Spectrum Scale User Group, Australia

Secured Storage and Security Solutions with Scale

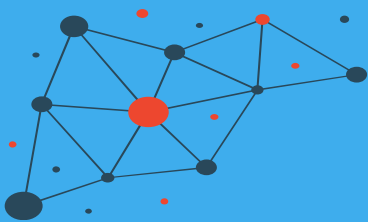Kaustubh Katruwar
Spectrum Scale Development

Mandar Vaidya
Storage Solutions Architect

IBM Spectrum Scale

Join user group:
www.spectrumscaleug.org/join

About the user group

- Independent, work with IBM to develop events

- Not a replacement for PMR!

- Email and Slack community

- www.spectrumscaleug.org/join

IBM CHAMPION

Disclaimer

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.

Outline

- *Secured Storage*

- Security Solutions

- Summary

IBM Spectrum Scale / IBM Elastic Storage Server Security

Data Security

The world's most valuable resource is no longer oil, but DATA

The Economist

Your data can be anywhere

Private cloud | Public cloud | Hybrid cloud | Multicloud

Massive data

Massive insight

Massive value

40% growth in global data generated

2-3% growth in IT spend

Source: Gartner & McKinsey Global Institute

Organizations are facing significant cyber security challenges

Average total cost of a data breech in 2018	Estimated global cost of WannaCry attack	Cost impact for one company impacted by NotPetya	No longer a question of "IF" you'll experience a breach, but "WHEN"
$3.86M	**$8B**	**$310+M**	**Risk**
$200k/hr downtime		206 days — Average amount of time hackers spend inside IT environments before discovery	World Economic Forum Global Risks Report 2019 — Likelihood #5 ranked — Impact #7 ranked

IBM Spectrum Scale - Leading use cases

Delivering the highest levels of scalability and performance with ==security==

Security

A

Storage for AI, Big Data, and Analytics
High performance and scalability

1. Data-intensive technical computing
2. Artificial Intelligence (AI)
3. Big Data and Analytics, Hadoop

B

Data lake, industry applications
Enterprise data architecture

4. "Data lake" unified storage
5. Select ISV and industry solutions
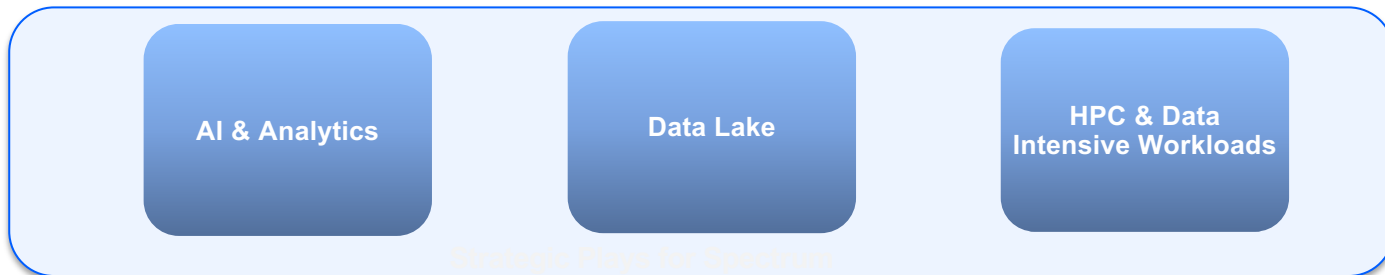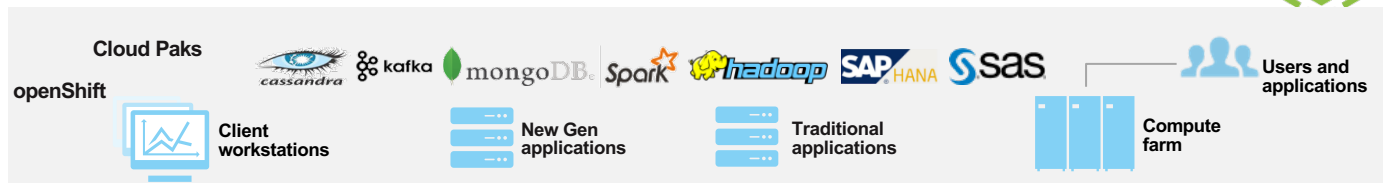
C

