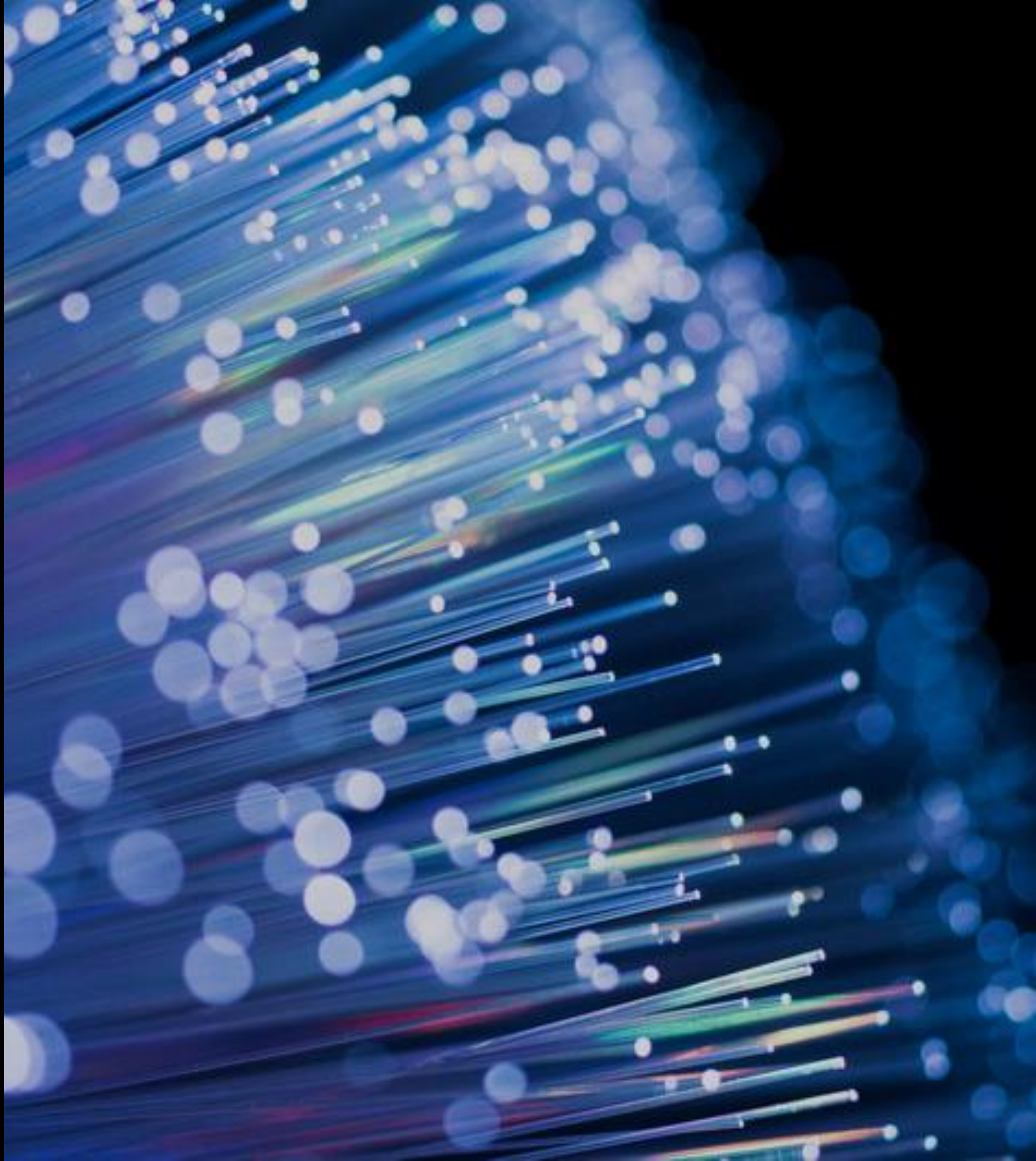
Resiliency Services

Cybervault for IBM Storage Scale



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.

Security Services Provide End to End Protection

Identify

Protect

← Pre-Attack →

Detect

← Peri-Attack →

Respond/ Recover

← Post-Attack →

Attack Surface Reduction

With IBM’s Cyber Resilience Assessment

Attack Defense

With Safeguarded Copy air-gapped solutions and and Data Security Services IBM provides all the tools required to protect your data

Attack Prevention

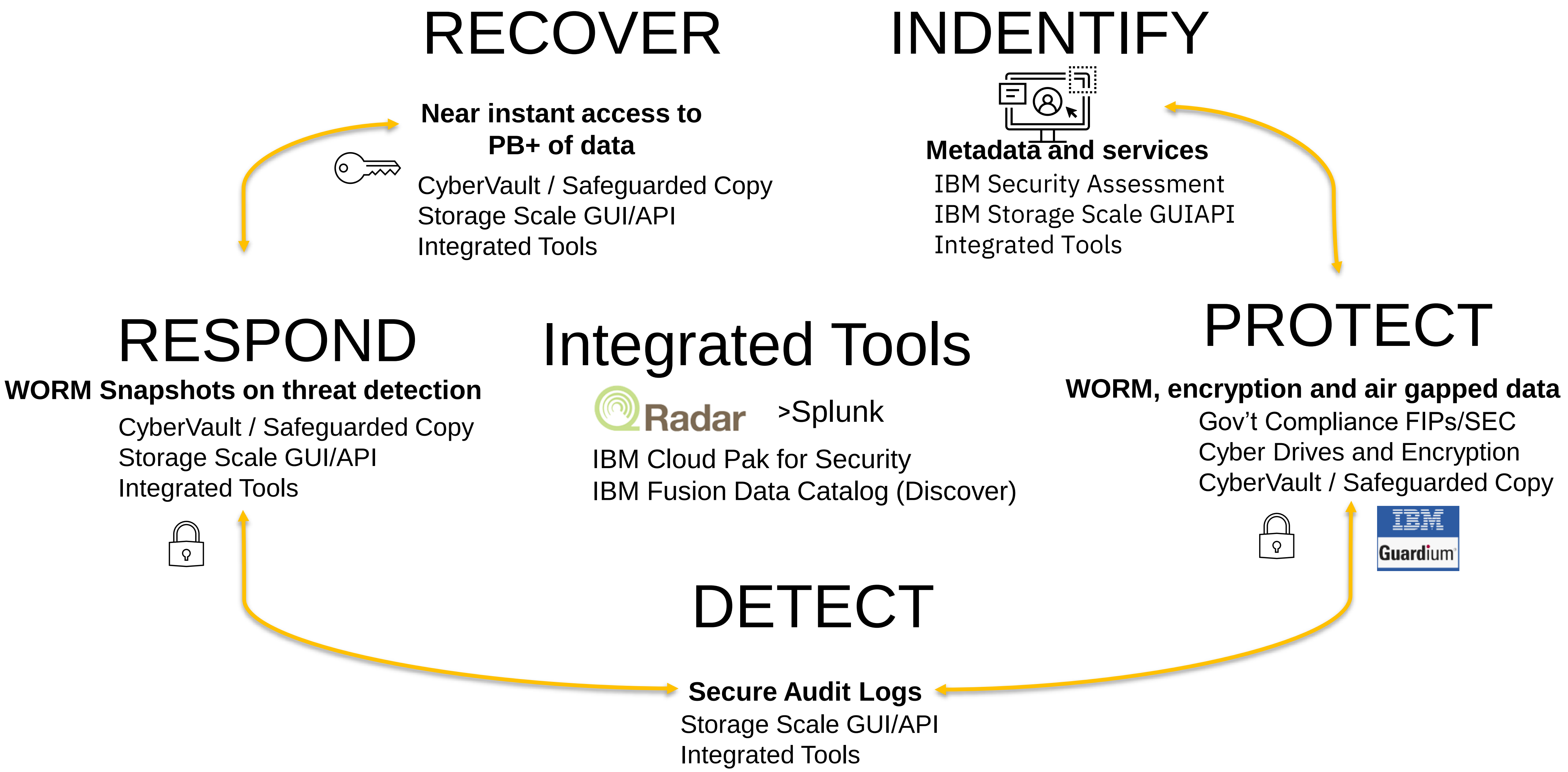
Integrations to AI enhanced IBM Qradar, Splunk, Guardium, Cloud Pak for Security and other ecosystem partners

