IBM Storage Scale Resiliency Services

IBM Storage Scale German User Meeting 2023
Sindelfingen, Germany – March 22-23, 2023

Ted Hoover
Product Manager, Storage for Data and AI

Cyber resilience and cyber security

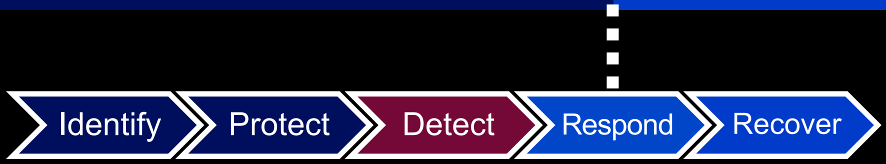
Organizations need the means to respond and recover from an attack

Cyber security	Cyber resilience

Ideally, an organization should be both cyber secure and cyber resilient

Cyber security is about prevention; it’s about trying to keep the bad actors out of your environment

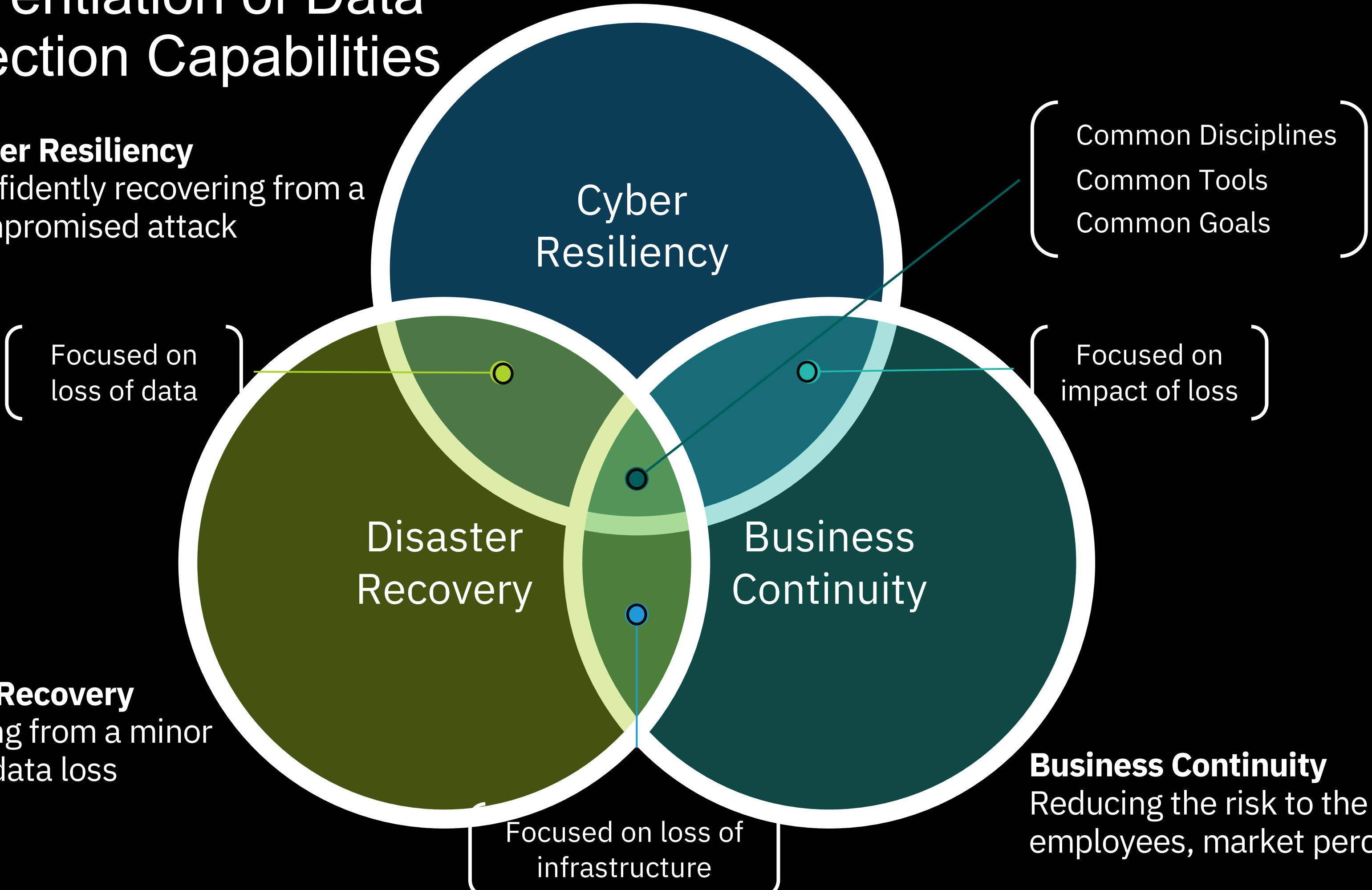
Cyber resilience is about an organization’s ability to continue operations despite a cyber-incident