Data optimization and resiliency
Enterprise data optimization and data management.
Infrastructure pre-requisites for segments A and B

6. Archive
7. Information Lifecycle Management
8. Back-up / restore

IBM Spectrum Scale - Providing Data Centric Security to Workloads

IBM **Spectrum Scale**

Cloud Paks
openShift

cassandra · kafka · mongoDB · Spark · hadoop · SAP HANA · sas

Users and applications

Client workstations · New Gen applications · Traditional applications · Compute farm

AI & Analytics

Data Lake

HPC & Data Intensive Workloads

Security & Privacy by Design

Comprehensive Data Security

Industry Compliance

- GDPR
- HIPAA
- LGPD & CCPA
- ISO 27040-2016

Features

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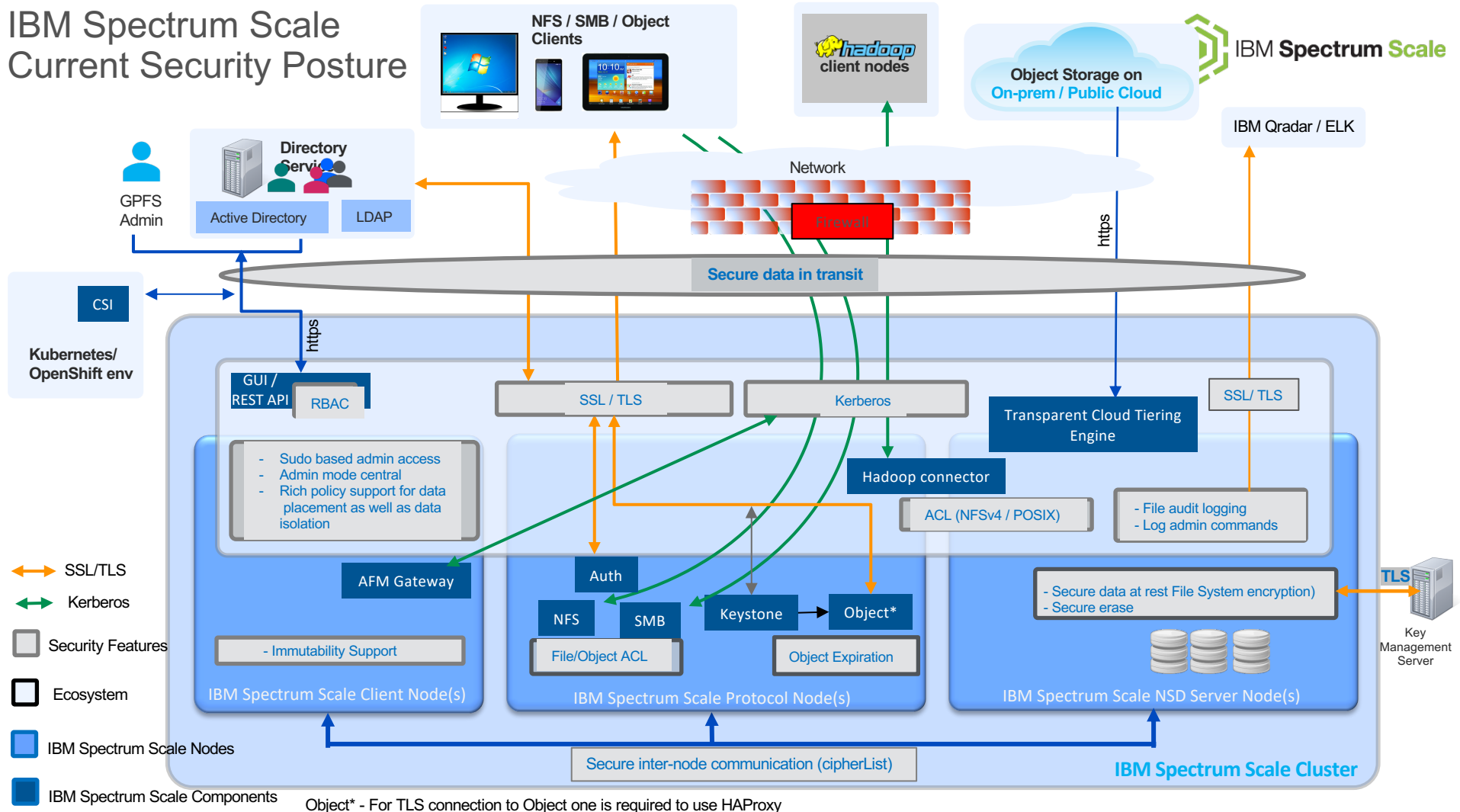- Admin mode central