Attack Response

With near-instant recovery and one-click response of Safeguarded Copy and as a service option with IBM CyberVault

Security Services Ensure Assets are Safe

Following the NIST Standard



RECOVER

Near instant access to PB+ of data

CyberVault / Safeguarded Copy
Storage Scale GUI/API
Integrated Tools

INDENTIFY

Metadata and services

IBM Security Assessment
IBM Storage Scale GUIAPI
Integrated Tools

RESPOND

WORM Snapshots on threat detection

CyberVault / Safeguarded Copy
Storage Scale GUI/API
Integrated Tools

Integrated Tools

Radar >Splunk

IBM Cloud Pak for Security
IBM Fusion Data Catalog (Discover)

PROTECT

WORM, encryption and air gapped data

Gov't Compliance FIPs/SEC
Cyber Drives and Encryption
CyberVault / Safeguarded Copy

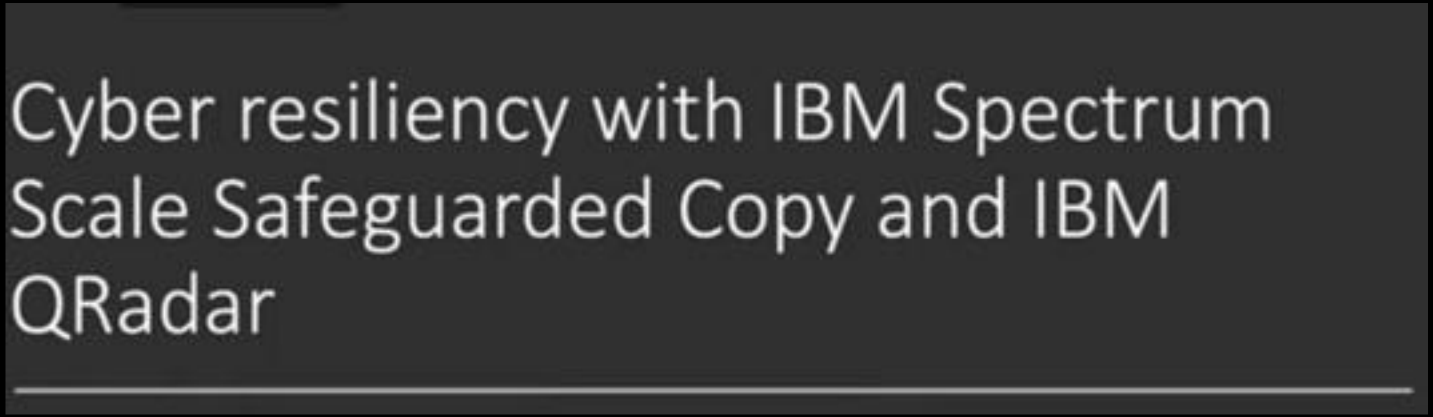
IBM Guardium

DETECT

Secure Audit Logs

Storage Scale GUI/API
Integrated Tools

Storage Scale and SIEM



Cyber resiliency with IBM Spectrum Scale Safeguarded Copy and IBM QRadar

https://mediacenter.ibm.com/media/IBM+Cyber+Resilency+using+Safeguarded+Copy+on+Storage+Scale+and+QRadar+/1_eel4kqpx

Demonstration

Bolstering Cyber Resilience with Threat Detection

IBM Spectrum Scale with IBM QRadar

IBM.

