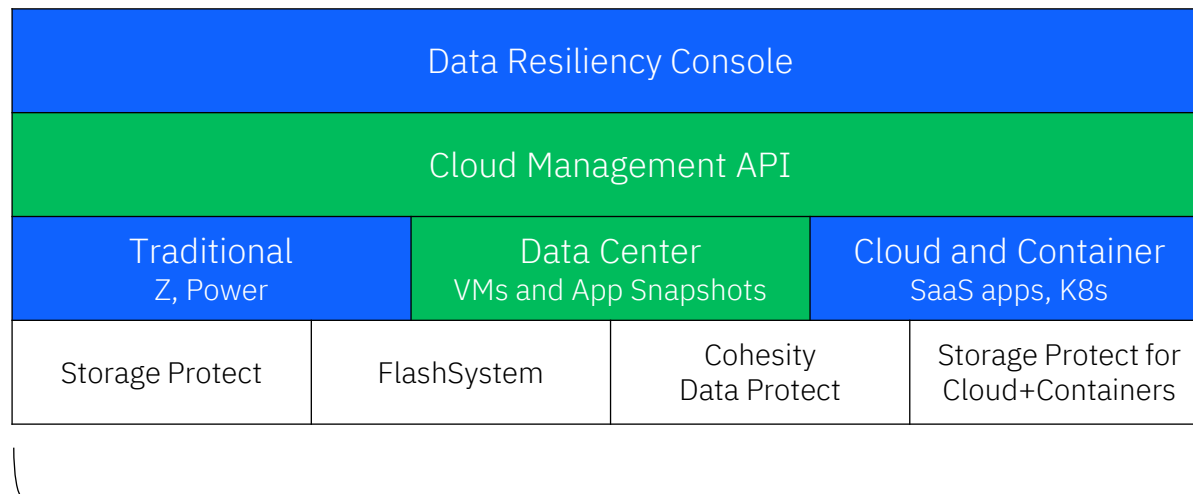
Early Detection



Safe and Fast Recovery



SecOps Integration



One IBM Storage Defender, One credit-based license

Cohesity OEM helps complete and strengthen our data protection portfolio:

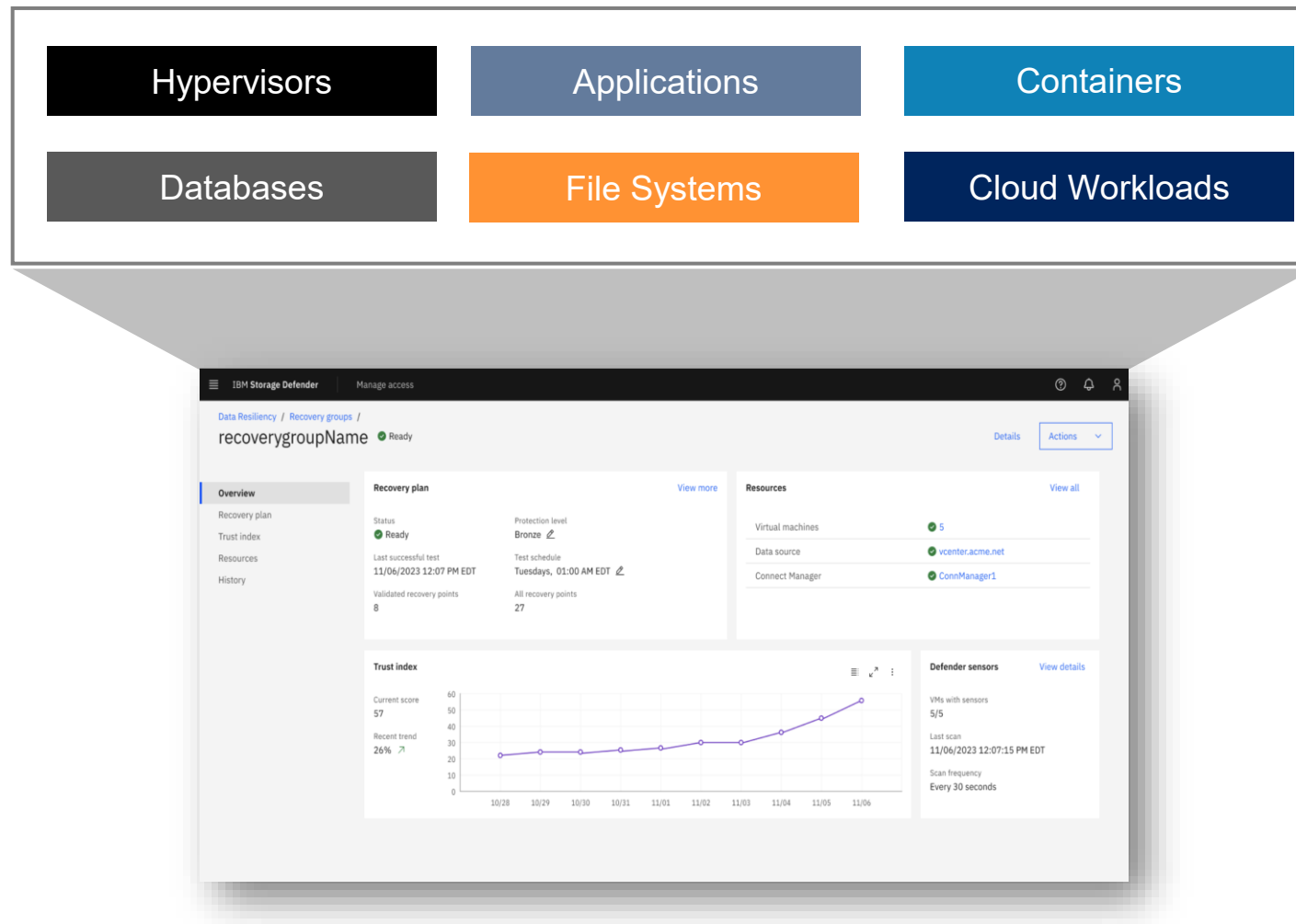
- Industry leading VMWare backup solution
- Fast, highly efficient, immutable backup at scale
- Detection of Ransomware or other threats **in backups**
- **Rapid recovery** from triaged safe backup – up and running **within minutes**
- Cloud based management platform

With IBM Storage Defender, we go beyond backup

- Data resilience for **all workloads**; across hybrid cloud, on primary/secondary storage
- **AI-powered early threat detection that is app aware**
- **Rapid recovery** from the safest backup or snapshot for each workload
- Collaborative Threat **response with SecOps**
- One IBM Storage Defender license for all IBM + Cohesity capabilities
- Operated and supported by IBM SRE, support, TLS, Expert Care teams

IBM Storage Defender: Workload Support

Unified Management for Data Resiliency across all workloads



1

Foundational Security
& Data Protection

2

3

4

5

IBM Storage Defender Data Protect Architecture

Tiering and Archiving

Cloud Tier

Enables an additional storage tier used to migrate cold data from primary storage to cloud storage

High deduplication rate reduces amount of data **migrated** to cloud.

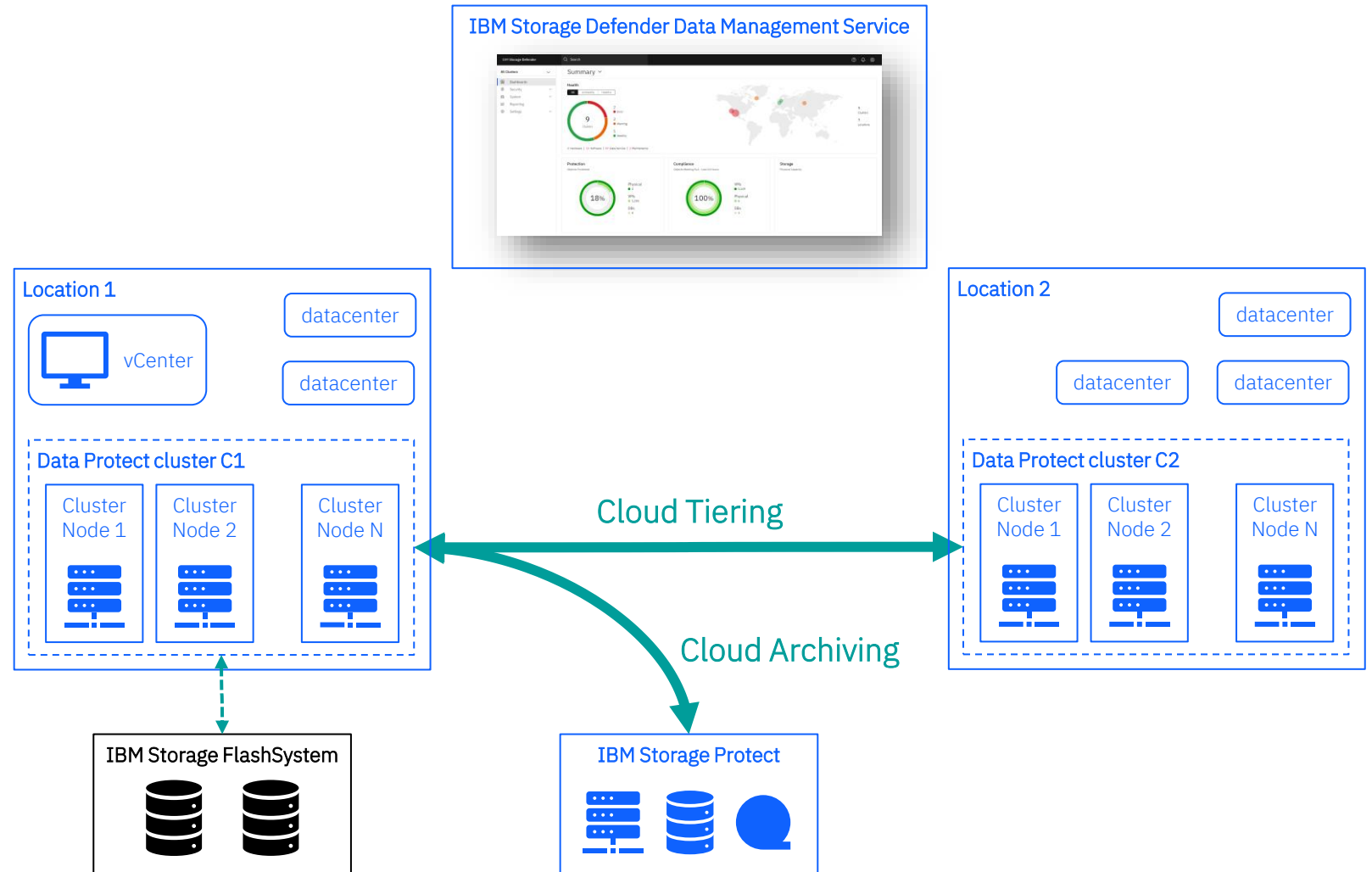
Compression of data sent to cloud tier always **enabled**.

Cloud Archive

Archive data to cloud or other secondary storage.