Holistic Data Security requires seamless operation and coordination across both

Differentiation of Data Protection Capabilities

Cyber Resiliency
Confidently recovering from a compromised attack

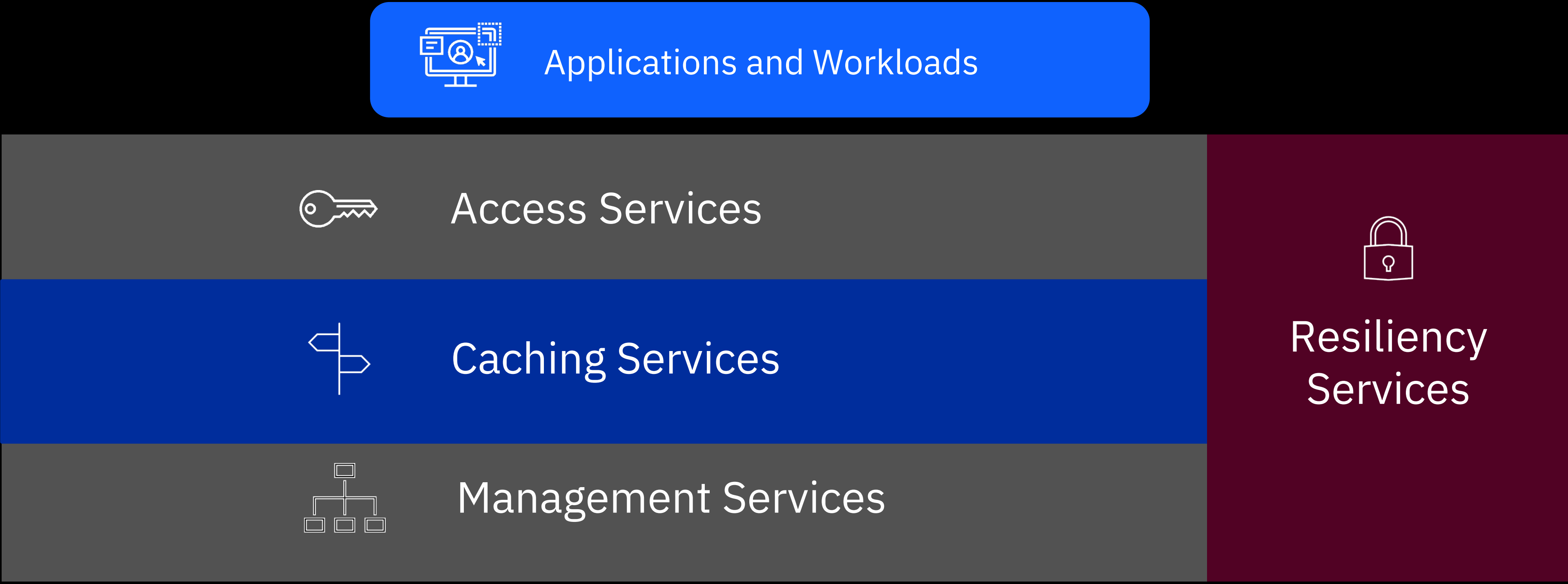


Disaster Recovery
Recovering from a minor to major data loss

Business Continuity
Reducing the risk to the business, employees, market perception, etc