https://youtu.be/FGVsYycsk1Q

Basic Demonstration

Proactive Threat Detection

IBM Spectrum Scale with Splunk Enterprise

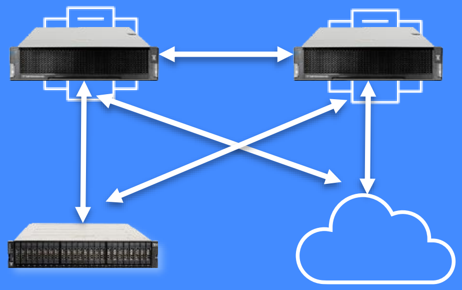
https://youtu.be/FGVsYycsk1Q

Security Services Prepare for the Worst

From Failure, to Protection, to Theft to Attack

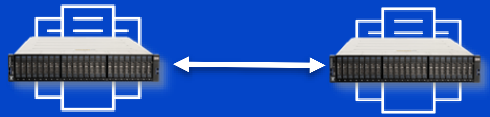
Failure Protection

Enhanced High-availability



Multi-Platform Support

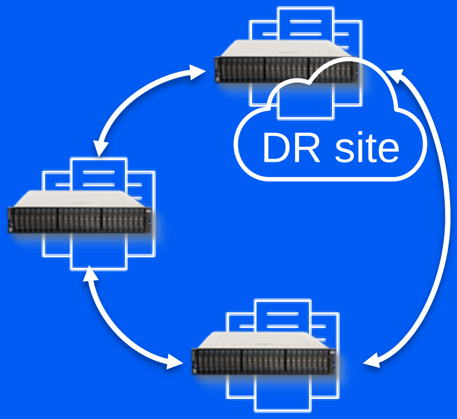
High Availability



Same data is on both sides

Disaster Protection

Enterprise Disaster Recovery

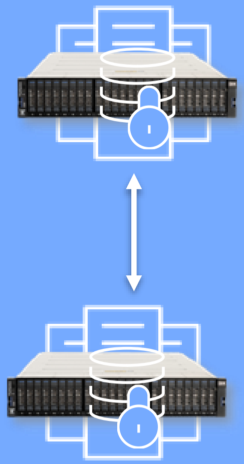


On-prem, on cloud or hybrid

Data Theft

Encryption

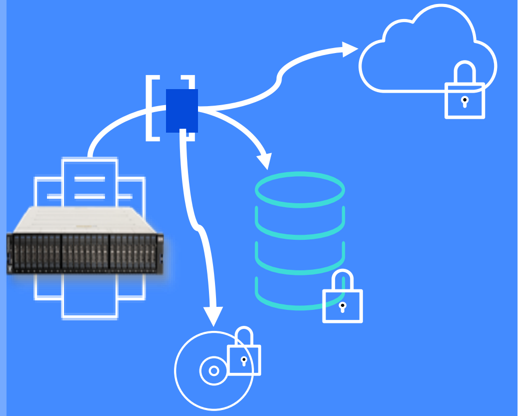
FIPS 140-3



End to end user keys

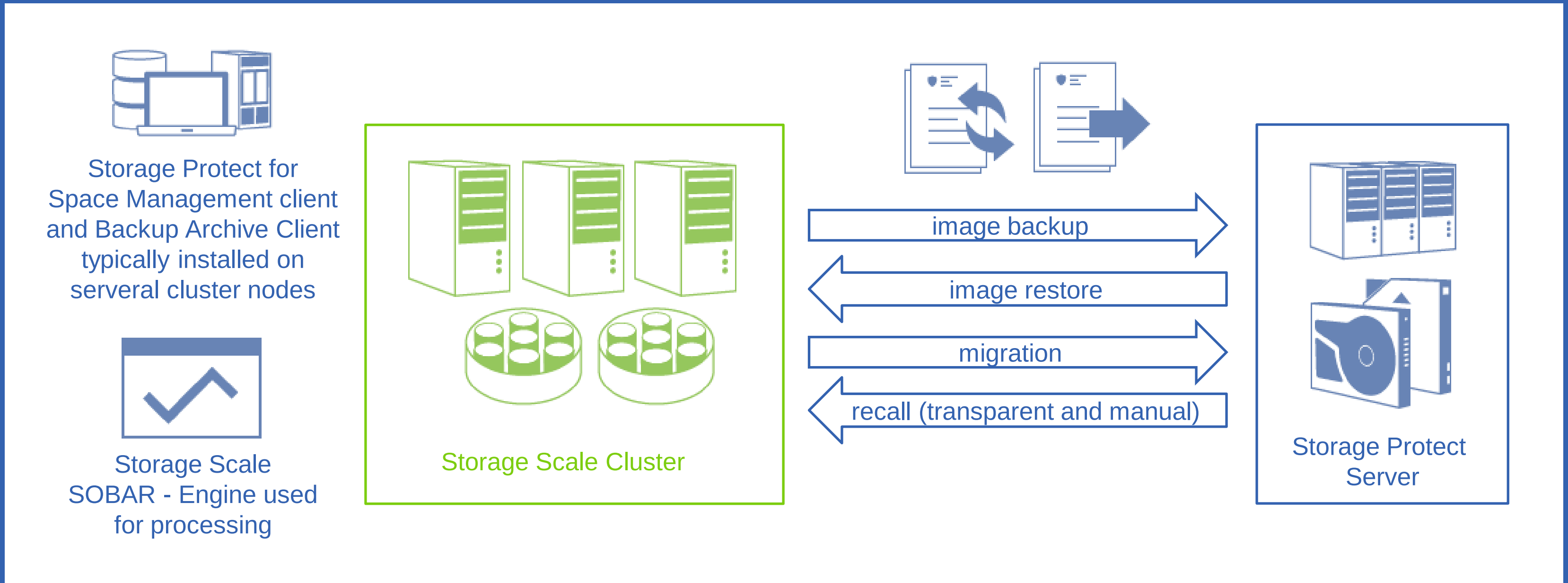
Cyber Attack

Immutable copies



Air Gap

Fast Disaster Recovery

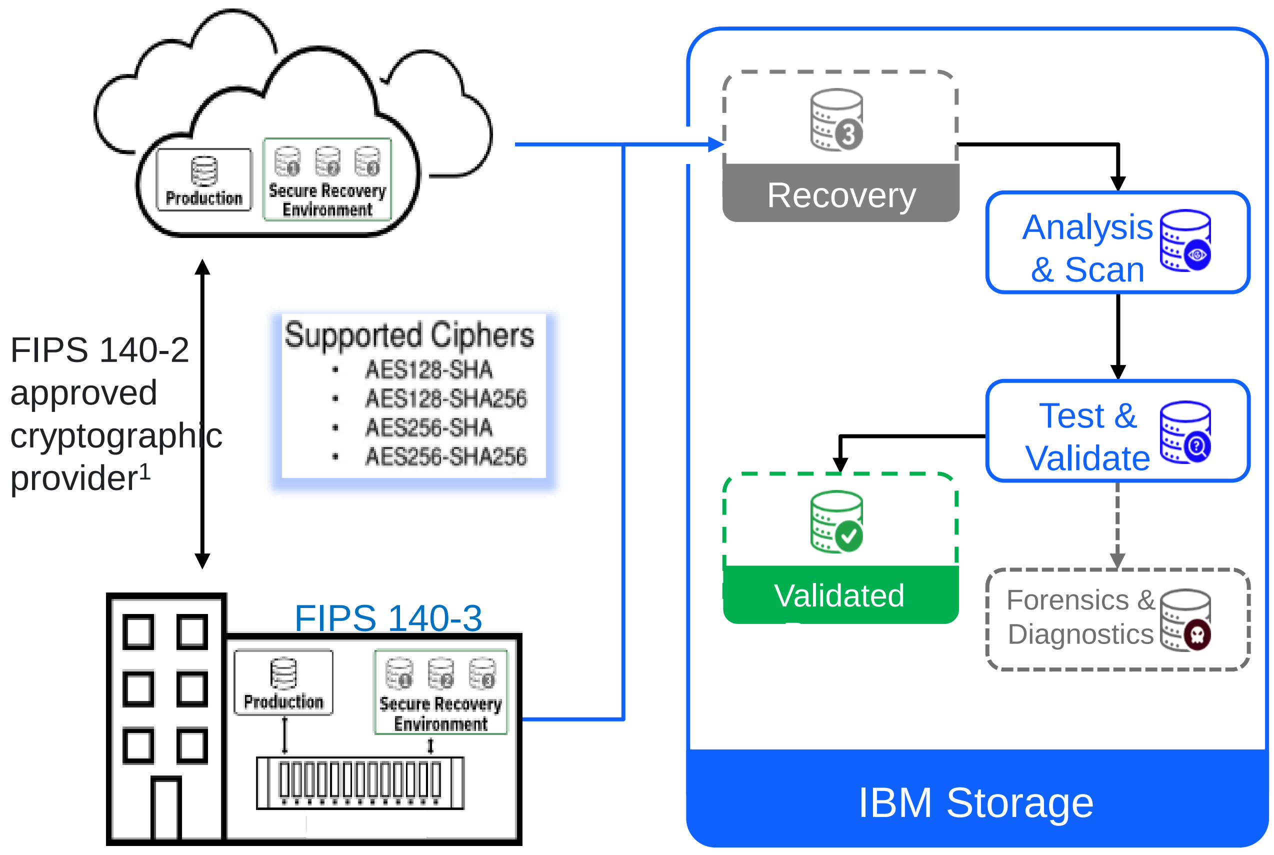

Storage Protect for Space Management client and Backup Archive Client typically installed on serveral cluster nodes
Storage Scale SOBAR - Engine used for processing