Supported Cloud archive targets:

- Public clouds
- Private clouds - S3-compatible device
- **IBM Storage Protect** server S3
- Storage system providing NFSv3



IBM Storage Defender Data Protect Architecture

Replication

In-Cluster replication

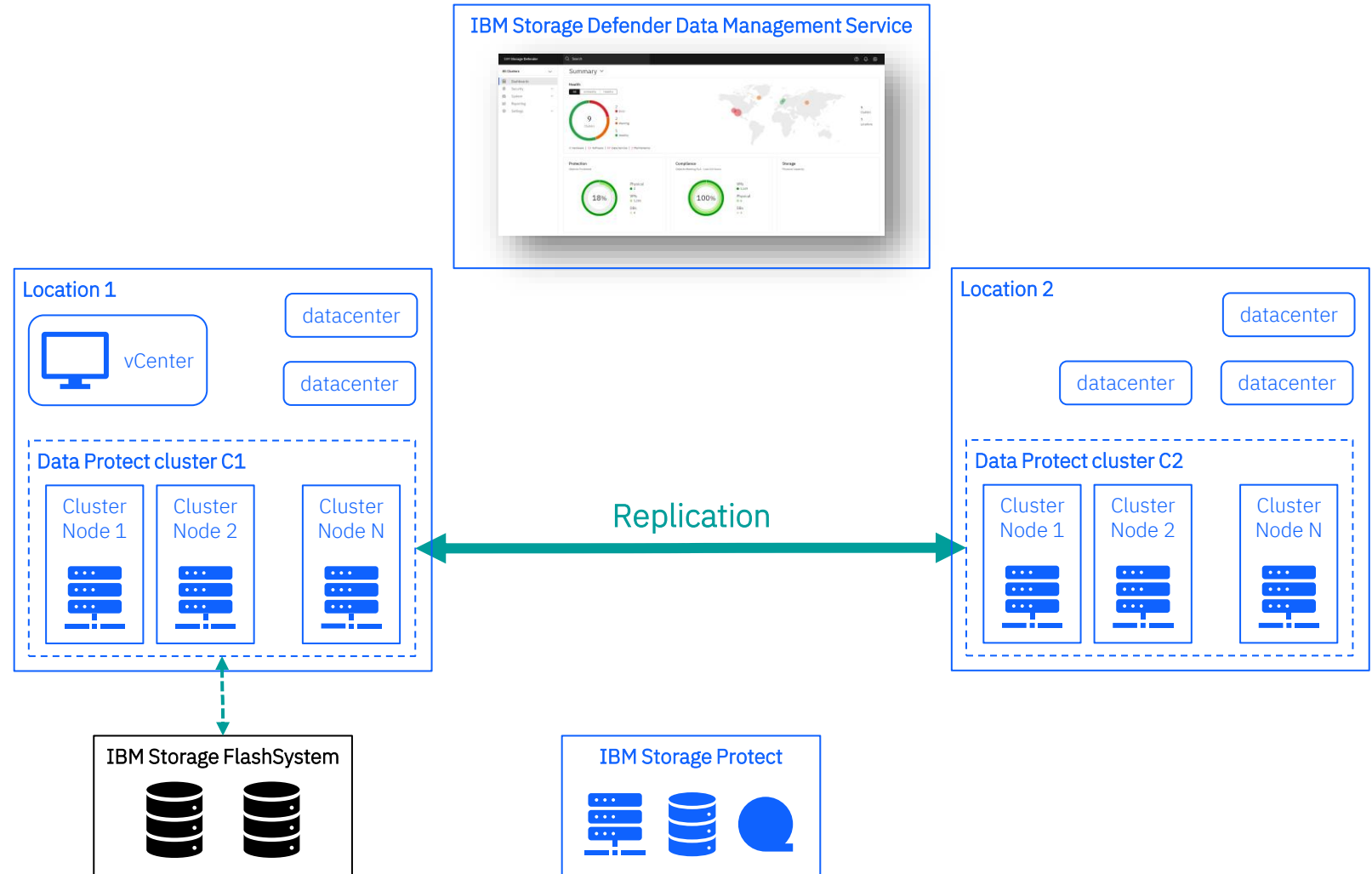
File blocks are distributed across the Cluster with a replication factor of two or more.

Cross-Cluster replication

Replication **leverages snapshot** compare methods to efficiently determine the changed entries and transmits the changes to the target cluster.

Replication to different Data Protect version is supported

Data in flight over HTTPS encrypted with AES-128-CBC



IBM Storage Defender

Data Management Service

Multi-cluster management

Actively manage all your clusters, including multi-cluster monitoring and reporting, from a single dashboard.

Global actionable search

Search **across clusters** and act directly from the search results page. For example, **search for all unprotected VMs** and **create jobs to protect them**.

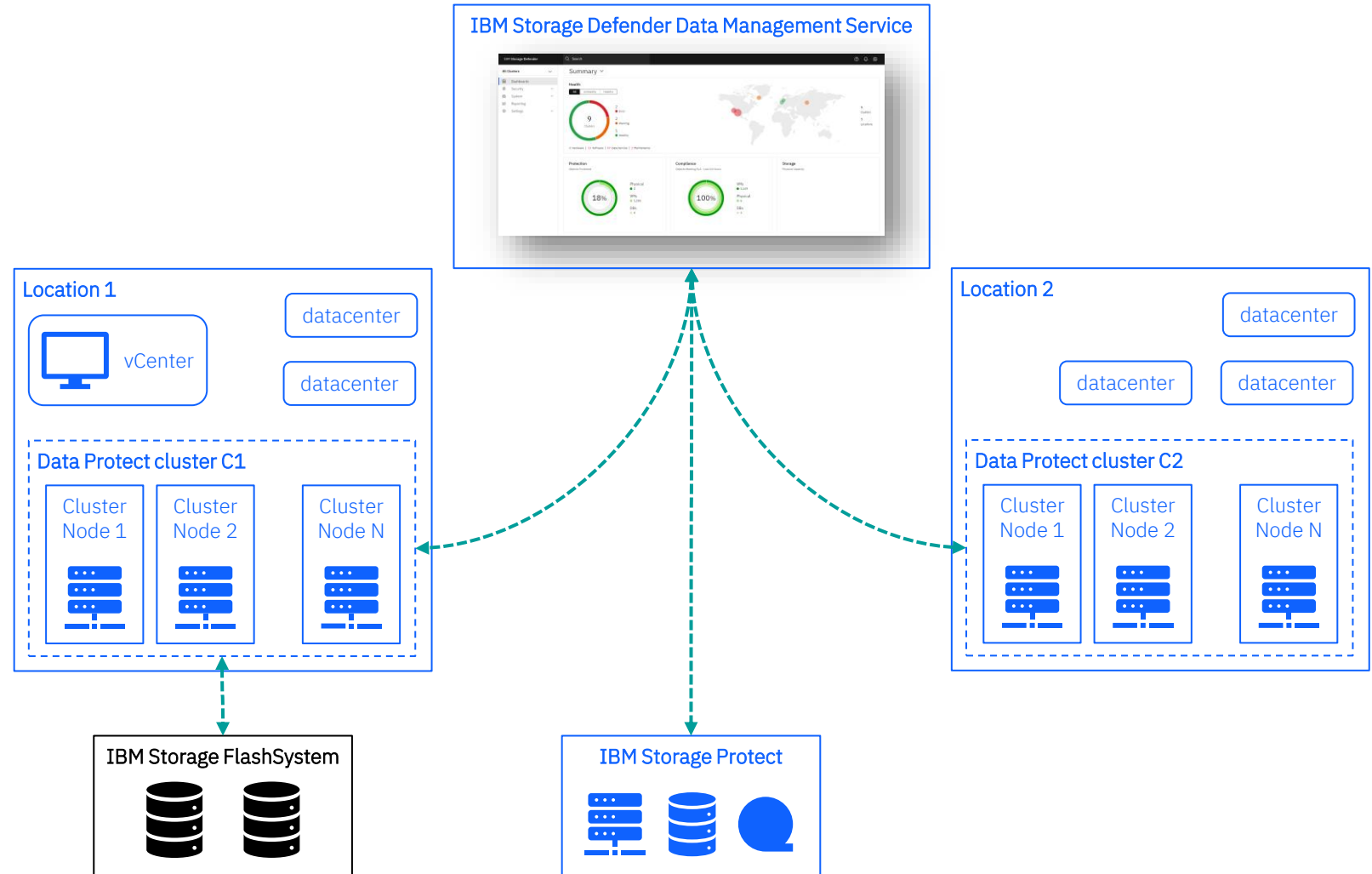
Smart Assist

Automatically schedule and orchestrate jobs and workloads to help meet SLAs.

Get recommendations based on capacity forecasting and disk failure prediction. View important Data Management field notices.

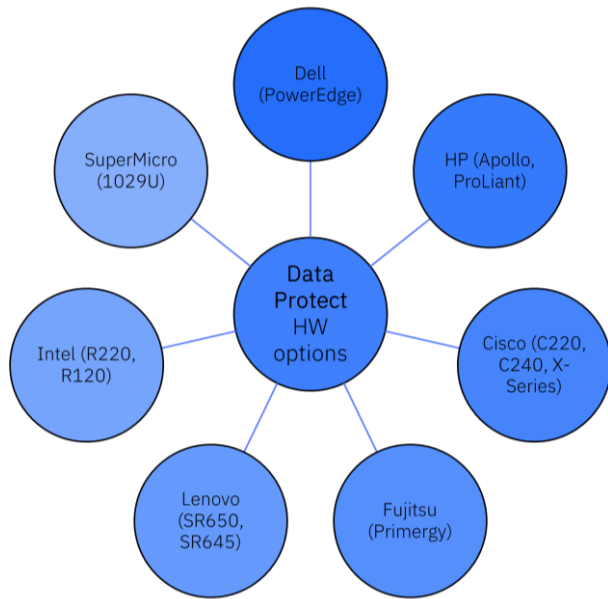
Security tools

Detect threats and other **anomalies** across clusters with the unified **Alerts** page.