Advanced Features

- Fileset level FAL
- Antivirus
- Security posture in single pane of glass
- Restricted root admin
- IPv6
- SELinux

Ecosystem/Solutions

- Secure AI
- Cyber Resilience
- SEIM Integration
  - QRadar
  - SPLUNK
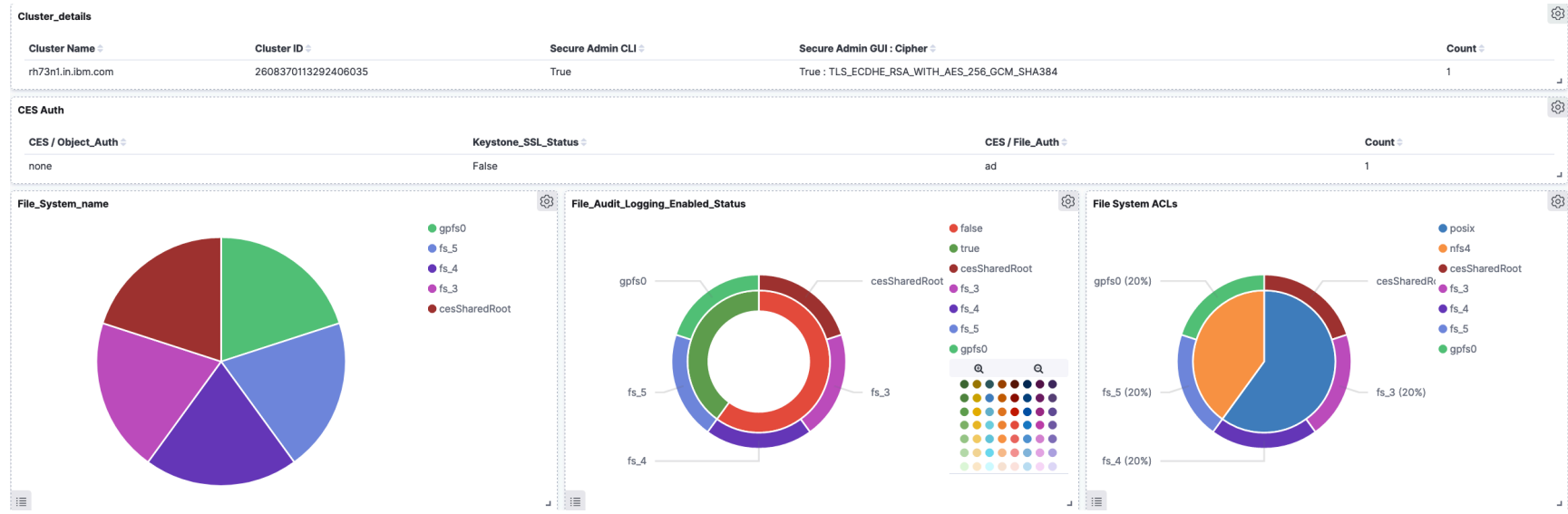- IBM Spectrum Discover

IBM Spectrum Scale Current Security Posture

Object* - For TLS connection to Object one is required to use HAProxy

IBM Spectrum Scale Scorecard - Storage Security Requirements

IBM Spectrum Scale

Key Security Requirement	Available on IBM Spectrum Scale
Policy based encryption for secure data at rest	✓
Policy based selective encryption for secure data in motion	✓
Secure Administration	✓
Secure tiering of data to immutable archive	✓
Continuous Authorization	✓
Continuous Authentication	✓
Data Threat Detection	✓
Audit Logging	✓
Secure Delete	✓
Cyber Resilience of Data	✓
Regulatory Compliance	✓
Security and Privacy by Design	✓

IBM Spectrum Scale Security Posture in Single Pane of Glass – Open Source

IBM Spectrum Scale

Cluster_details

Cluster Name	Cluster ID	Secure Admin CLI	Secure Admin GUI : Cipher	Count
rh73n1.in.ibm.com	2608370113292406035	True	True : TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	1