IBM Global Data Platform for Unstructured File & Object Data

Unstructured Data Services Framework



Applications and Workloads

Access Services

Caching Services

Management Services

Resiliency Services

Data Resiliency Services - Active Protection for Cyber Resiliency

IDENTIFY

- Cyber Resiliency Assessment Tool, Probes 100s of different controls and best practices link
- Cyber Incident Response Storage Assessment (CIRSA)

PROTECT

- Multifactor Auth, RBAC, Privileged Access Monitoring (IBM Security Verify)
- Safeguarded Copy, Logical air gap
- Scan snapshots for signs of ransomware (CyberVault)
- Log all Admin & user actions

IBM Global Data Platform

DETECT

- QRadar and Splunk SEIM integration
- File Audit Logging, Watch Folders
- Analyze backup data for signs of ransomware (Storage Protect)
- Reporting: QRadar User behavior analytics

RECOVER

- Instant access with Storage Scale AFM
- Storage Scale and Storage Protect – recover multi-petabyte filesystems in hours
- CyberVault 4Q22
- QRadar Incident Forensics

RESPOND

- Automated action upon threat detection (QRadar)
  - Snapshot, Block Session , Etc..
- Alerts automatically prioritized based on the severity of the threat and criticality of the assets involved

Capabilities for the NIST Cybersecurity framework

Identify: Take an assessment

Storage Cyber Resiliency Assessment Tool

No-charge assessment

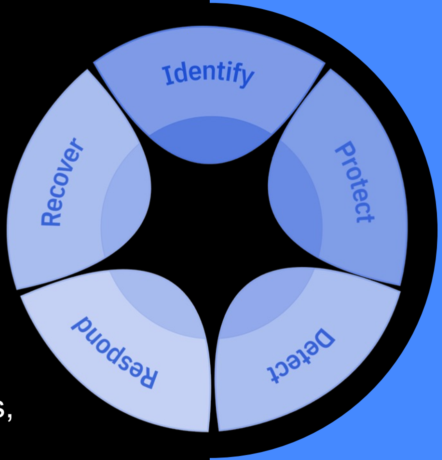
Helps assess your current state

Identifies gaps, strengths, and weaknesses against best practices

Outcomes

- Identify blind spots and recommended areas for improvement
- Discover use of existing solutions, integrations, and overlaps that can be fine-tuned
- Create customized cyber resilience strategy

To request an assessment, contact your IBM Sales Rep or Business Partner, or send an email to the following address: Request an assessment.



Cyber Incident Response Storage Assessment

Identifies strategic cyber resiliency goals

Overview of storage and current cyber resiliency capabilities

Identifies gaps and exposures

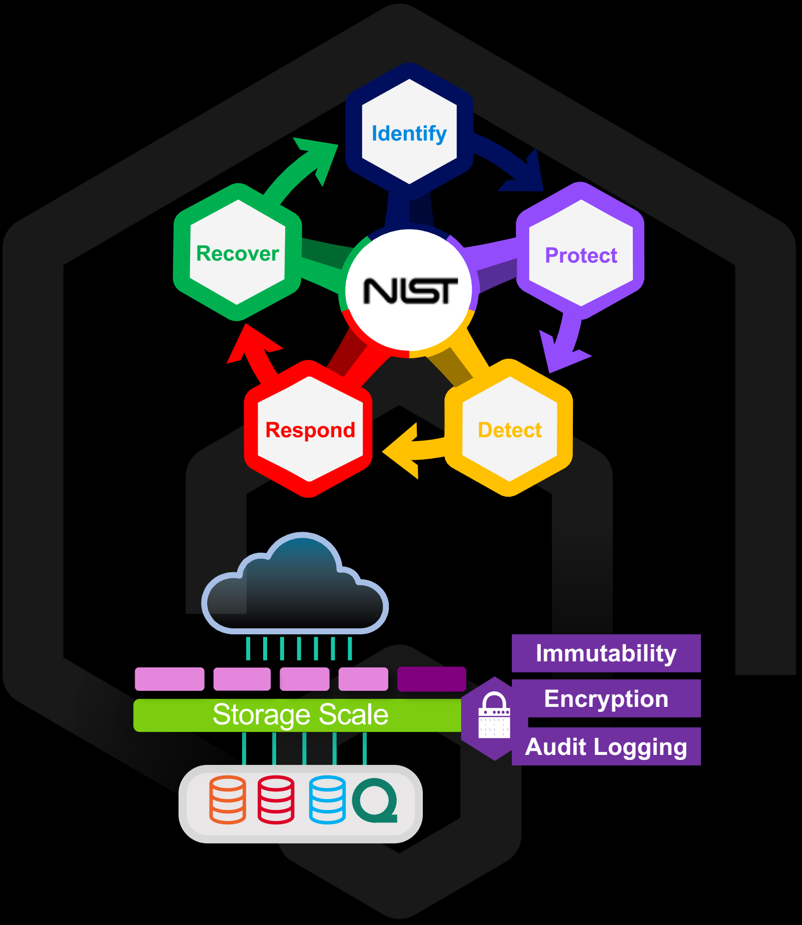
Provides recommendations and highlights best practices