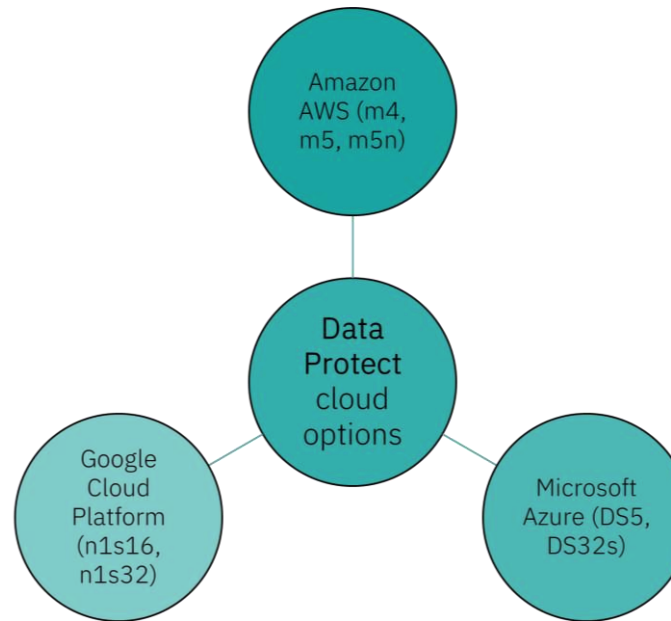
IBM Storage Defender Data Protect

Platform options

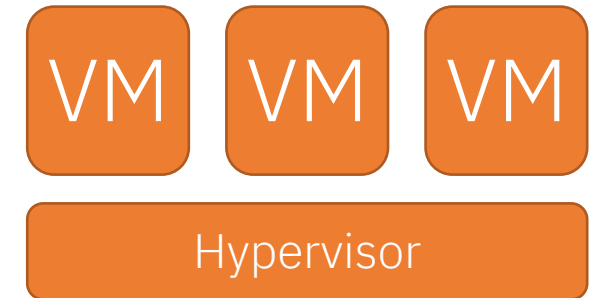


Physical Deployment

Most workloads on-premises will involve physical deployments



Cloud Deployment



Virtual / ROBO Deployment

Most virtual/ROBO deployments are configured to replicate to a physical cluster in another location

IBM Storage Defender - PORTFOLIO

– Workload Support

Databases

ORACLE®
ORACLE® RAC

SAP HANA

SAP

IBM DB2

Microsoft®
SQL Server®

SYBASE®

Sybase
IQ

Informix

InterSystems®
Caché
IRIS Data Platform

Couchbase

MySQL

APACHE
HBASE

mongoDB®

PostgreSQL

HIVE

DataStax

Apache
CASSANDRA

Cockroach DB

amazon
RDS
Aurora

Primary Storage

Over 500 systems
supported

Hypervisors

vmware®

Microsoft
Hyper-V

NUTANIX AHV

Red Hat
Virtualization

ORACLE® VM

Containers

RED HAT®
OPENSIFT
Container Platform

kubernetes

VMware Tanzu

Physical

Windows®

AIX

LINUX

solaris

Applications

Exchange

Microsoft
Active Directory

SharePoint

Lotus® Domino

File Systems

NetApp

ISILON

GPFS

hadoop

Cloud

Exchange
Online

Microsoft 365

Dynamics 365

salesforce

Azure
Active Directory

Azure File
Storage

Azure Blob
Storage

AzureVM

Google Workspace

1

Foundational Security
& Data Protection

2

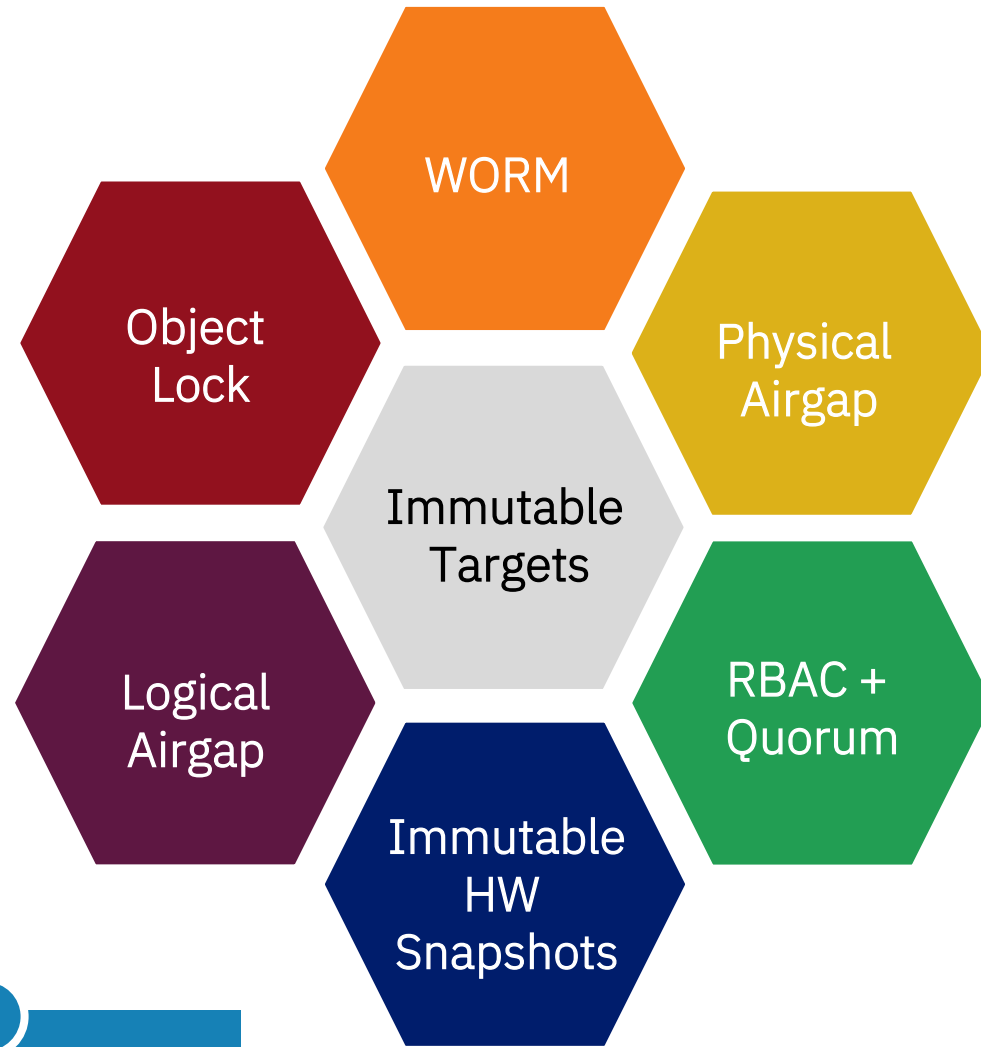
3

4

5

Implementing immutability at multiple points

Ensuring data lands somewhere it cannot be deleted or altered until it expires



But, you need to ensure that data is not already corrupted..

1

2

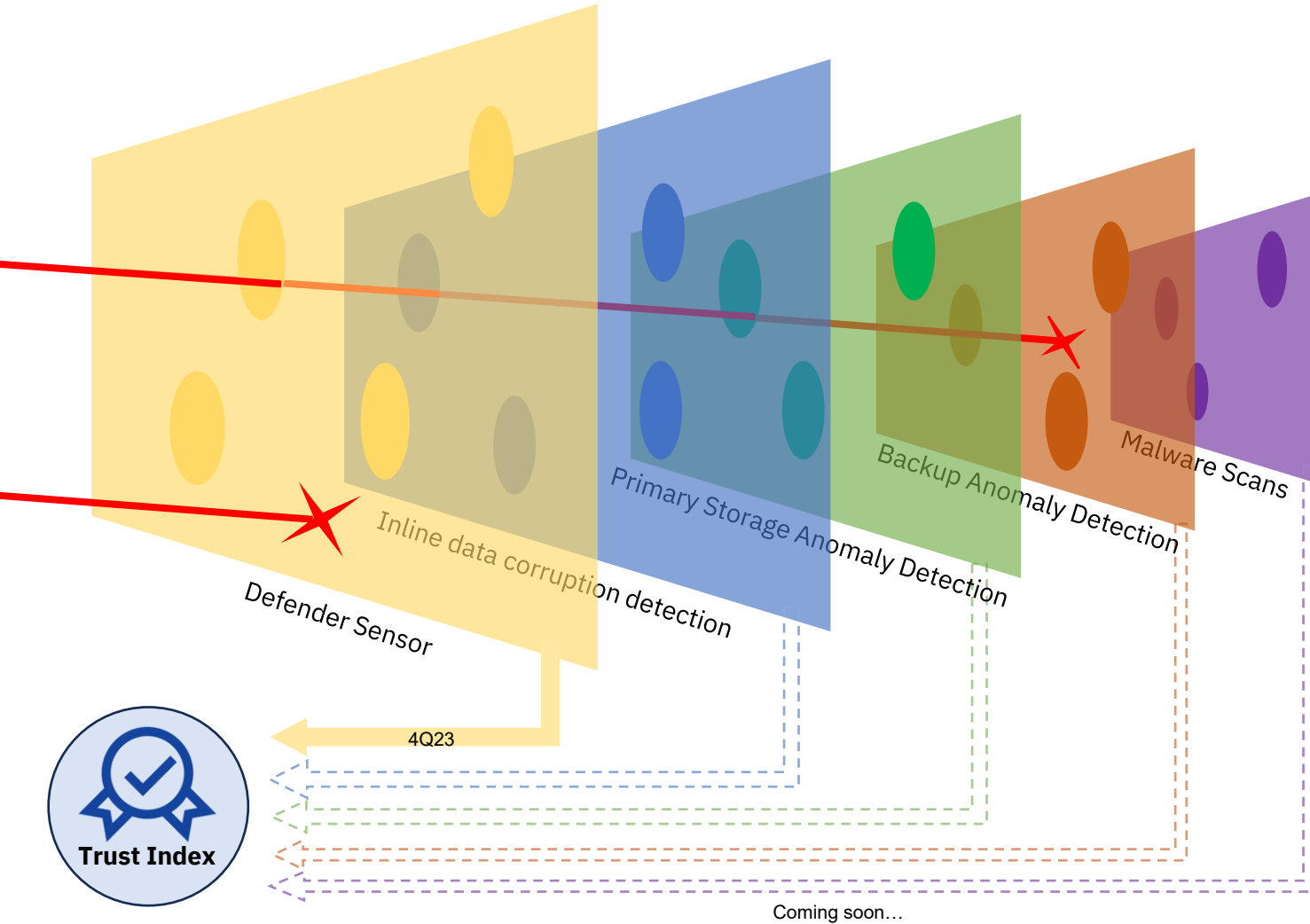
Immutability

3

4

5

Early Threat Detection



Defender Sensor

- Detects anomalies on a live system by **analyzing attack patterns against file metadata and deep file analysis**

Inline Data Corruption Detection

- Provides **entropy-based** anomaly detection
- Occurs at the **array level** through array SW (**FMC4**)

Primary Storage: Anomaly Detection

- **Application aware** anomaly scanning of **Immutable** HW Snapshots (SGCs)
- Notifies of anomalies and finds the latest clean snapshot (latest snapshot without anomaly)

Backup Storage: Anomaly Detection

- Leverages **AI and ML** to identify anomalies in size of data written, data reduction rates (dedup & compression)

Isolated Environment: Malware Scan

- Scans mounted data for known malicious files and executables
- Provides ability to **clean** or **quarantine** found malware