CES Auth

CES / Object_Auth	Keystone_SSL_Status	CES / File_Auth	Count
none	False	ad	1

File_System_name

- gpfs0
- fs_5
- fs_4
- fs_3
- cesSharedRoot

File_Audit_Logging_Enabled_Status

- false
- true
- cesSharedRoot
- fs_3
- fs_4
- fs_5
- gpfs0

gpfs0 · cesSharedRoot · fs_5 · fs_3 · fs_4

File System ACLs

- posix
- nfs4
- cesSharedRoot
- fs_3
- fs_4
- fs_5
- gpfs0

gpfs0 (20%) · cesSharedRoot · fs_5 (20%) · fs_3 (20%) · fs_4 (20%)

IBM Spectrum Scale and IBM StoredIQ: Identifying and securing your business data to support regulatory requirements (like GDPR and beyond)

Having the appropriate storage for hosting business critical data and the proper analytic software for deep inspection of that data is becoming a necessity, especially for data subject to regulatory compliance.

IBM Spectrum Scale, combined with the data analysis and categorization features of IBM StoredIQ, provide an excellent platform for hosting unstructured business data subject to regulatory compliance guidelines like General Data Protection Regulation (GDPR).
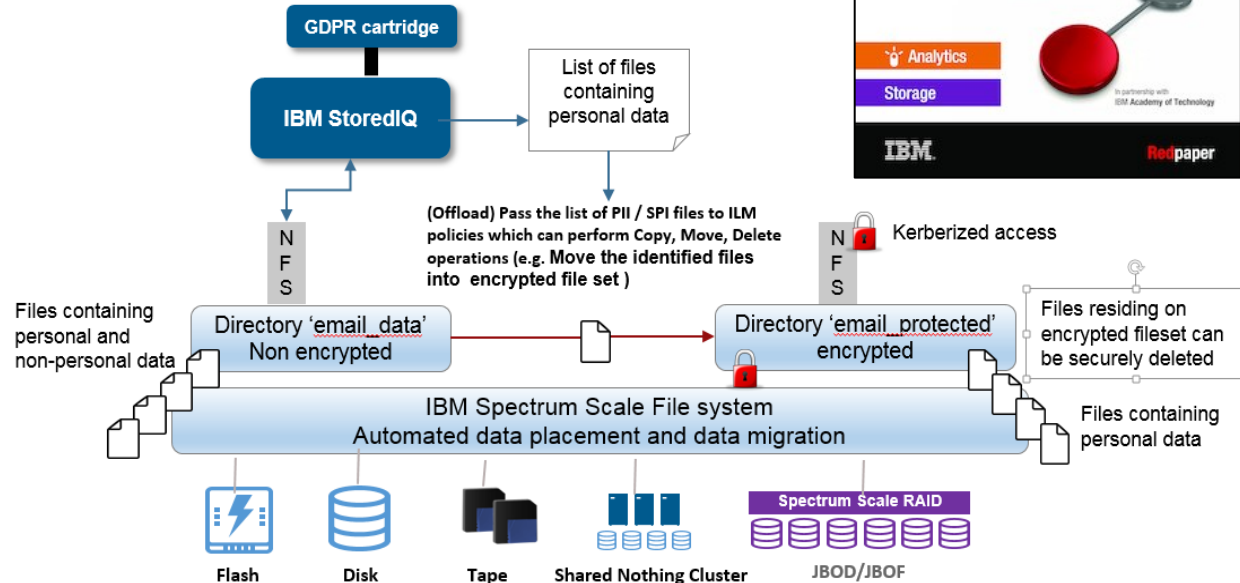
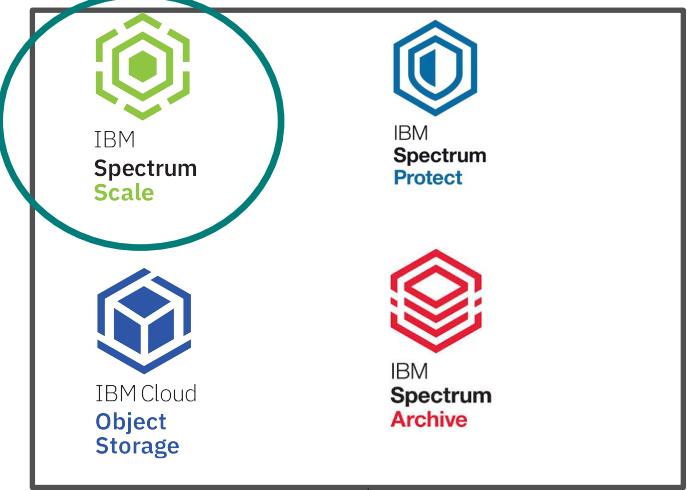# HIPPA Complaint Security Solution :Spectrum Scale Security for Healthcare Workloads