Outcomes

- Develops a cyber resiliency plan that aligns storage infrastructure capabilities and business requirements
- Provides a prioritized recommendations roadmap

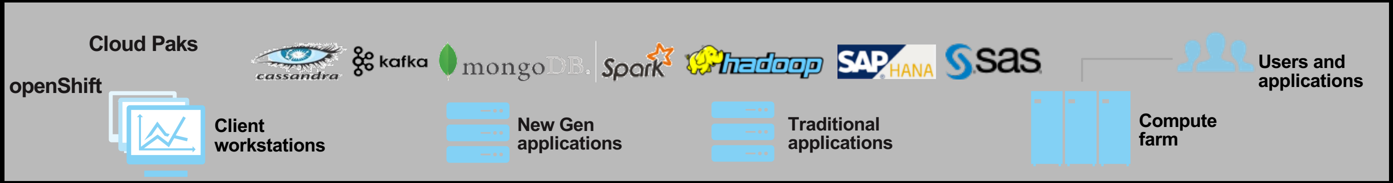
Storage Scale Security and Cyber Resiliency

- Centralized authentication and access control
- Data encryption and cryptographically secure erase
- Immutability
- Audit logging
- Data protection through snapshots, replication, backup, and/or disaster recovery
- Data dispersal and erasure code for faster rebuild times
- End-to-end checksum to catch errors
- Integration with Spectrum Storage family
- NIST/FIPS certification



Storage Scale – Providing Data Centric Security to Workloads

Security & Privacy by Design



AI & Analytics

Data Lake

HPC & Data Intensive Workloads

Workloads

Comprehensive Data Security

Industry Compliance

- GDPR
- HIPAA
- FFIEC
- PCI-DSS
- LGPD & CCPA
- ISO 27040-2016
- NIST/FIPS

Features

- Filesystem Encryption
- Secure Delete
- Immutability
- FAL – File Audit Logging
- Kerberos (NFS, SMB)
- POSIX & NFSV4 ACL
- AD/LDAP support
- RBAC Admin (GUI)
- Admin mode central

Advance Features

- Multi Factor Auth
- Fileset level FAL
- Live Antivirus
- Trusted Boot (5.1.8)
- sudo root admin
- IPv6 (IPSEC)
- SELinux

Ecosystem/Solutions

- Secure AI
- Safeguarded Copy
- CyberVault
- Cloud Pak for Security
- SEIM Integration
  - QRadar
  - SPLUNK
- IBM Secret Server
- IBM Spectrum Discover

Storage Scale Safeguarded Copy

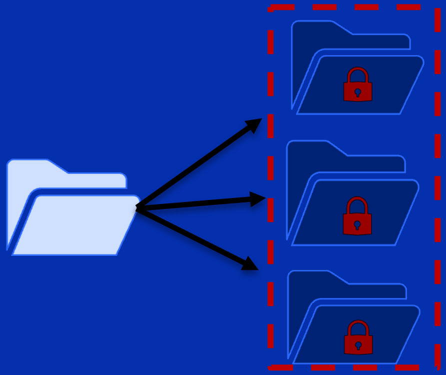
Protect against and recover from a cyber attack