1

2

3

Discovery

4

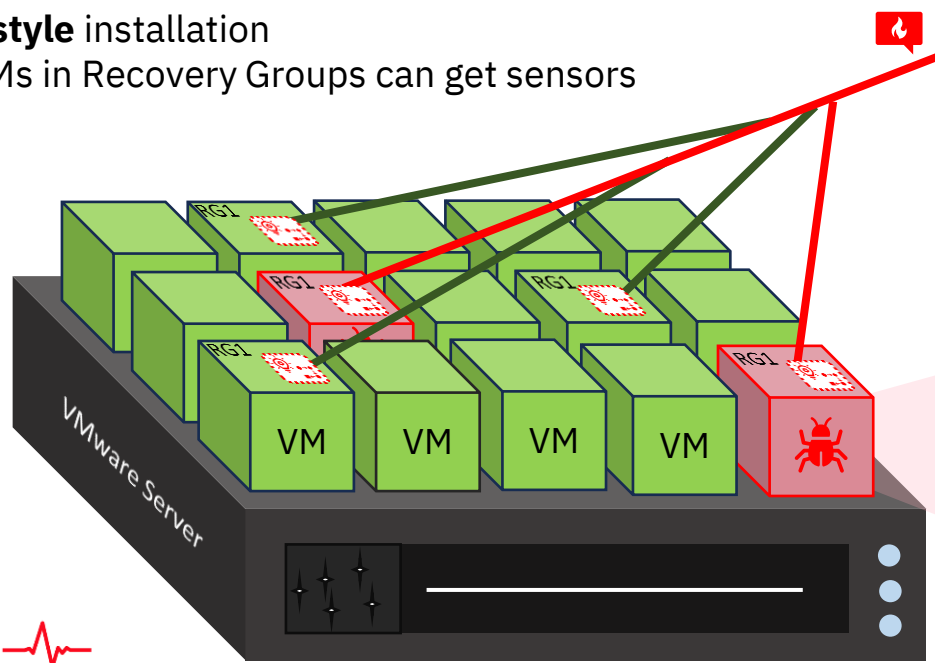
5



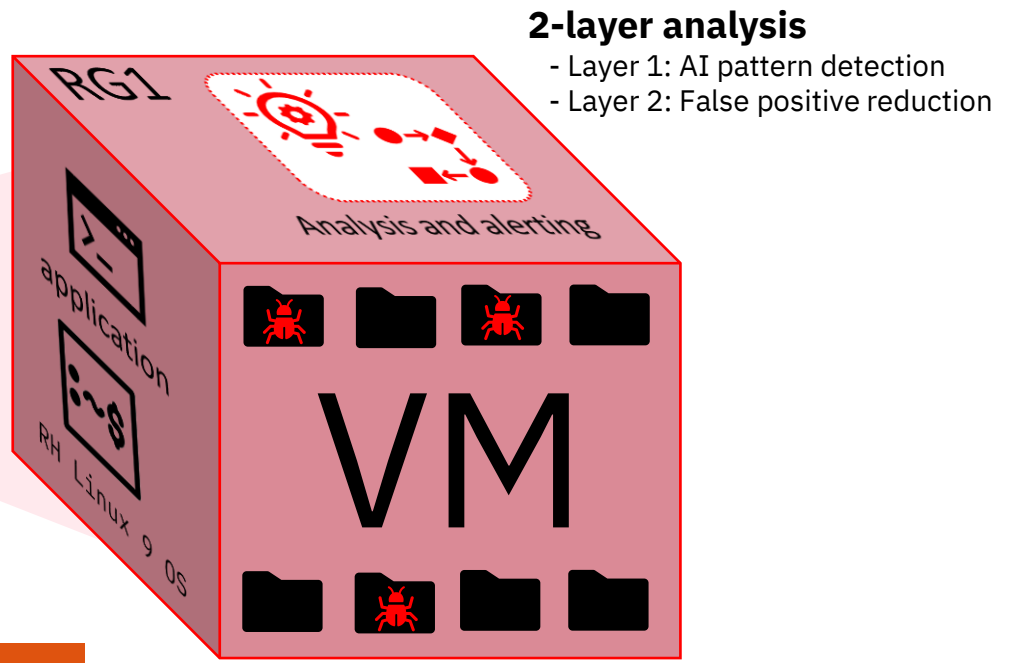
IBM Storage Defender

Defender Sensors - Near real time lightweight ransomware detection

- ✓ Adds and additional layer of detection
- ✓ Installs at the **file system layer** of the host
- ✓ Finds infected file(s) in the local filesystem
- ✓ Applies **IBM patented and trade secret techniques** to find corruption host layer vs storage device layer
- ✓ **Low overhead** install
- ✓ **Agent style** installation
- ✓ Only VMs in Recovery Groups can get sensors



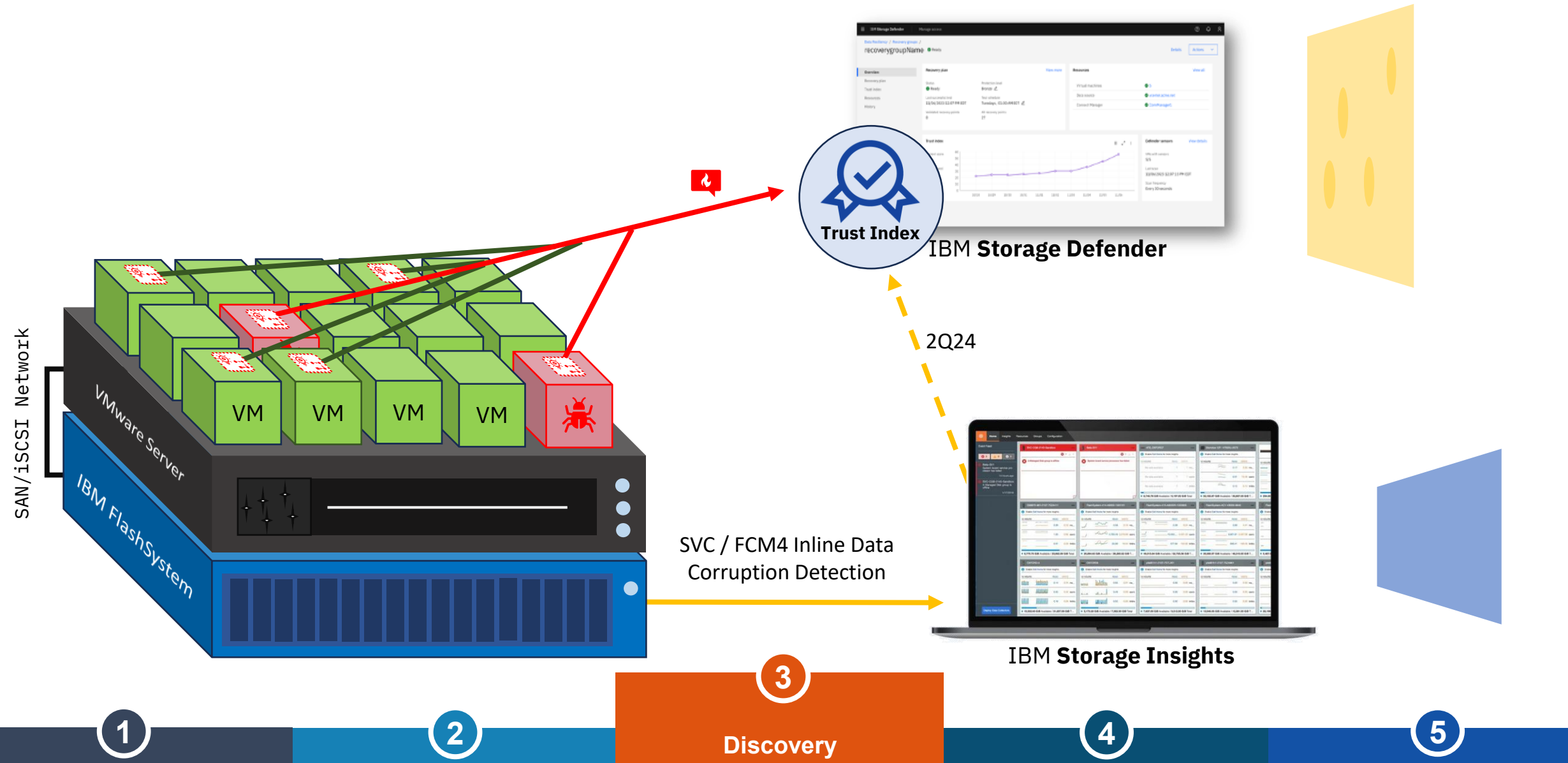
Heartbeat 
Alerts feed into Trust Index every 30 seconds