▪ Institutes are deploying artificial intelligent (AI) workloads that are mining the health data (which may include ePHI) to get meaningful insights for enhancement in healthcare and precision medicine

▪ One of the important building blocks of such healthcare solution stack is the underlying storage where the sensitive data (that is, ePHI) is stored.

▪ t is important to understand the HIPAA requirements for storage solutions that are used to host ePHI-related data.

▪ Need for Secure AI solutions that starts with addressing the HIPAA requirements at the storage level and then building up the Secure AI solution stack from there.

▪ IBM Spectrum Scale features aid in the overall heath care solution to be compatible with applicable safeguards required by HIPPA

▪ The Redpaper analyzes all the relevant safeguards from HIPPA compliances and shows how IBM Spectrum Scale security and other features help you meet the requirement

IBM Spectrum Discover with IBM Spectrum Scale – Content Classification Workflow

Policy based, fully automated content inspection and classification
1. Leverage pre-configured terms / regular expressions and classification mappings
2. Create custom terms / regular expressions
3. Modify classification mappings

| PII	Sensitive	Public
SSN	Confidential	Security: None
DOB		
Phone #		

What kind of sensitive data is store in my enterprise?

Need to identify all the documents containing Credit Card Info, SSN, Emails and Phone Numbers.

Where is this data stored?

System metadata

Classification:
PII   PUBLIC
SENSITIVE

Policy Engine:
- Classifier

Capacity Used by **Classification**

public

12000001
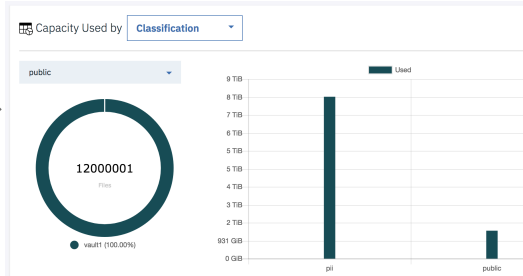
IBM Spectrum Scale CSI Driver for Container Persistent Storage – Run container workloads that require security with peace of mind.

- ✓ Secure administration

- ✓ Ownership of data to ensure Persistent Volume access for non-root containers

- ✓ Allows granular and selective secure data at rest for containers- leveraging Spectrum Scale policies and Kubernetes storage classes

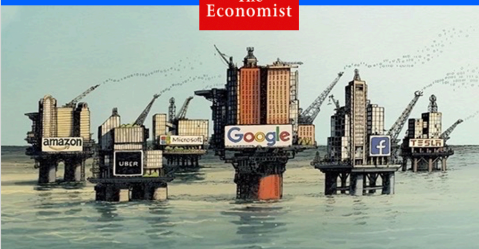- ✓ Allows secure data in motion across the cluster

Cyber Resiliency Solutions for IBM Spectrum Scale

The world's most valuable resource is no longer oil, but DATA

The Economist

Your data can be anywhere

Private cloud | Public cloud | Hybrid cloud | Multicloud

Massive data
Massive insight
Massive value

40% growth in global data generated

2-3% growth in IT spend

Source: Gartner & McKinsey Global Institute

Organizations are facing significant cyber security challenges

| Average total cost of a data breech in 2018	Estimated global cost of WannaCry attack	Cost impact for one company impacted by NotPetya	No longer a question of "IF" you'll experience a breach, but "WHEN"
$3.86M	**$8B**	**$310+M**	**Risk**
$200k/hr downtime		206 days — Average amount of time hackers spend inside IT environments before discovery	World Economic Forum Global Risks Report 2019 — Likelihood #5 ranked, Impact #7 ranked

Cybersecurity is the biggest challenge for board directors
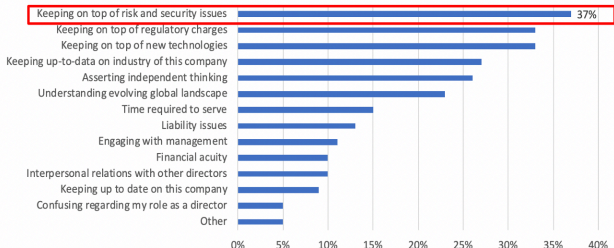
Q: Which of the following do you find **challenging** in your role as a director of this board? (select all that apply)