- **Immutability:** Safeguarded Copy for immutable point-in-time copies of production data with policy-based control
- **Isolation**: Air Gap “offline by design” and separation from other files
- **Access Restrictions:** Separation of duties between different administration staff to create a checks and balances approach

Up to 256 Immutable point-in-time **metadata enhanced** copies of data

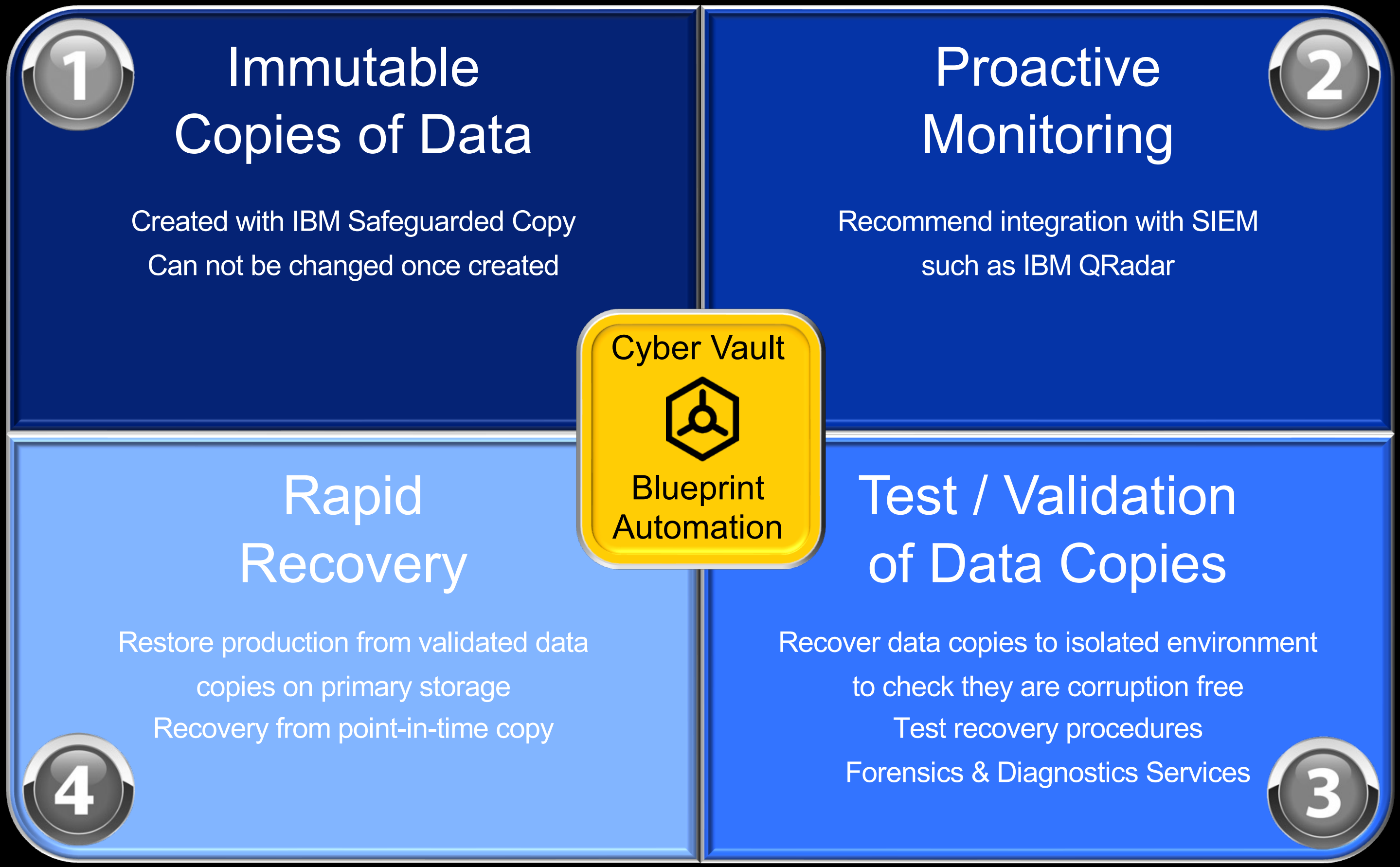
Fast restore from Primary Storage

Prevents modification or deletion of sensitive point-in-time copies due to user error, malicious destruction, or ransomware attack