IBM Storage Defender

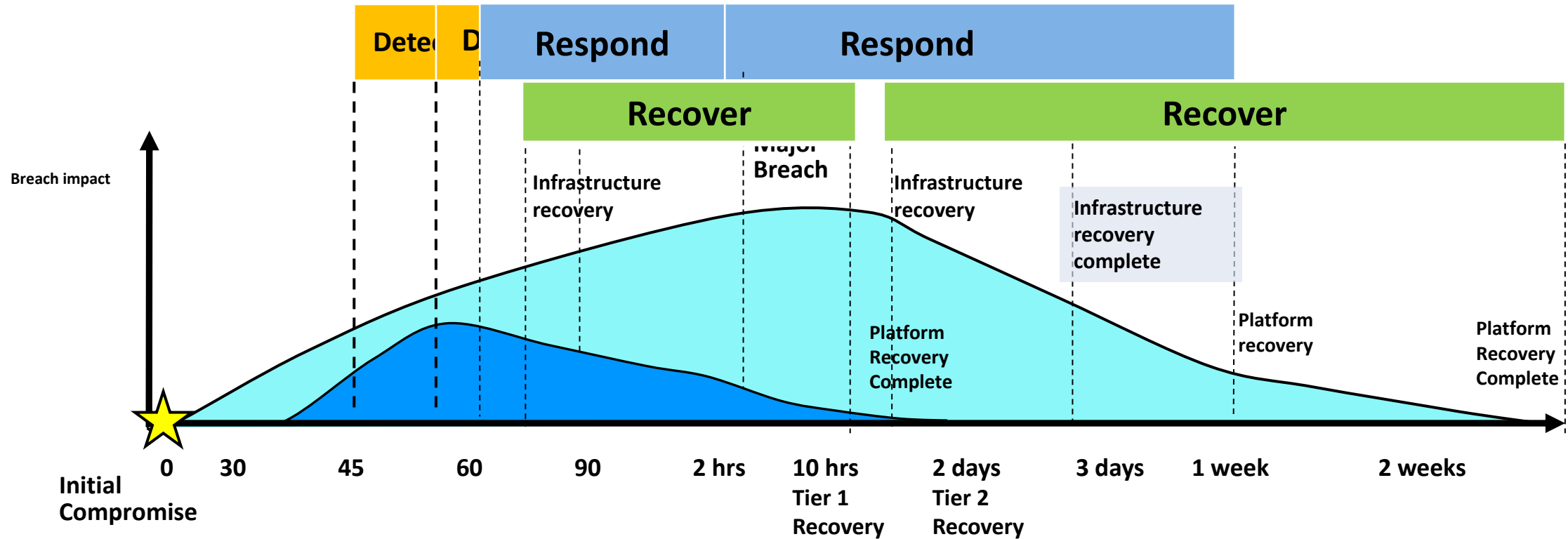


Defender Sensors + Inline Sensors and IBM FlashSystem working together



Attack, detection, and recovery

Cyber Incident Timeline



1

2

3

4

5

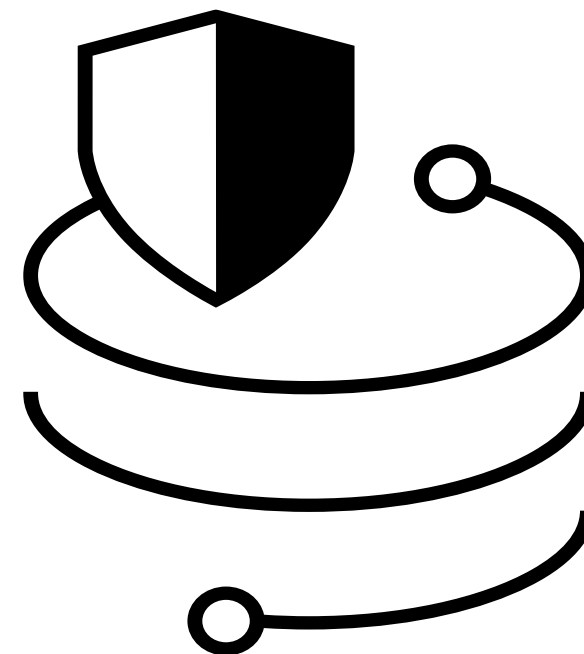
Recovery

Automation & Orchestration

IBM and Partner Ecosystem Integration

Automation & Orchestration for IBM Data Resilience

- Integration for IBM backup and primary storage products
- **Fully automated** disaster recovery testing
- **SOAR** solution **integration**
- **Infection** signature **detection** across storage environment
- **Automated** anomaly and virus **scanning** with **cleansing**
- On-prem or cloud **cleanroom** for safe and secure testing of suspect copies
- Full management of the environment
- Automation for simplicity



5

Automation

1

2

3

4

Data Resilience is a team sport

IBM and our partners combat threats together



Breadth and depth of cyber resilience capabilities



Early threat detection & closed loop remediation

QRadar® SIEM

QRadar® SOAR



IBM **Storage Sentinel**

Data Integrity verification & Ransomware Recovery



PREDATAR

Backup scan, anomaly detection, on-prem or cloud clean room, cleanse & restore



Many more..

2.1.2 IBM Storage Defender — Threat Aggregation

SENSOR MANAGEMENT

Centralized Sensor Management

- View all [VMware](#) hosts & sensor status from a single location
- Deploy, update & remove sensors without navigating recovery groups
- Install sensors on VMs [outside recovery groups](#) (new in 2.1.2)

THREAT VISIBILITY

Threat Aggregation & Trust Scoring

- Surface threats against the specific storage object detected
- Ingest alerts from IBM Data Protect ([DMS](#)) and [ESPIAL](#) sensors
- AI-powered [Trust Score Engine](#) calculates risk per protected resource

RECOVERY ORCHESTRATION

Integrated Recovery & SIEM Forwarding

- Recovery Manager [triggers plans](#) for compromised resources [automatically](#)
- Forward [all threats to SIEMs](#) (QRadar, Splunk) via REST API & [Kafka](#)
- Existing threats auto-migrated to new unified model on upgrade

What's New

One place to manage all sensors

Customers [no longer need to navigate recovery groups](#) to deploy or update sensors. Every VMware host is visible and manageable from a [single Threat Management screen](#).

Threats tied directly to storage objects

Threats now surface against the specific VM or storage asset they were detected on — giving customers [immediate context](#) without manual correlation.

AI Trust Scores reduce alert fatigue

The Trust Score Engine [continuously assesses](#) each protected resource. Sales can position this as intelligent prioritization — customers know which assets are at highest risk.

Built-in SIEM integration

All detected threats flow [automatically to QRadar and Splunk](#). Positions Defender as a native part of the customer's existing security operations workflow.

Zero-friction upgrade path

Existing [threat data is automatically migrated](#) to the new unified model — customers upgrading from earlier versions retain full history with no manual steps.

2.1.2 IBM Storage Defender — Isolated Scan Environment (ISE)

ISOLATED SCAN ENVIRONMENT

Automated AI-Driven Malware Scanning

- Scans FlashSystem recovery points in a secure, isolated environment before they're needed
- [Powered by](#) Index Engines CyberSense via IBM Storage Defender [Sentinel](#) (v1.1.12.1+)
- Prevents lateral movement — scanned in isolation; production systems stay untouched

SCAN CAPABILITIES

Flexible Scanning & Threat Classification

- Scheduled (daily/weekly/monthly) and on-demand manual scans with optional priority override
- Results tagged CLEAN, SUSPICIOUS, MALICIOUS, or INCONCLUSIVE per recovery point
- Detailed anomaly reporting per VM; recovery points [auto-tagged](#) on scan completion

DATA PROTECT THREAT SCANNING

Security Center & Threat Scanning (DMS)

- Analyzes backup snapshots for malware, ransomware & IOCs using 100K+ rules and custom YARA
- New [Security Center UI](#) in DMS; requires compute nodes, threat scanning entitlement & DP 7.1.2_u4+

What's New

Scan before you need to recover

Customers can now [verify recovery points are clean before](#) a crisis — not after. A major shift from reactive to proactive resilience.

Isolation means zero risk to production

Potentially infected data is [scanned in a fully isolated environment](#). Malware cannot spread to production systems during scanning.

Fully automated, policy-driven workflow

No manual steps. Defender [automatically clones](#) snapshots, [mounts volumes, scans, and cleans](#) up on a customer-defined schedule.

Every recovery point is trusted & labeled

Each scanned recovery point gets a [trust label](#) — CLEAN or MALICIOUS. Position as a 'clean copy guarantee' customers can rely on.

Two scanning paths, full lifecycle coverage

ISE + CyberSense covers FlashSystem VMware snapshots. DMS Threat Scanning covers backup data with 100K+ rules. Full coverage.

2.1.2 IBM Storage Defender — Data Protect Target

WHAT IS SMARTFILES

Enterprise File & Object Storage in DMS

- [Software-defined, multi-protocol file and object solution](#) — consolidates unstructured data silos
- Storage Domains define dedupe, compression, erasure coding, encryption & fault tolerance
- Views are logical endpoints (NFS/SMB/S3) with configurable QoS, quotas, and DataLock/WORM

KEY CAPABILITIES

Security, Protocols & Data Efficiency

- [Multi-protocol support](#): NFS v3/v4.1, SMB 2.x/3.0, S3 (AWS-compatible API with versioning & ACLs)
- [Data reduction](#) via inline/post-process dedupe & compression; AES-256 encryption (FIPS 140-2)
- [WORM/DataLock](#) compliance, self-service snapshot restores, audit logs & antivirus integration

KEY USE CASES

Backup Target, File Share & S3 Object Storage

- [Backup target](#) for Spectrum Protect, Veeam, Commvault & NetBackup with dedupe/compression
- Corporate file shares (SMB/NFS) and S3 object storage for Splunk SmartStore & archival

What's New

Unstructured data now lives inside Defender

SmartFiles brings enterprise file and object storage directly into DMS — customers [manage backups, file shares, and S3 buckets from a single Defender interface](#).

One platform for every protocol

[NFS, SMB, and S3 are all supported](#) in the same solution. Customers with mixed workloads no longer need separate storage platforms for each protocol.

Built-in data reduction cuts costs

[Inline dedupe and compression](#) reduce storage footprint automatically. Combined with AES-256 encryption and [WORM compliance](#), this is a strong story for regulated industries.

Self-service restores reduce IT burden

[End users can restore their own files](#) via hidden snapshot directories — [no IT ticket required](#). This is a meaningful operational efficiency win for enterprise customers.

Backup target for all major ISV tools

SmartFiles works as a [backup repository for Veeam, Commvault, NetBackup & Spectrum Protect](#) — letting customers land backups directly on Defender-managed storage.

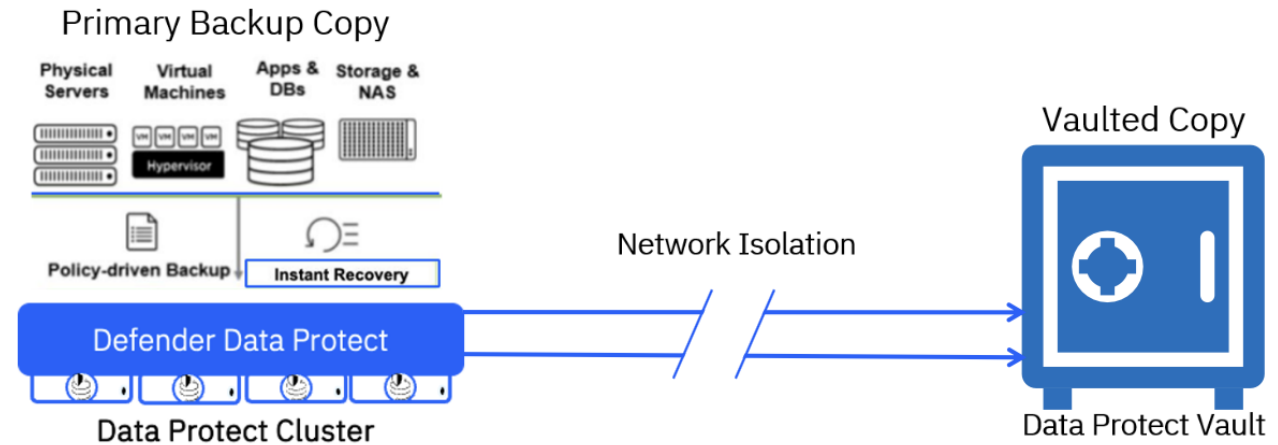
2.1 Data Protect

IBM Storage Defender Data Protect Vault

IBM Defender Data Protect Vault Service: A fully managed **SaaS solution managed by IBM**, ideal for organizations seeking rapid deployment, minimal operational overhead, and expert management. **Choose from two tiers** of storage, without compromising on security features, based on recovery SLAs.

- **Cold Storage:** Recovery can take **up to 4 hours to start** after initiation depending on size of data with recovery of full objects back to the source or an alternate location
- **Warm Storage:** Recovery **starts immediately** upon initiation and allows granular recovery back to source or alternate location

Customer Managed On-Premises Data Protect Vault: A customer-managed solution deployed within an organization's data centers, perfect for businesses with strict data sovereignty requirements, enhanced compliance needs, or fastest RTO.