- Keeping on top of risk and security issues — 37%
- Keeping on top of regulatory charges
- Keeping on top of new technologies
- Keeping up-to-data on industry of this company
- Asserting independent thinking
- Understanding evolving global landscape
- Time required to serve
- Liability issues
- Engaging with management
- Financial acuity
- Interpersonal relations with other directors
- Keeping up to date on this company
- Confusing regarding my role as a director
- Other

(0% 5% 10% 15% 20% 25% 30% 35% 40%)

41%
Increase in cyber attacks in the last year
The New York Times by Emsisoft

2x
Ransomware costs from Q3 to Q4 2019 Average cost per attack in Q4 2019 $84,116

$190,946
Average cost per ransomware attack in Dec. 2019

(Cost per cyber attack in Q4 2019, doubled again in just the last month)

30 hours
Shut down of Coast Guard transfer facility due to cyber attack

Cyber resiliency is an organization's **ability to continue** delivering the intended outcomes despite adverse cyber incidents

1 in 2
Indian firms faced cyber breach in past two years

34%
of data breaches involved internal actors

Planning + Protecting + Testing + Learning

Customers needs broader and more coordinated response

Clients need to protect their business with a resilient, flexible IT infrastructure. **They need to strengthen their business continuity with the right tools, technology and skills to deal with crises.**

They also need to protect and recover from cyber attacks by having a robust cyber recovery plan. And they need secure data storage to ensure smooth operations of their environments if a crisis impacts physical access to data centers.

As a result, areas such as network resiliency, crisis management, employee safety, client engagement and zero-touch operations are paramount.

Cyber Security Vs Cyber Resiliency:

An ideal environment should be both cyber secure and cyber resilient. You want both!

- **Security:** "Lock the doors! Prevent intruders!"
- **Prevention**: It's about trying to keep the bad actors out of your environment in the first place.

- **Resiliency:** "My locks are broken! How do I replace my property?"
- **Recovery:** once the bad actors are in, does the organization have the means to recover quickly and continue business operations

68% act only after disaster

Most enterprises have limited proactive plans to move critical workloads in the event of a disaster. 68% act only after a disaster.

SIEM
(Security Information Event Management)

- Provides real-time security event management for cyber security, network and applications.

- Early detection of attacks and breaches

Main functions:
- Data Aggregation
- Correlation
- Alerting
- Dashboards
- Compliance
- Retention
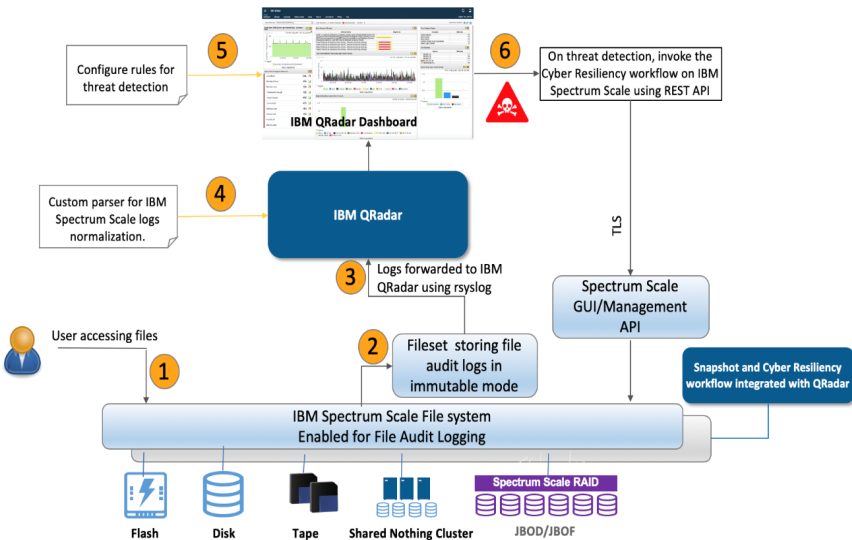- Analysis

Storage for Data and AI Alignment:
- Splunk => COS
- IBM Qradar => Spectrum Scale