Data Resiliency Services - Active Protection for Cyber Resiliency

4Q22



1

Immutable Copies of Data

Created with IBM Safeguarded Copy

Can not be changed once created

2

Proactive Monitoring

Recommend integration with SIEM such as IBM QRadar

Cyber Vault

Blueprint Automation

Rapid Recovery

Restore production from validated data copies on primary storage

Recovery from point-in-time copy

4

Test / Validation of Data Copies

Recover data copies to isolated environment to check they are corruption free

Test recovery procedures

Forensics & Diagnostics Services

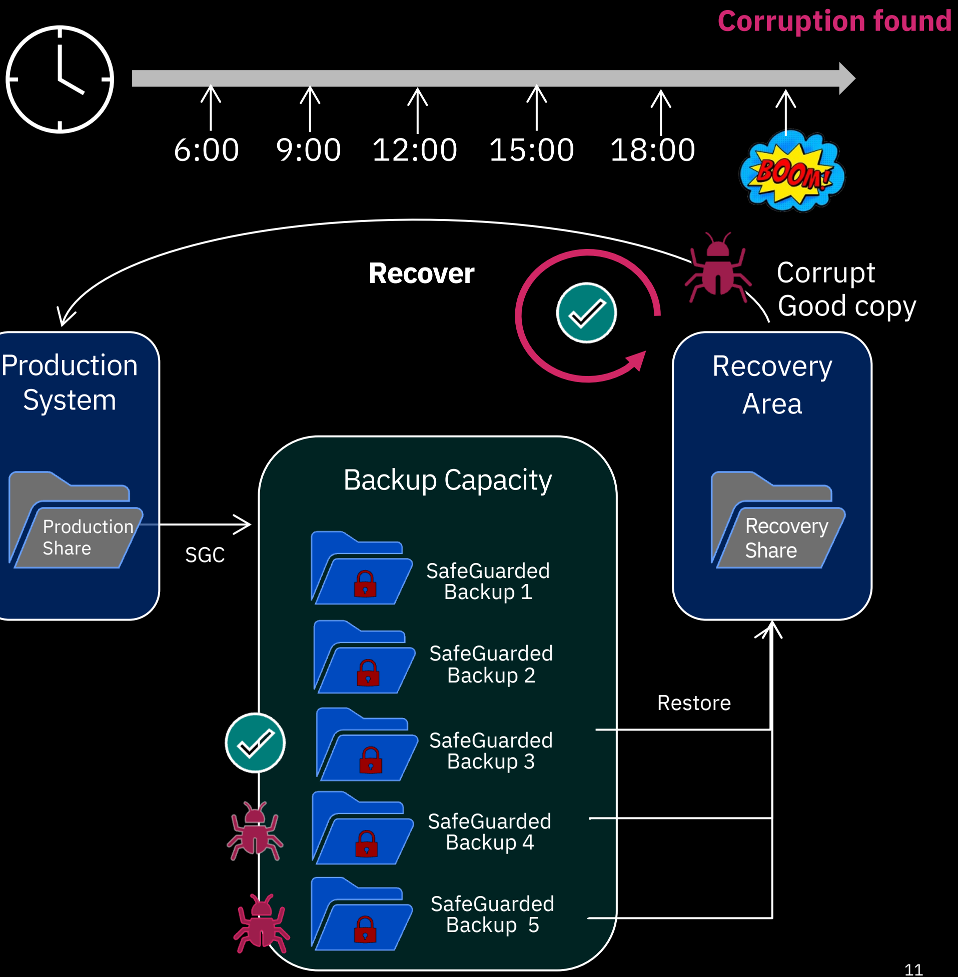
3

IBM Storage Scale provides Safeguarded Copy

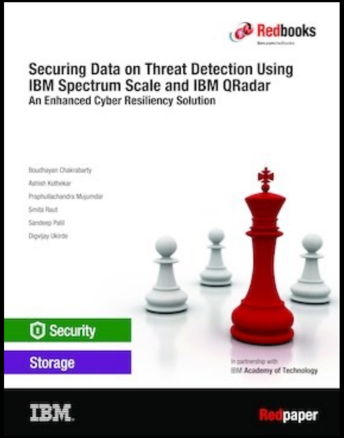
- **Logical Corruption Protection** to prevent sensitive point in time copies of data from being modified or deleted due to errors, destruction or ransomware

- Recovery copies are used for:
  - Data validation
  - Forensic analysis
  - Restoration of production data

- Space efficient Safeguarded snapshots, with up to to 256 snapshots per filesystem which can be;
  - i) scheduled,
  - ii) manual,
  - iii) triggered
- Simple GUI Interface with single screen policies