2.1 Data Protect



Kubernetes

- Quiesce workloads during backups
- Granular recovery of files and folders within PVCs



Virtualization

- Red Hat Virtualization support:
 - IPv6 Support
 - Label-based VM backup selection
- Disk inclusion in VMware backups



Physical Servers

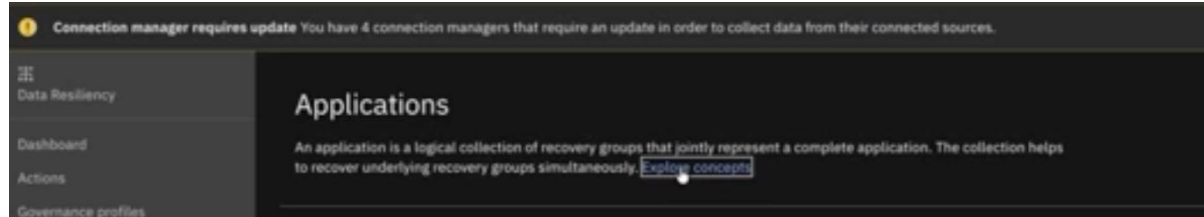
- Files and folders backup for Linux on z/Architecture
- Support for S3-compatible storage protection



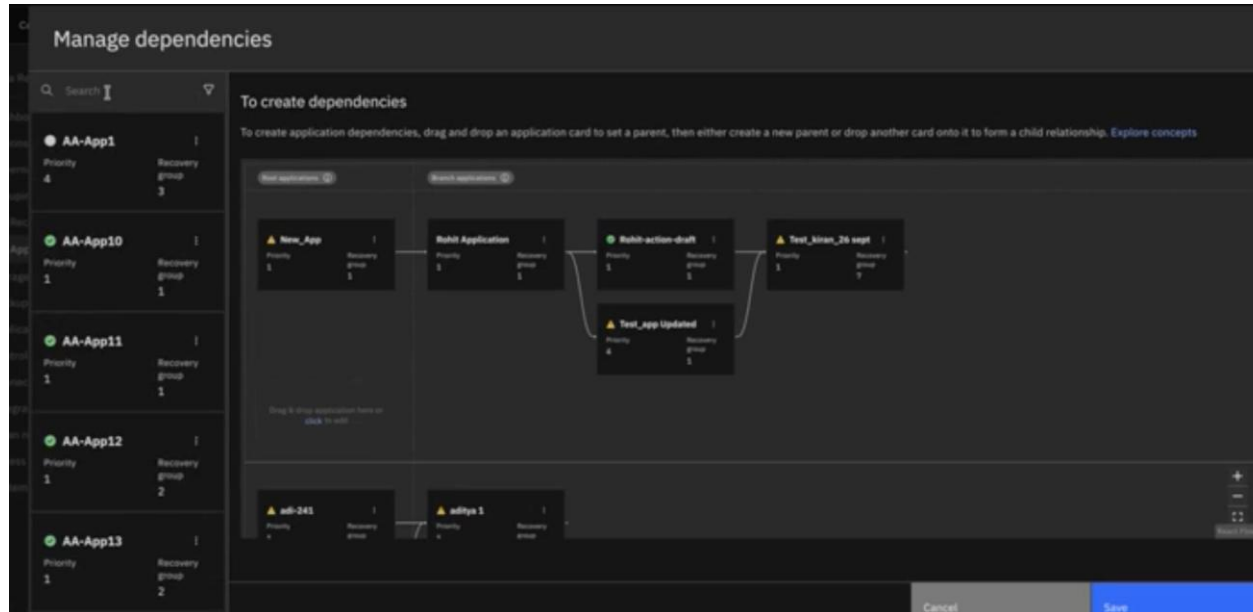
Databases

- Backup and recovery in partitioned IBM DB2 environments

2.1.0 Application Dependency Mapping

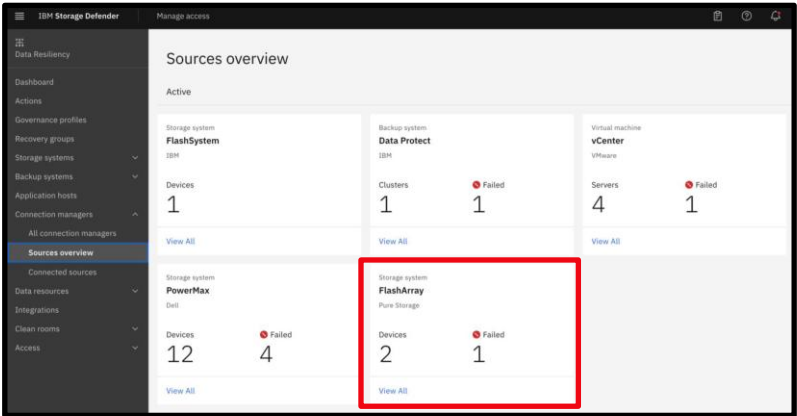


- User can click on “Explore Concepts” on how to create a dependency or remove an application. “Manage Dependencies” will allow users to view and edit applications.

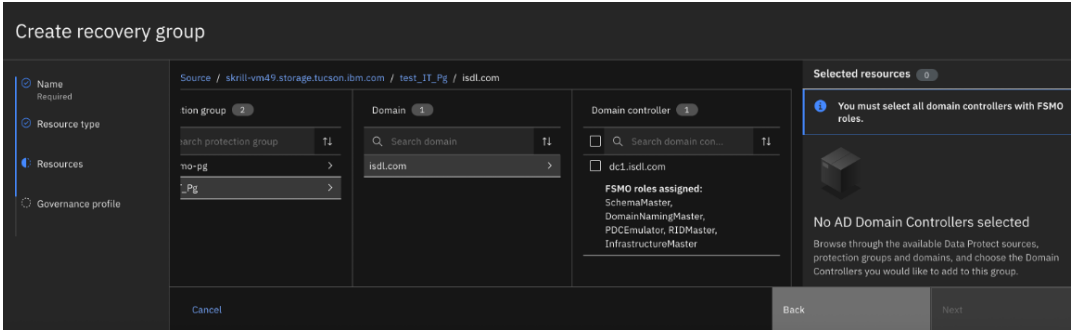


- Can search dependencies on left hand side. On the right you can see root applications and branch applications to create dependencies.
- Ability for users to map dependencies between previously defined Applications for environment visibility, understanding, and prioritization during recovery.

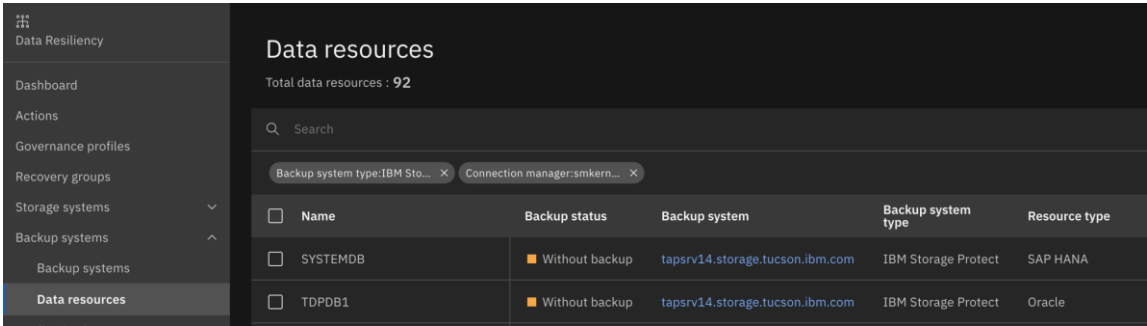
2.0.14 Data source improvements



Pure Storage FlashArray support
New support for indexing of Pure FlashArray //X and //C storage. This extends Defenders storage array coverage across IBM, Dell, and Pure.

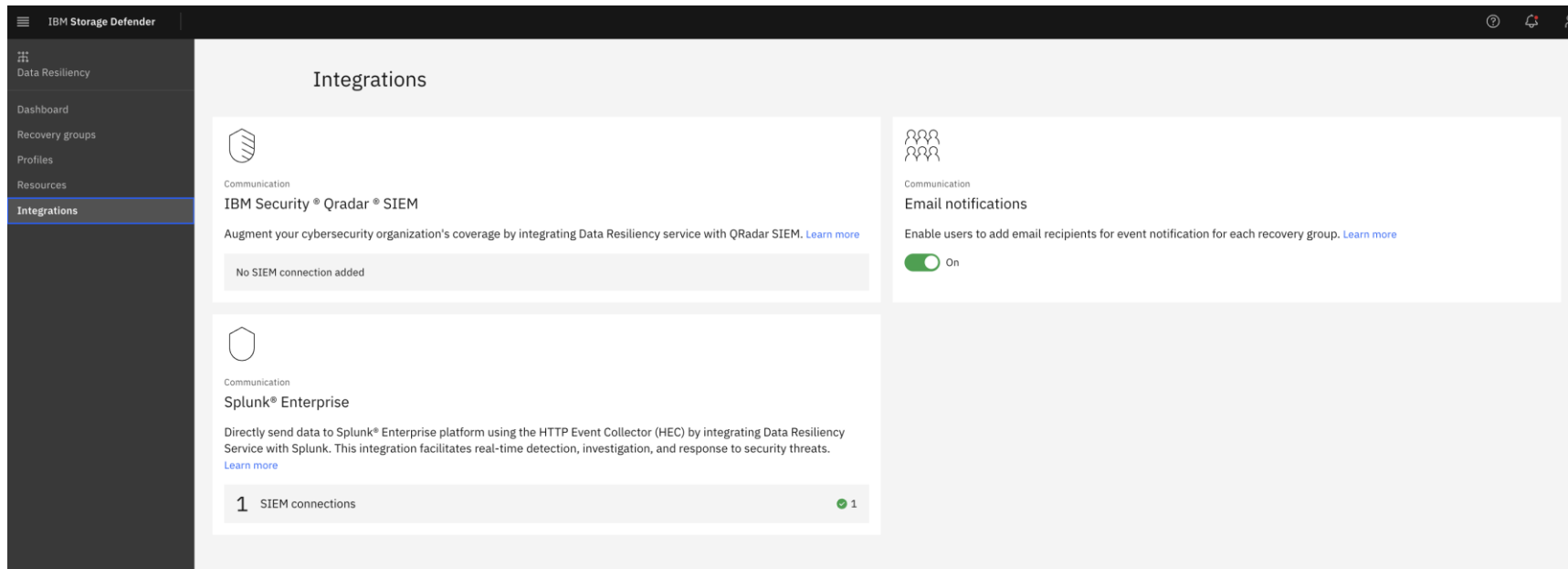


Active Directory registration constraints
When AD is part of the protection profile, Defender now enforces recovery groups to contain all AD servers that have critical FSMO roles. This helps prevent mistakes protecting important critical infrastructure.