Storage Scale Cluster
image backup
image restore
migration
recall (transparent and manual)
Storage Protect Server

SOBAR – Engine creates and backs up file system metadata image from snapshot

Ultra fast backup and recovery due to massive parallel metadata processing

RTO counted in hours … not weeks

Security Services Enable Cyber Security



Logical Air Gapping
IBM Safeguarded
Copy

Secure Operational Air
Gapping

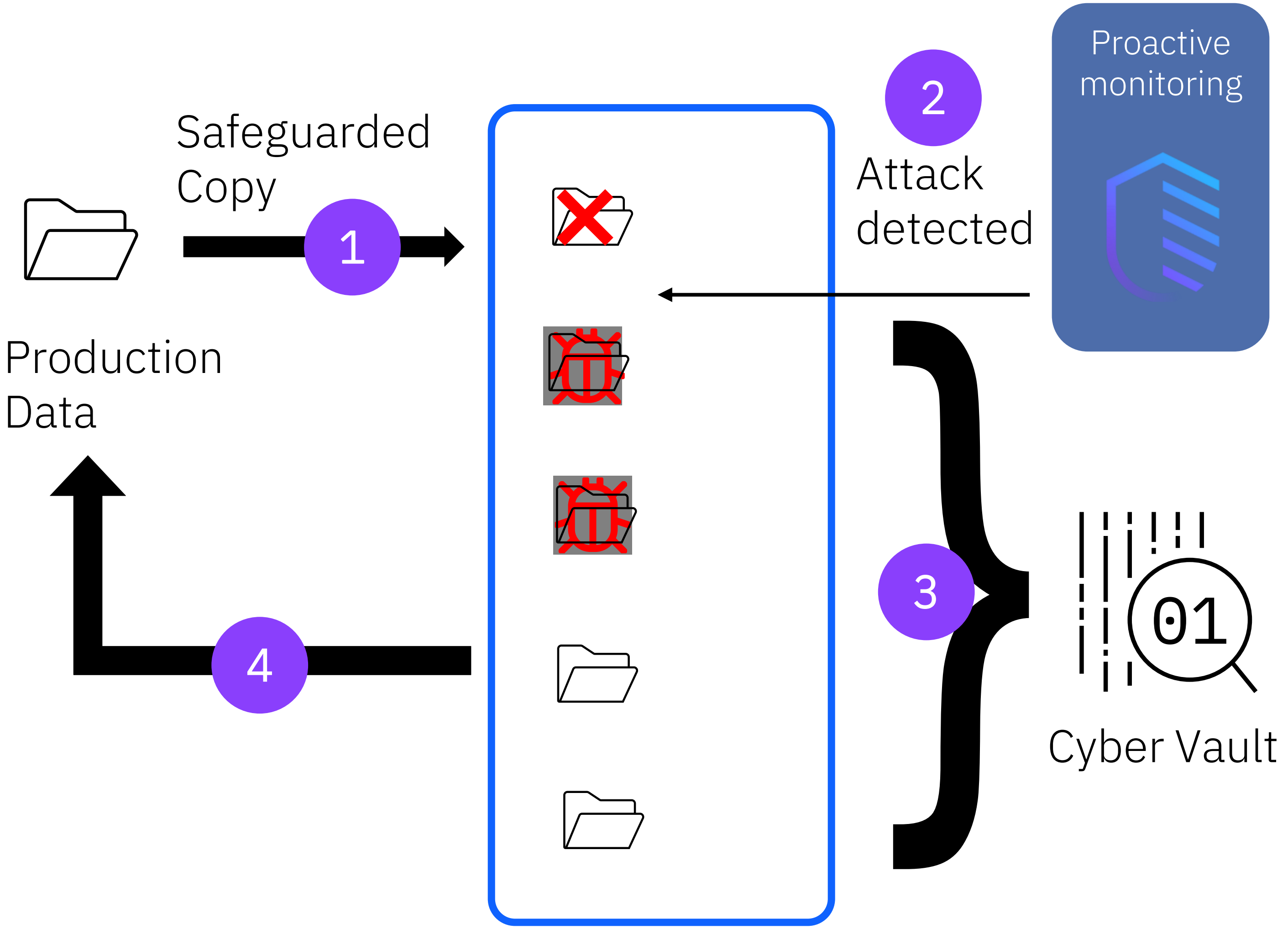
Safeguarded Copy

- Space efficient snapshots (scheduled, manual, triggered) stored in an immutable secure recovery location
- Simple GUI Interface with single screen policies
- Logical air gapping solutions with security controls using separation of duties for checks and balances

Benefits

- Reduce recovery from days and/or hours to minutes
- Backups cannot be accessed or modified by unauthorized applications/staff
- Up to 256 recovery points per fileset
- Integrates with Security Information and Event Management (SIEM) tools for response automation