- Copies stored in an immutable secure recovery location
- Creates separation of duties with a checks and balances system



IBM ESS/IBM Storage Scale Security Related Papers


Redbooks

Securing Data on Threat Detection Using IBM Spectrum Scale and IBM QRadar
An Enhanced Cyber Resiliency Solution

Boudhayan Chakrabarty
Ashish Kothekar
Praphullachandra Mujumdar
Smita Raut
Sandeep Patil
Digvijay Ukirde

Security
Storage

In partnership with
IBM Academy of Technology

IBM. Redpaper

Redbooks

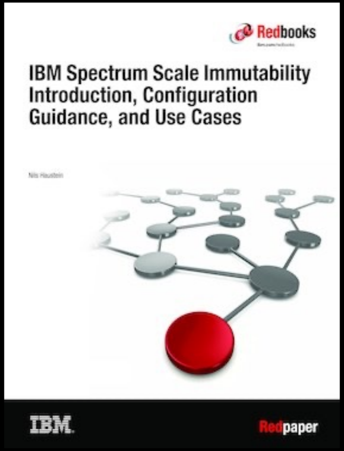
HIPAA Compliance for Healthcare Workloads on IBM Spectrum Scale

Sandeep R. Patil
Sandeep Zende

Security
Storage

In partnership with
IBM Academy of Technology

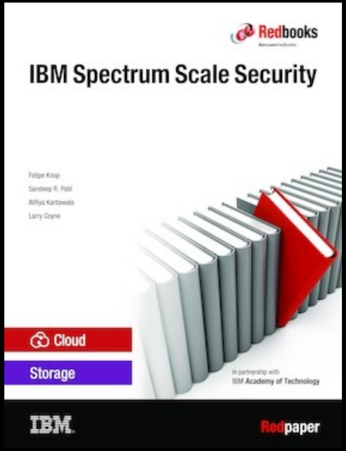
IBM. Redpaper


Redbooks

IBM Spectrum Scale Immutability Introduction, Configuration Guidance, and Use Cases

Nils Haustein

IBM. Redpaper


Redbooks

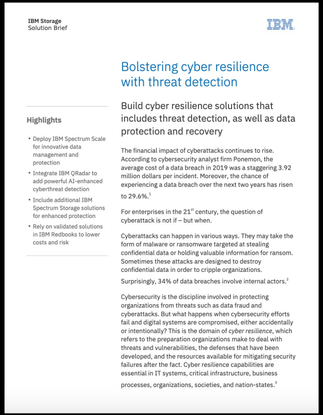
IBM Spectrum Scale Security

Felipe Knop
Sandeep R. Patil
Alifiya Kantawala
Larry Coyne

Cloud
Storage

In partnership with
IBM Academy of Technology

IBM. Redpaper


IBM Storage
Solution Brief

IBM.