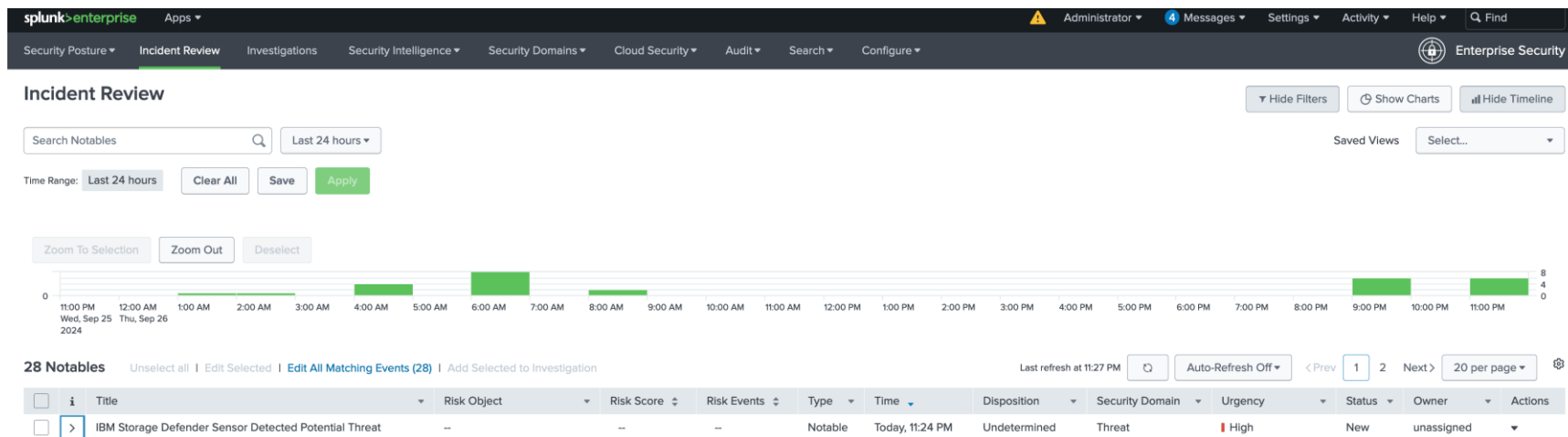


IBM Storage Protect supporting Oracle and SAP HANA in application aware manner
Supports inventory, recovery groups, and governance for Oracle and SAP HANA workloads protected by IBM Storage Protect. This provides enhanced visibility and control of data bases across backup platforms.

2.0.9 Splunk enhancement



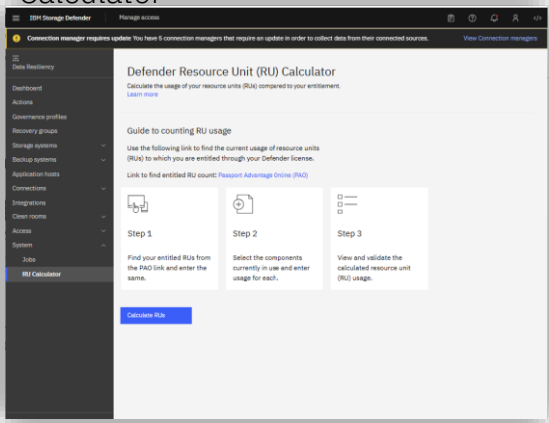
- In 2.0.8, Defender could send alerts to their company's Splunk instance.



- In 2.0.9, the team enhanced the integration to **make it easier** to understand the information flowing to Splunk.

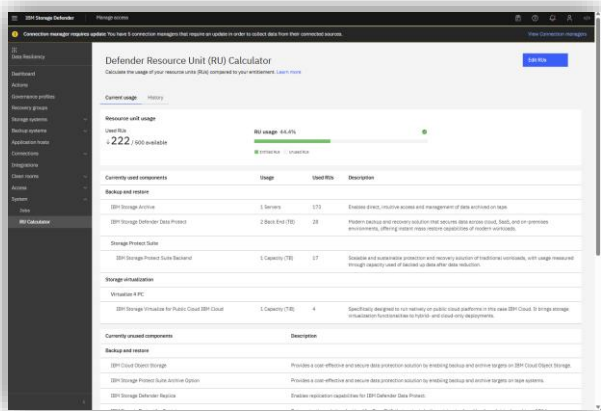
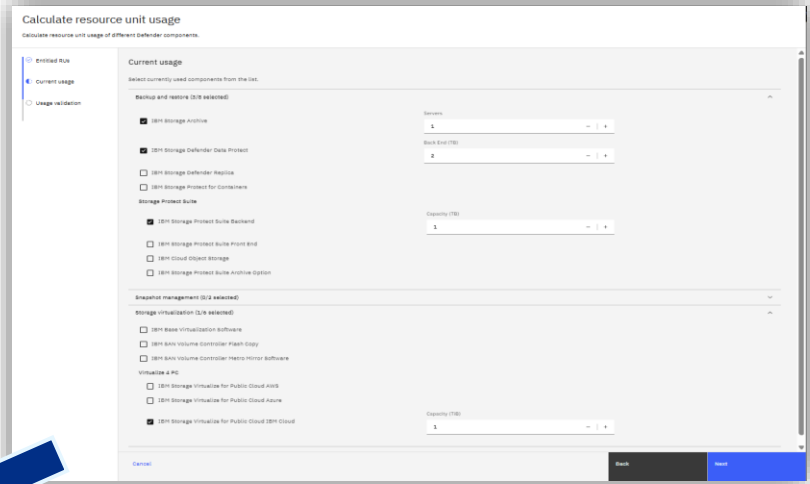
2.0.17- Defender Resource Unit Calculator

Navigate to Data Resiliency -> System -> RU Calculator

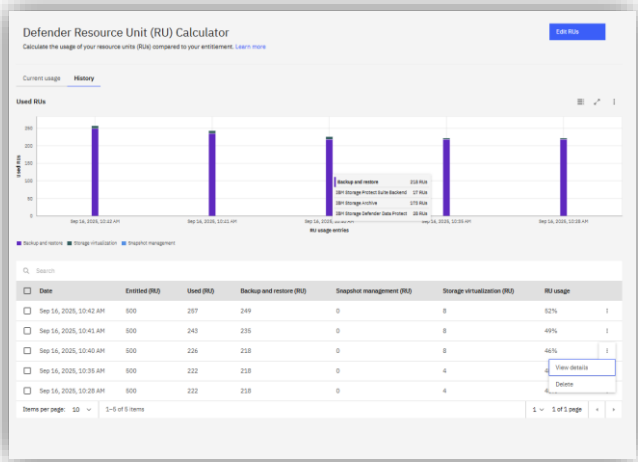


Click “Calculate Rus” button to start

Follow instructions on current usage and estimation



Current Usage Tab: Shows the summary of the most recent provided usage information.



History Tab: Shows the history of user-entered data and calculated RU usage. A bar chart is also displayed to visualize the RU usage.

- A tool for users to compare their Defender entitlements with their usage of Defender components
- To utilize the calculator, you will need to enter your current entitled RUs, then enter estimated data usage for applicable products
- Under the utilization tab, you can review the summary of computed RU usage.
- After submission, there will be two views of the RU calculator: Current Usage and History

How is Data Protect packaged and sold?

SaaS Portal and Cluster



IBM Storage Defender
Data Protect

IBM Storage Defender
Data Protect **Software**
(deployed on 3rd party Defender Nodes)

Defender Data Protect Cluster Nodes

- Hosted on public clouds (AWS EC2, Azure VM, Google)
- Hosted on-prem using certified 3rd party hardware/platform (Defender [3rd party] HW Nodes)



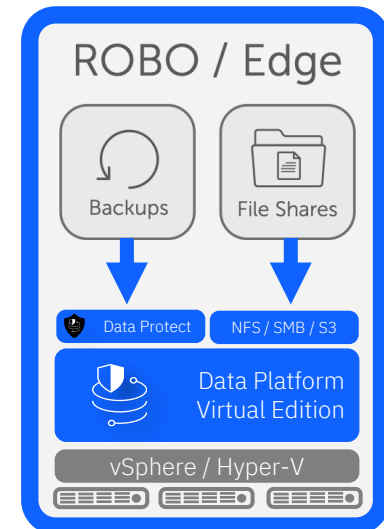
IBM Storage Defender
Data Protect HW
(deployed on IBM Ready Nodes)

Hardware Ready Nodes for Defender

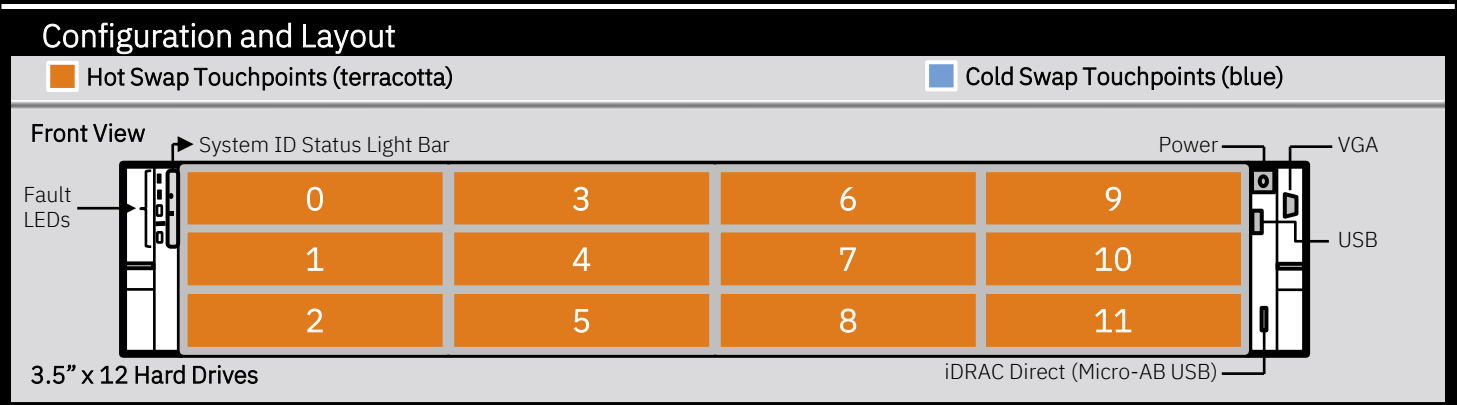
- Hosted on-prem
- Sold through IBM
- IBM support is single point of contact for HW and Defender SW



IBM Storage Defender
Data Protect **Virtual Edition**
(hosted on virtual machine)
Limited Functionality for constrained
Environments