Security Services Speeds Recovery with Cyber Vault



Safeguarded Copy

1

Production Data

2

Attack detected

Proactive monitoring

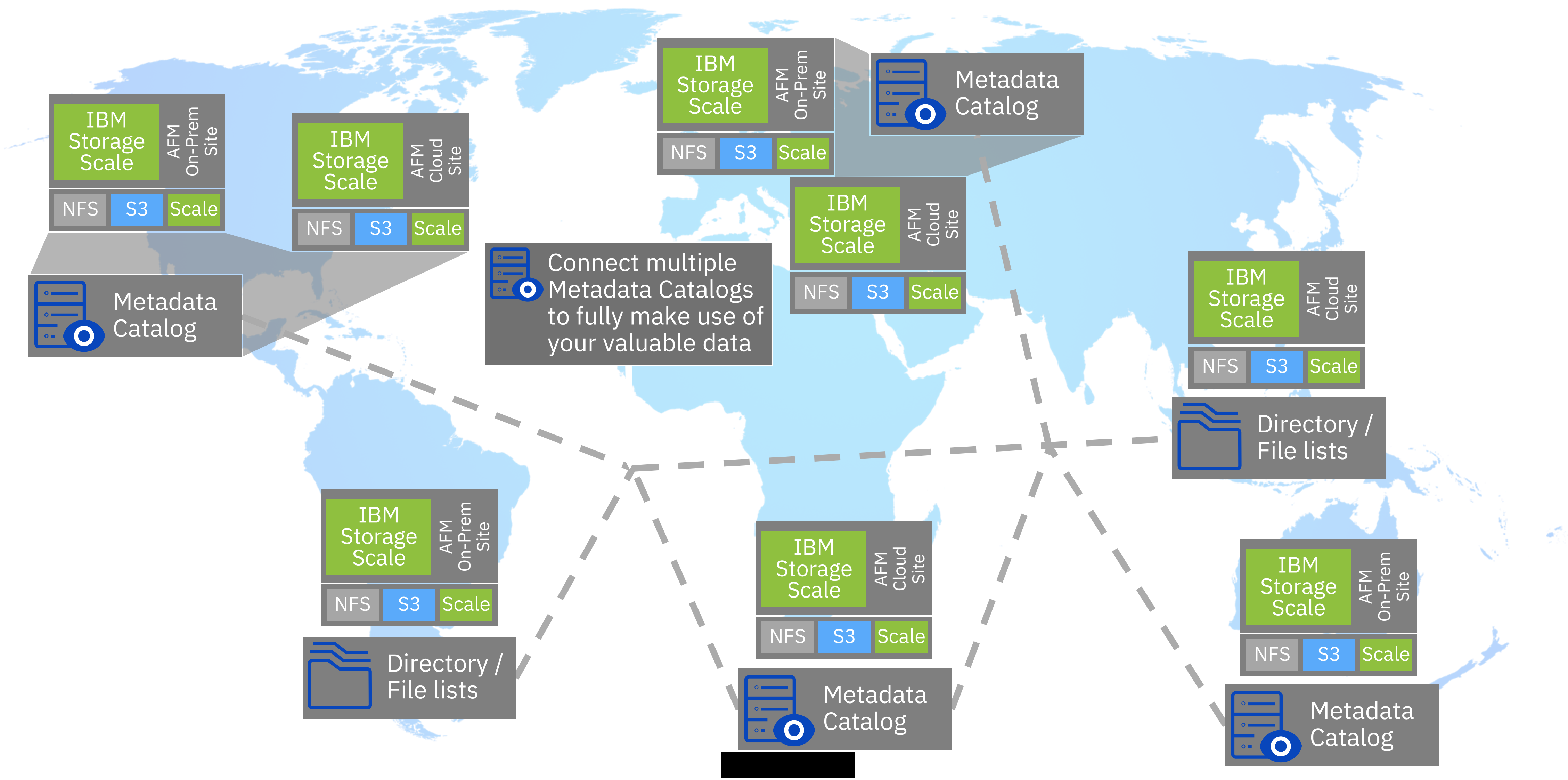
3

Cyber Vault

4

Resurgence of privacy regulations

Enterprises struggle with complex regulatory requirements and the demand for data security



IBM Storage Scale | AFM On-Prem Site | NFS | S3 | Scale

Metadata Catalog

IBM Storage Scale | AFM Cloud Site | NFS | S3 | Scale

IBM Storage Scale | AFM On-Prem Site | NFS | S3 | Scale

Metadata Catalog

IBM Storage Scale | AFM Cloud Site | NFS | S3 | Scale

Connect multiple Metadata Catalogs to fully make use of your valuable data

IBM Storage Scale | AFM Cloud Site | NFS | S3 | Scale

Directory / File lists

IBM Storage Scale | AFM On-Prem Site | NFS | S3 | Scale

Directory / File lists

IBM Storage Scale | AFM Cloud Site | NFS | S3 | Scale

Metadata Catalog

IBM Storage Scale | AFM On-Prem Site | NFS | S3 | Scale

Metadata Catalog

[redacted]

Data intensive workloads with security services: Client success

A large healthcare organization doing research, realized they had many security vulnerabilities with critical data that needed to be addressed with their current environment.

Business Challenge

Client scheduled a CRAT or cyber resilience assessment. After the assessment, the customer created a redundant environment that was used to offload main production site accommodating for growth and provide a multi-site DR with cyber secure data using Safeguarded Copy.