Source: Gartner (February 2020)

Enhanced Cyber Security and Proactive Cyber Resilience

**Proactive Data Protection on Threat Detection
Proactive Cyber Resilience**

Configure rules for threat detection ⑤

⑥ On threat detection, invoke the Cyber Resiliency workflow on IBM Spectrum Scale using REST API

IBM QRadar Dashboard

Custom parser for IBM Spectrum Scale logs normalization. ④

IBM QRadar

TLS

③ Logs forwarded to IBM QRadar using rsyslog

Spectrum Scale GUI/Management API

User accessing files

① ② Fileset storing file audit logs in immutable mode

Snapshot and Cyber Resiliency workflow integrated with QRadar

IBM Spectrum Scale File system Enabled for File Audit Logging

Flash   Disk   Tape   Shared Nothing Cluster   Spectrum Scale RAID   JBOD/JBOF

5 mins Demo link:
https://ibm.ent.box.com/s/spk5nmovv4rufbper4f5m0wdk4utc0bs

Business Need:

- Need for Cyber Resiliency - a key storage solution play.

- Proactive trigger for Cyber Resiliency Workflow on Threat Detection

- Lead Spectrum Scale as a market leader in storage security/Cyber Resiliency with IBM QRadar Integration.

- Monitoring Spectrum Scale file system for potential attacks to the data stored therein

- IBM QRadar users required long-term logs retention on a Spectrum Scale file system leveraging (HSM) for compliance.
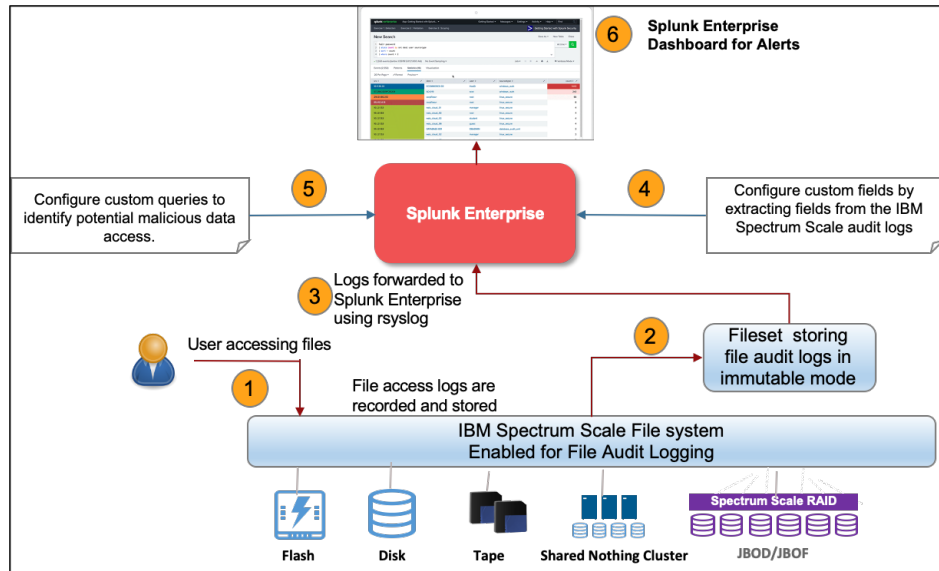
Solution:

- Integration of IBM Spectrum Scale data protection (snapshot/backup) with threat detection security software (IBM QRadar for security)

- When IBM QRadar detects a threat, data on IBM Spectrum Scale is automatically protected.

- The cyber resiliency workflow is automatically triggered.

- Spectrum Scale addresses long-term logs retention requirements via NFS transferring from QRadar appliance to Sp. Scale, allowing tiering to object storage in IBM COS or to lower-cost storage Tape (including WORM Tape immutability).

Enhanced Threat detection with Splunk Enterprise

Enhanced threat detection by Splunk Enterprise using Spectrum Scale File Audit Logs

6 — Splunk Enterprise Dashboard for Alerts

5 — Configure custom queries to identify potential malicious data access.