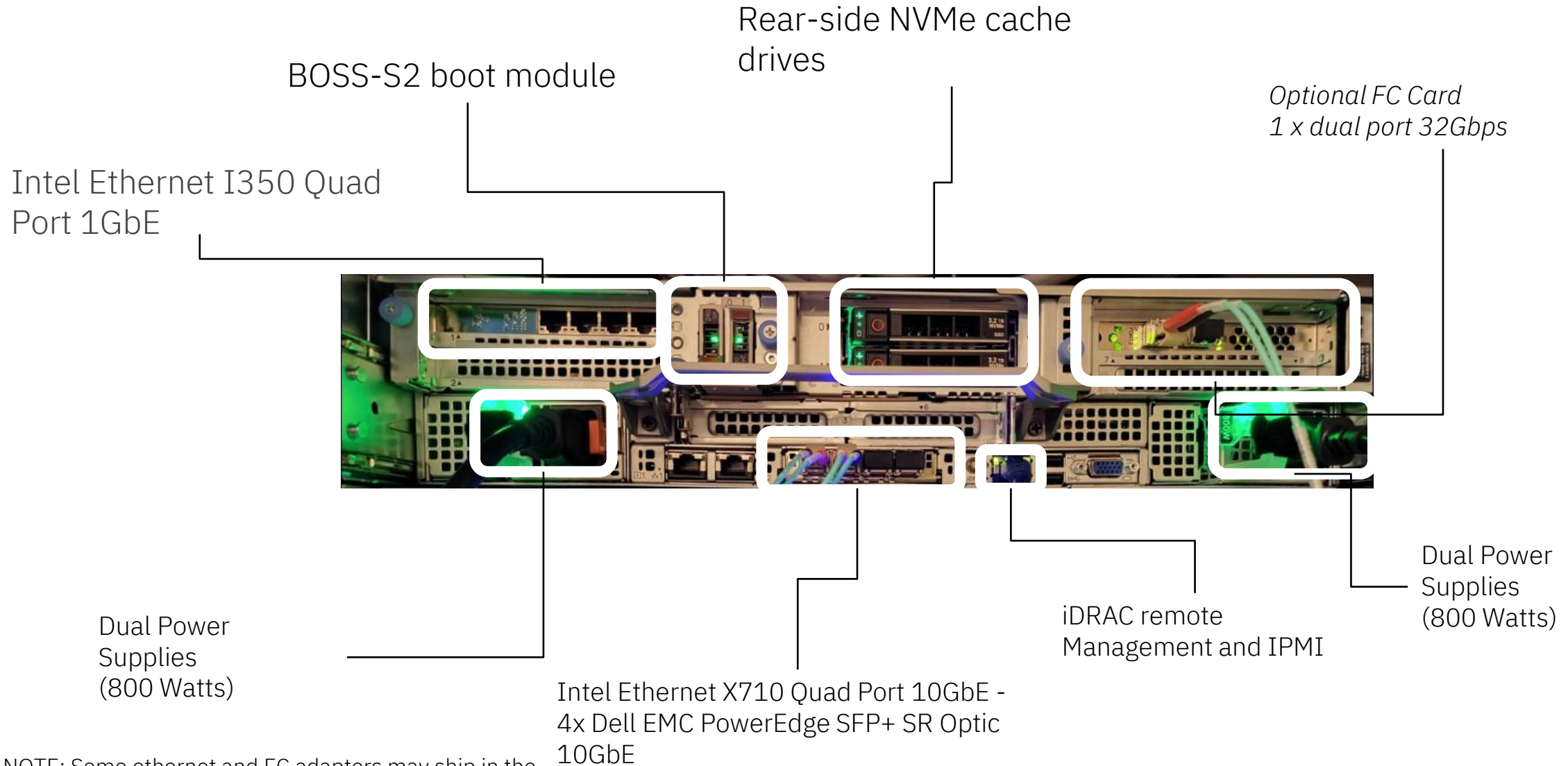
IBM Storage Defender Ready Node front view



- Network
- Intel Ethernet X710 Quad Port
10GbE SFP+, OCP NIC 3.0 included:
- 4x Dell EMC PowerEdge SFP+ SR Optic 10GbE 850nm
 - *Optional FC Card – 1 x dual port 32Gbps*
 - Front-side drives are SAS ISE 12Gbps 7.2K 512e 3.5in Hot-Plug

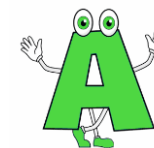
PSU	Class	Heat dissipation (maximum)	Frequency	Voltage	Peak power	N/A	N/A	Peak power	N/A	Current
					High line/- 72 VDC	High line/- 72 VDC	High line/ 240 VDC	Low line/- 40 VDC	Low line/- 40 VDC	
800 W Mixed Mode	N/A	3139 BTU/hr	N/A	240 V	1360 W	800 W	800 W	1360 W	800 W	3.8 A

IBM Storage Defender Ready Node rear view



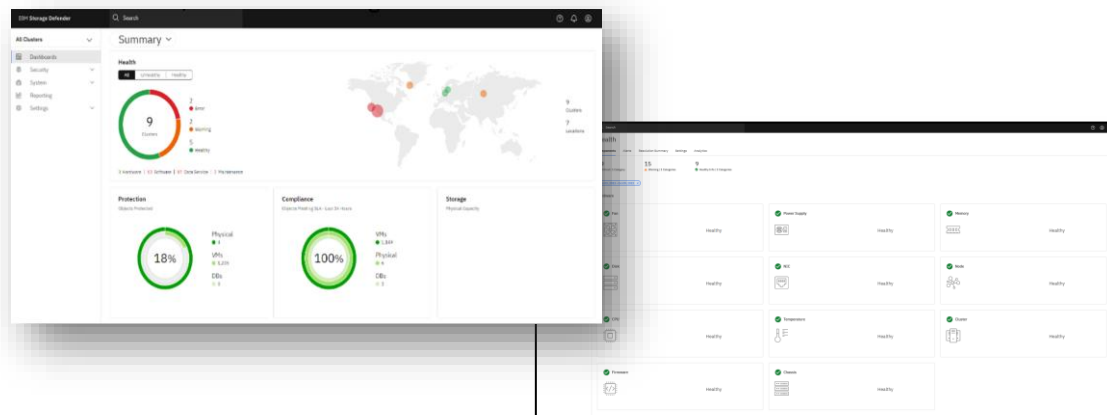
NOTE: Some ethernet and FC adapters may ship in the same models as half-height vs. full height cards

IBM Storage Ready Nodes for IBM Storage Defender



IBM Storage Ready Node for IBM Storage Defender Data Protect

- Nodes for Defender Data Protect scale-out storage cluster
- Interlocked with OEM partner on optimized configurations



2U Generation 15 Models

Models	Size	HDD	NVMe	Processor	Memory
R750	96TB	12 x 8TB SAS	2x3.2TB	2x Intel Xeon 16 core	128GB
R750	192TB	12 x 16TB SAS	2x6.4TB	2x Intel Xeon 16 core	128GB

2U Generation 16 Models

Models	Size	HDD	NVMe	Processor	Memory
R760XL	96TB	12 x 8TB SAS	2x3.2TB	2x Intel Xeon 16 core	128GB
R760XL	192TB	12 x 16TB SAS	2x6.4TB	2x Intel Xeon 16 core	128GB

1U Server Models

Model	Size	HDD	E3.S SSD	Processor	Memory
R6625XL	16TB	4 x 4TB SAS	2x3.84TB	2x AMD EPYC 16 core	128GB
R6625XL	32TB	4 x 8TB SAS	2x3.84TB	2x AMD EPYC 16 core	128GB
R6625XL	48TB	4 x 12TB SAS	2x3.84TB	2x AMD EPYC 16 core	128GB
R6625XL	64TB	4 x 16TB SAS	2x3.84TB	2x AMD EPYC 16 core	128GB

Optional Fibre Channel HBA available with initial order

Optional Fibre Channel HBA add-on available soon

IBM Storage Defender Ready Node use cases



Multi-use cluster nodes

Generation 15

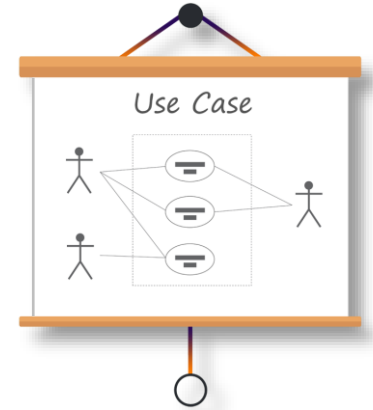
Model	Size	HDD	SSD	Processor	Memory
R750	96TB	12 x 8TB SAS	NVMe 2x3.2TB	2x Intel Xeon 16 core	128GB

Generation 16

Model	Size	HDD	SSD	Processor	Memory
R760XL	96TB	12 x 8TB SAS	NVMe 2x3.2TB	2x Intel Xeon 16 core	128GB
R6625XL	16TB	4 x 4TB SAS	E3.S 2x3.84TB	2x AMD EPYC 16 core	128GB
R6625XL	32TB	4 x 8TB SAS	E3.S 2x3.84TB	2x AMD EPYC 16 core	128GB
R6625XL	48TB	4 x 12TB SAS	E3.S 2x3.84TB	2x AMD EPYC 16 core	128GB
R6625XL	64TB	4 x 16TB SAS	2x3.84TB	2x AMD EPYC 16 core	128GB

Use Cases;

- Normal DP Cluster
- DR Cluster
- Replication Cluster
- Data Vault Cluster



Large Block / alternate use cluster nodes

Generation 15

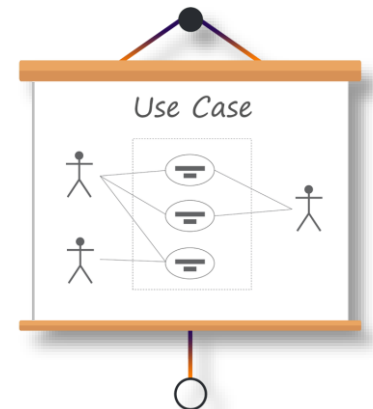
Model	Size	HDD	NVMe	Processor	Memory
R750	192TB	12 x 16TB SAS	2x6.4TB	2x Intel Xeon 16 core	128GB

Generation 16

Model	Size	HDD	NVMe	Processor	Memory
R760XL	192TB	12 x 16TB SAS	2x6.4TB	2x Intel Xeon 16 core	128GB

Use Cases;

- Replication Cluster
- Data Vault Cluster
- Fan in cluster target



How to progress your Defender opportunities ?

1

Enable yourself & your channel partner ...

- [IBM Storage Defender Level 1](#) training for IBMers &
- [IBM Storage Defender Data Protect Level 2](#) training for IBMers
- [IBM Storage Defender Level 1](#) training for BPs
- [IBM Storage Defender Data Protect Level 2](#) training for BPs

2

IPAI - IBM Partner Incentive Program

- IBM Partner Advantage URL :
<https://ibm.biz/IBMPartnerAdvantage>
- IBM Partner Advantage Terms and Conditions:
<https://ibm.biz/IPAIProgram>
- IBM partner Advantage Eligible Product List :
<https://ibm.biz/IPAISell>
- IBM **Integrity Training**: Course: DL18115G: Business Partner Integrity Training - IBM Training - Global
- For all support queries send an email to
service@ibmpartneradvantage.com

Köszönöm a megtisztelő figyelmet!

Gergely Ferenc
IBM HW Presales & BDM
Arrow ECS Kft.
Ferenc.Gergely@arrow.com,
+36 30 121 8007