Results

Quick Recovery

Safeguarded Copy created an environment where quick recovery was now possible

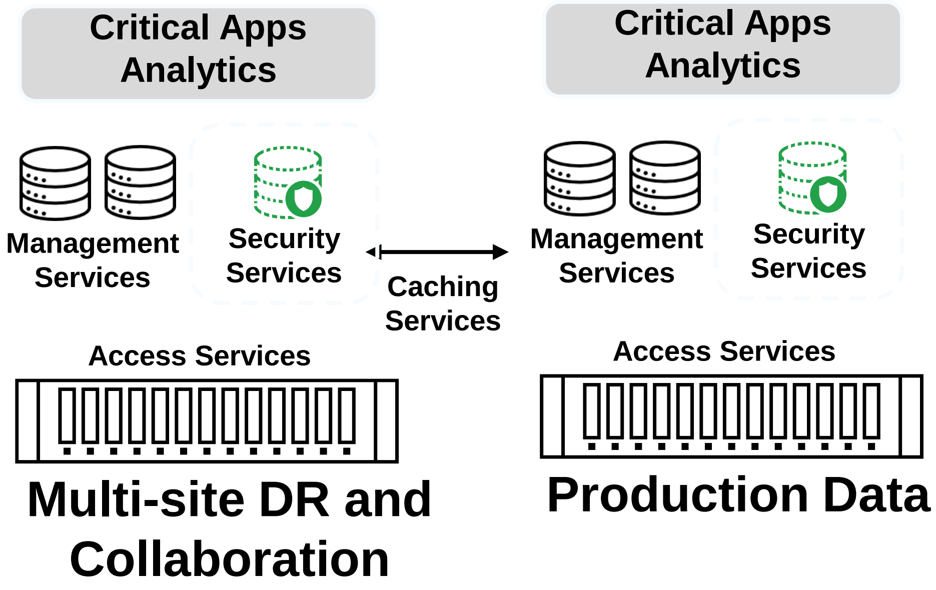
60PB+

Total Amount of Accessible data

Assessment

Customer did not know what they did not know, and IBM helped

IBM Solution



Expert Labs - Securing IBM Storage Scale with Cyber Vault

Tom Zito & Don Mathisen

Cyber Vault framework: significantly reduce the impact of breaches

1) IBM STORAGE WITH INTEGRATED COPY MANAGEMENT

- IBM Storage Scale
- IBM Storage Scale System
- IBM Storage Virtualize
- IBM Storage FlashSystem

Cyber Vault framework: significantly reduce the impact of breaches

1) IBM STORAGE WITH INTEGRATED COPY MANAGEMENT

- IBM Storage Scale
- IBM Storage Scale System
- IBM Storage Virtualize
- IBM Storage FlashSystem

2) SAFEGUARDED COPIES

Protected point in time (PIT) copies: Immutable and Isolated with stringent Role Based Access Control (RBAC)

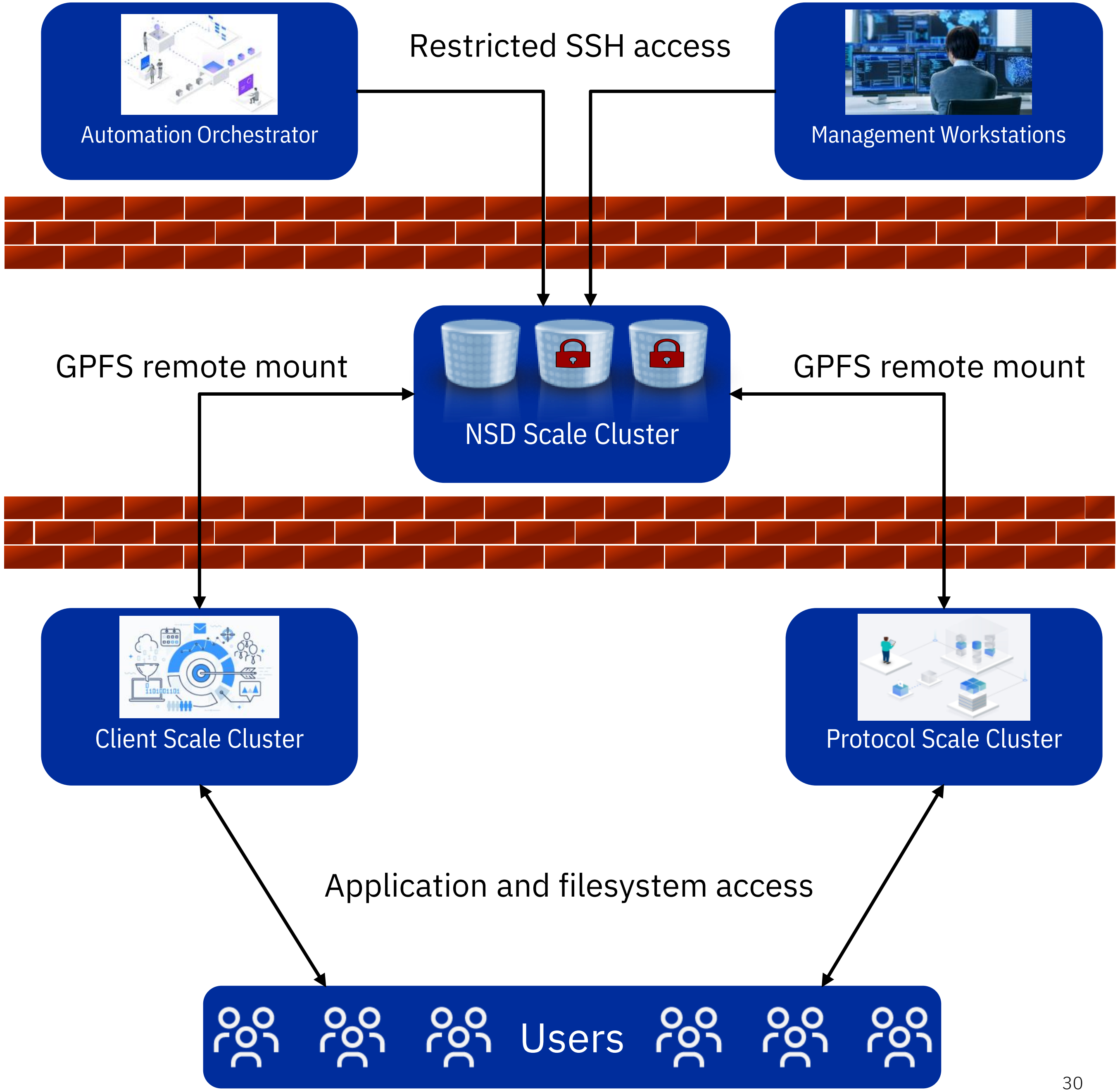
Safeguarded Copies on Scale

Core Requirements

- IBM Storage Scale version 5.1.5.0 (Sep 02, 2022) or
  IBM Storage Scale System version 6.1.5.0 (Dec 12, 2022).
- SUDO wrappers configured and tested for the cluster(s) per Best Practice guidelines.
- Limited number of root or security admin accounts, reserved for specific tasks, not everyday use.
- Disable direct logins as the root user on all Scale nodes. (Optional, but recommended)
- Create a Safeguarded snapshot schedule with the desired retention.