Splunk Enterprise

4 — Configure custom fields by extracting fields from the IBM Spectrum Scale audit logs

3 — Logs forwarded to Splunk Enterprise using rsyslog

User accessing files

1

2 — Fileset storing file audit logs in immutable mode

File access logs are recorded and stored

IBM Spectrum Scale File system Enabled for File Audit Logging

Flash   Disk   Tape   Shared Nothing Cluster   Spectrum Scale RAID   JBOD/JBOF

Solution Brief:
https://www.ibm.com/downloads/cas/1OLV7L3Z

Business Need:

- Need for Cyber Resiliency - a key storage solution play.

- Lead Spectrum Scale as a market leader in storage security/Cyber Resiliency with Splunk Enterprise Integration.

- Monitoring Spectrum Scale file system for potential attacks to the data stored therein

- Proactive alerts to Splunk administrators on Threat Detection

Solution:

- Ability to send Spectrum Scale File Audit Logs (FAL) to Splunk Enterprise and Splunk Enterprise for Security for threat detection using rsyslog.

- Easy to configure custom queries based on customized Spectrum Scale fields.

- When Splunk Enterprise detects a threat, alerts are generated as per severity.

IBM Spectrum Scale with IBM Spectrum Protect: Cyber Resiliency Solution
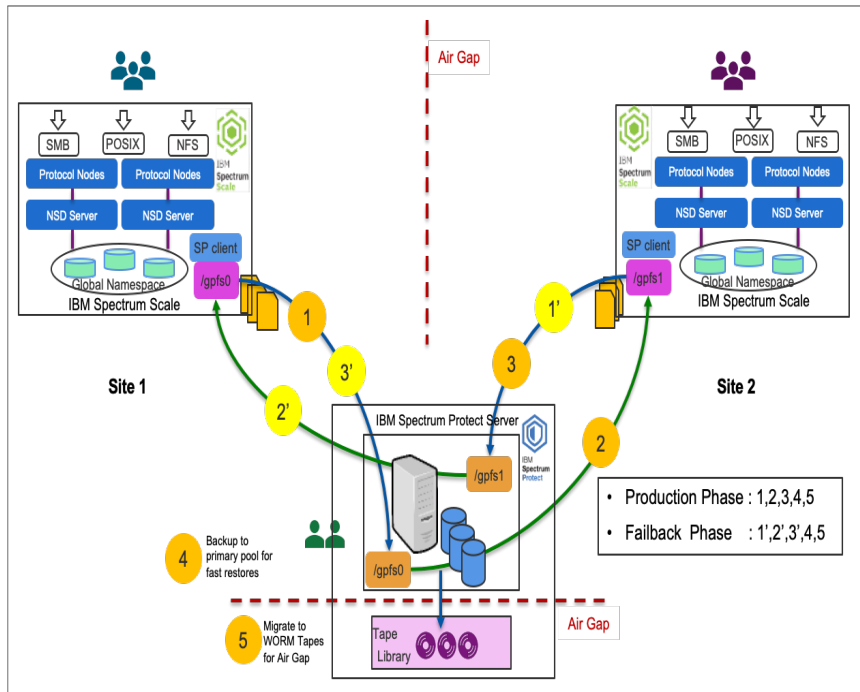
Business Need:

- Need for Cyber Resiliency for Spectrum Scale – an essential storage solution play.

- Airgap solution for the data stored in Spectrum Scale

- Minimize business impact in case of disaster and cyber attacks

Solution:

Cyber Resiliency Solution for Spectrum Scale using its integration with Spectrum Protect and as per NIST framework.

Key Takeaways

- Implemented as per NIST Framework.

- Flexible solution, which allows creating various air-gap provisions for data protection.

- Ability to recover data and bring up applications on both sites.

- Solution implemented using multiple IBM product offerings integrations (IBM Spectrum Protect, IBM Tapes for immutability)

Thank you!

IBM Spectrum Scale

Please help us to improve Spectrum Scale with your feedback
- If you get a survey in email or a popup from the GUI, please respond
- We read every single reply

Provide Feedback ✕

Tell IBM What You Think

Let us know what you think about IBM Spectrum Scale. It takes only a couple of minutes for you to help us improve our service. ☐↗ IBM Privacy Policy

Not Now   ↗ Provide Feedback

Spectrum Scale User Group

The Spectrum Scale (GPFS) User Group is free to join and open to all using, interested in using or integrating IBM Spectrum Scale.

The format of the group is as a web community with events held during the year, hosted by our members or by IBM.

See our web page for upcoming events and presentations of past events. Join our conversation via mail and Slack.

www.spectrumscaleug.org