Bolstering cyber resilience with threat detection

Build cyber resilience solutions that includes threat detection, as well as data protection and recovery

Highlights

- Deploy IBM Spectrum Scale for innovative data management and protection
- Integrate IBM QRadar to add powerful AI-enhanced cyberthreat detection
- Include additional IBM Spectrum Storage solutions for enhanced protection
- Rely on validated solutions in IBM Redbooks to lower costs and risk

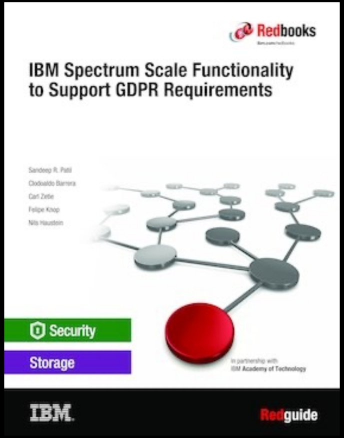
The financial impact of cyberattacks continues to rise. According to cybersecurity analyst firm Ponemon, the average cost of a data breach in 2019 was a staggering 3.92 million dollars per incident. Moreover, the chance of experiencing a data breach over the next two years has risen to 29.6%.[1]

For enterprises in the 21st century, the question of cyberattack is not if – but when.

Cyberattacks can happen in various ways. They may take the form of malware or ransomware targeted at stealing confidential data or holding valuable information for ransom. Sometimes these attacks are designed to destroy confidential data in order to cripple organizations.

Surprisingly, 34% of data breaches involve internal actors.[2]

Cybersecurity is the discipline involved in protecting organizations from threats such as data fraud and cyberattacks. But what happens when cybersecurity efforts fail and digital systems are compromised, either accidentally or intentionally? This is the domain of *cyber resilience*, which refers to the preparation organizations make to deal with threats and vulnerabilities, the defenses that have been developed, and the resources available for mitigating security failures after the fact. Cyber resilience capabilities are essential in IT systems, critical infrastructure, business processes, organizations, societies, and nation-states.[3]


Redbooks

IBM Spectrum Scale Functionality to Support GDPR Requirements

Sandeep R. Patil
Clodoaldo Barrera
Carl Zetie
Felipe Knop
Nils Haustein

Security
Storage

In partnership with
IBM Academy of Technology

IBM. Redguide

Redbooks

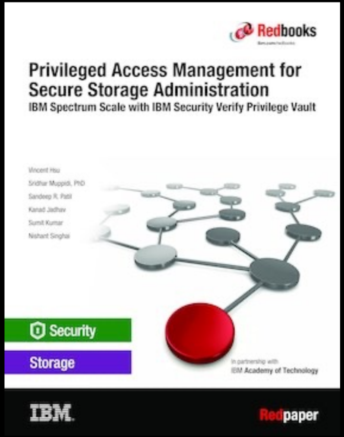
IBM Spectrum Scale and IBM StoredIQ
Identifying and securing your business data to support regulatory requirements

Sandeep R Patil
Sasikanth Eda
Atul V Gore
Nils Haustein

Analytics
Storage

In partnership with
IBM Academy of Technology

IBM. Redpaper


Redbooks

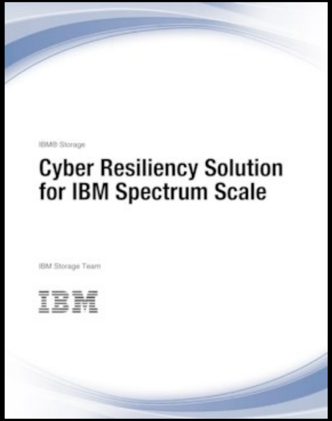
Privileged Access Management for Secure Storage Administration
IBM Spectrum Scale with IBM Security Verify Privilege Vault

Vincent Hsu
Sridhar Muppidi, PhD
Sandeep R. Patil
Kanad Jadhav
Sumit Kumar
Nishant Singhai

Security
Storage

In partnership with
IBM Academy of Technology

IBM. Redpaper


IBM® Storage

Cyber Resiliency Solution for IBM Spectrum Scale

IBM Storage Team

IBM.

IBM