Enhanced security via client and protocol clusters connected via remote mount

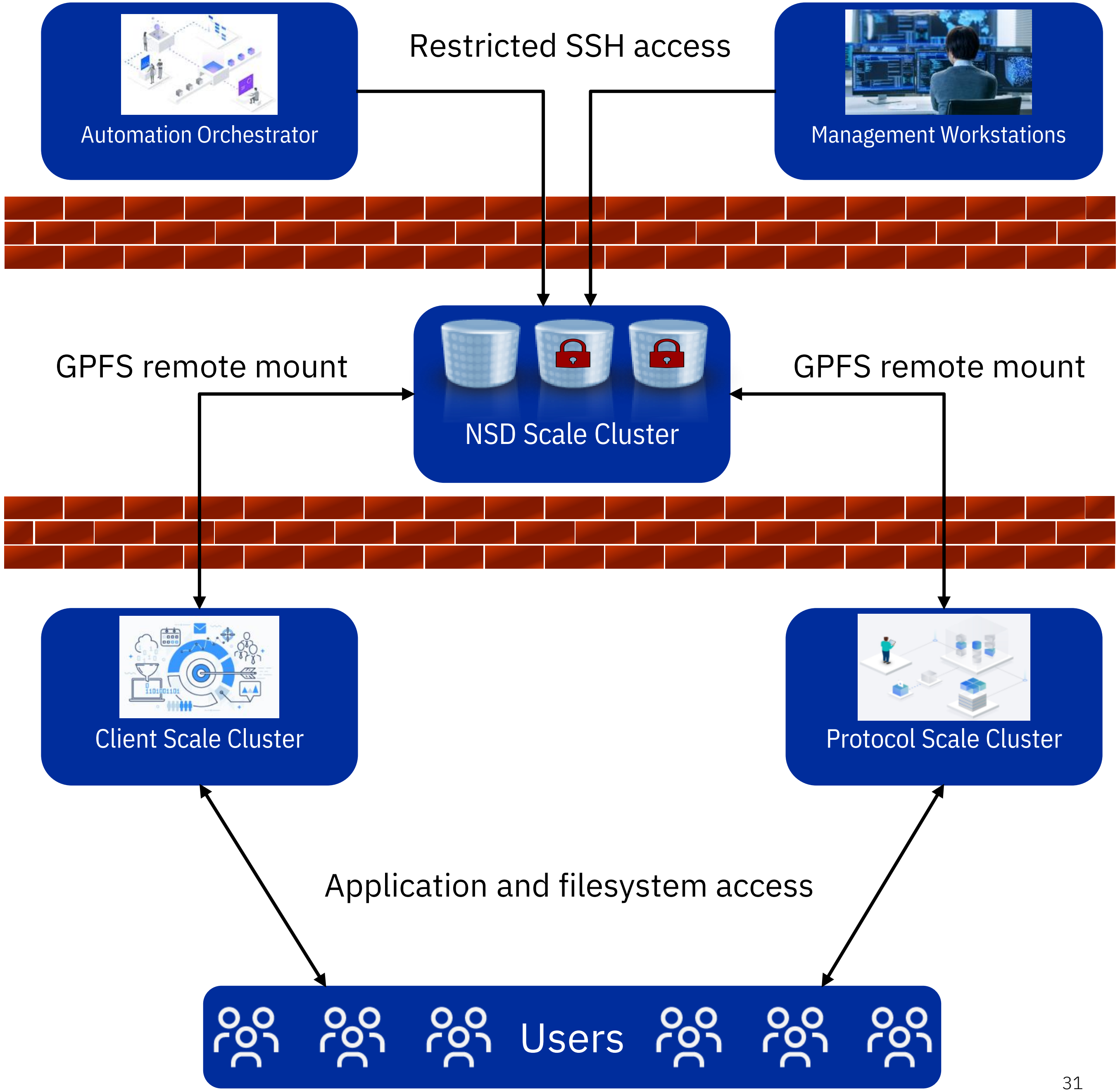
- NSD cluster only contains NSD nodes and has use restricted to only providing the GPFS filesystem.
- Cyber Vault core requirements properly implemented on NSD cluster.
- The root and security admin account passwords on the NSD cluster are unique for only that cluster.
- The NSD cluster is firewalled such that client and protocol cluster may only communicate with the GPFS protocol for remote mount.
  - Don’t forget - also Remote Fileset Access Control (RFAC)!
- NSD cluster remote access is limited to only management or automation and only from a limited number of specific IP addresses.
- No SSH keys between clusters, only within cluster.



Security Incident

Malicious User Activity

- Cyber Vault core requirements properly implemented on NSD cluster:
  - Create a Safeguarded snapshot schedule with desired retention.



Security Incident

Brute Force Attack

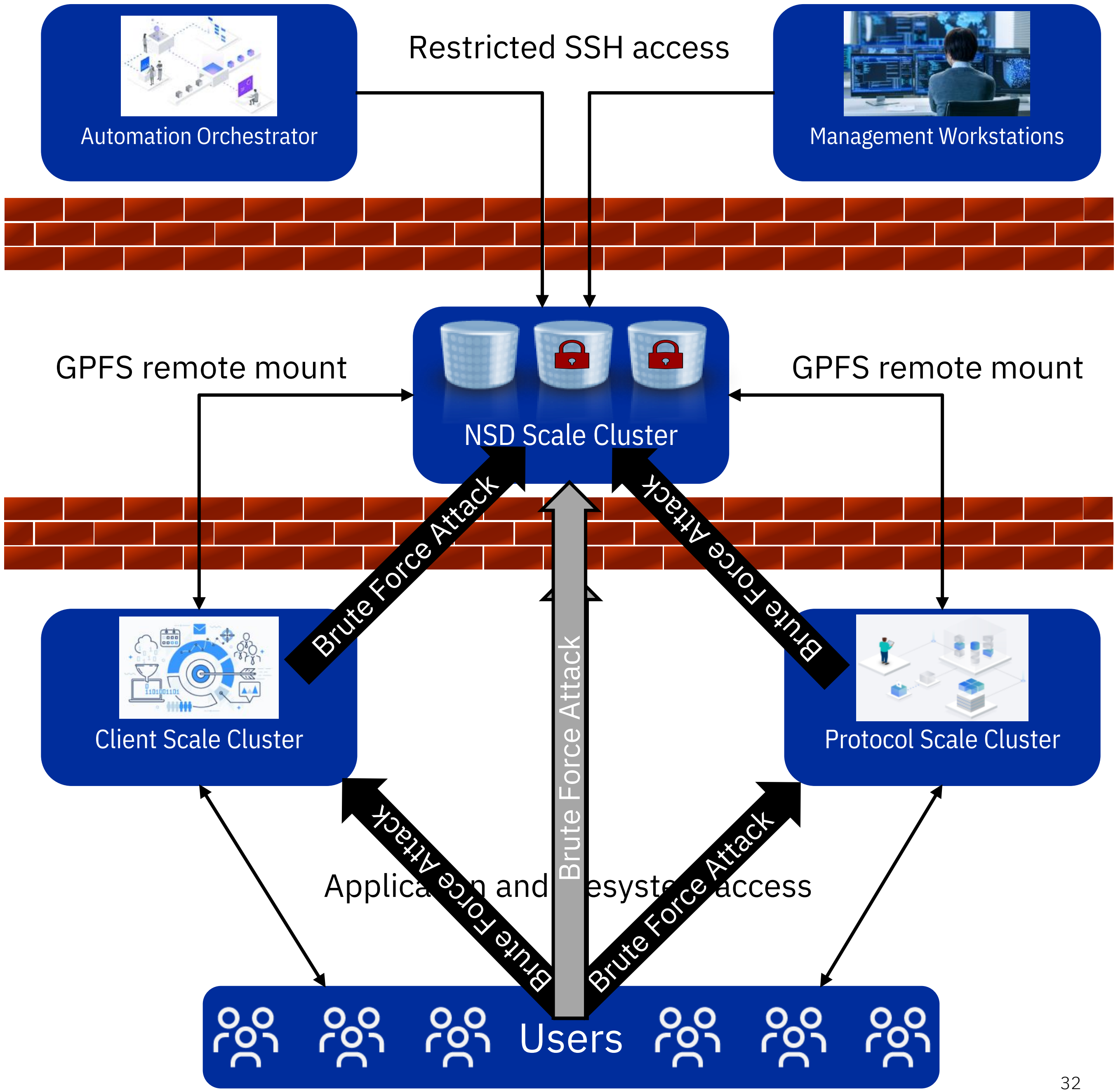
- Cyber Vault core requirements properly implemented on NSD cluster:
  - Disable direct logins as the root user on all Scale nodes.

- The NSD cluster is firewalled such that client and protocol cluster may only communicate with the GPFS protocol for remote mount.

- The root and security admin account passwords on the NSD cluster are unique for only that cluster.

- NO SSH keys between clusters, only within cluster.

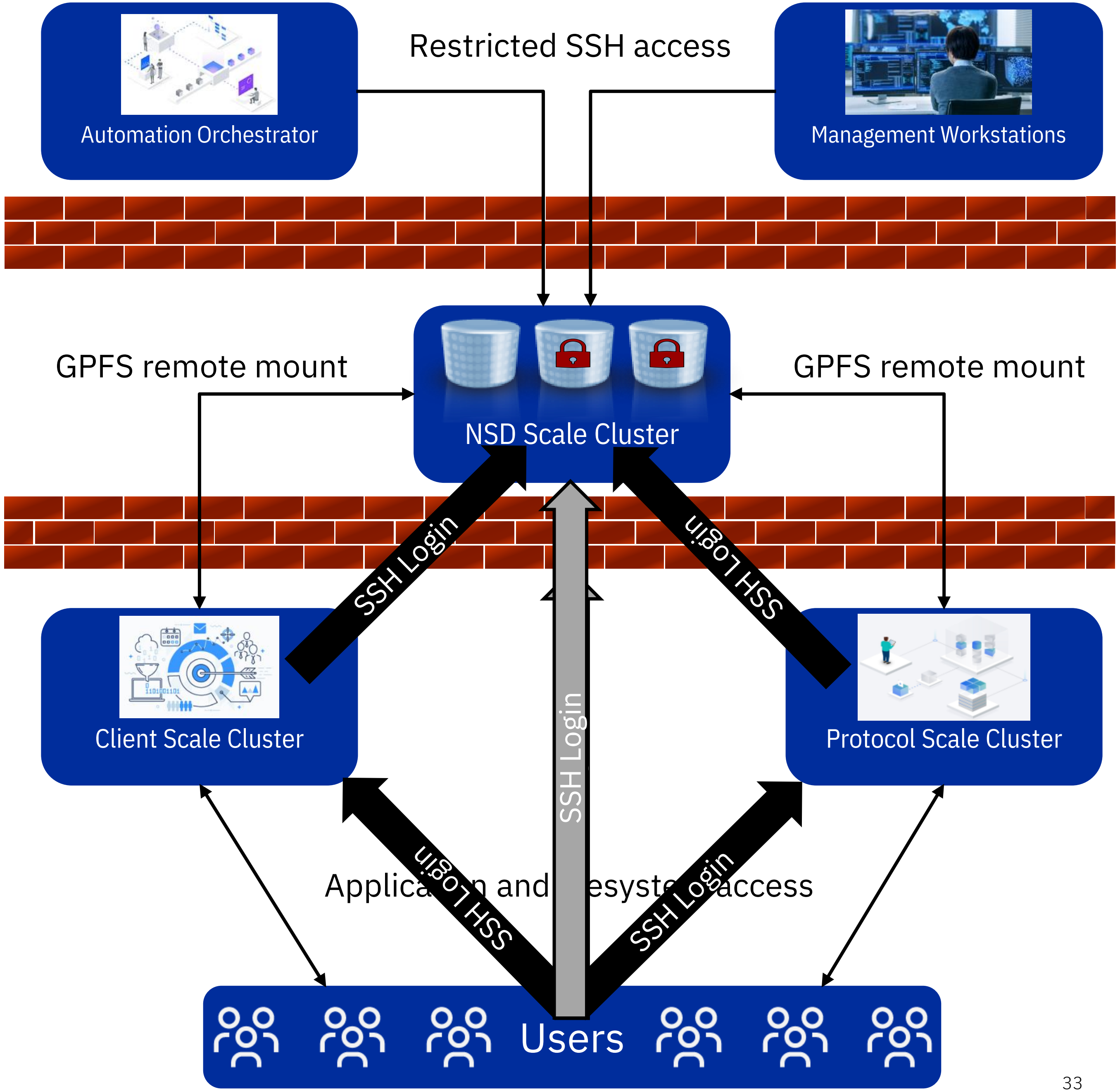
- NSD cluster remote access is limited to only management or automation and only from a limited number of specific IP addresses.



Security Incident

Root Password Compromise

- Cyber Vault core requirements properly implemented on NSD cluster:
  - SUDO wrappers configured and tested for the cluster(s) per Best Practice guidelines.
  - Limited number of root or security admin accounts, reserved for specific tasks, not everyday use.
  - Disable direct logins as the root user on all Scale nodes.
- The NSD cluster is firewalled such that client and protocol cluster may only communicate with the GPFS protocol for remote mount.
- The root and security admin account passwords on the NSD cluster are unique for only that cluster.
- NO SSH keys between clusters, only within cluster.
- NSD cluster remote access is limited to only management or automation and only from a limited number of specific IP addresses.



Security Incident

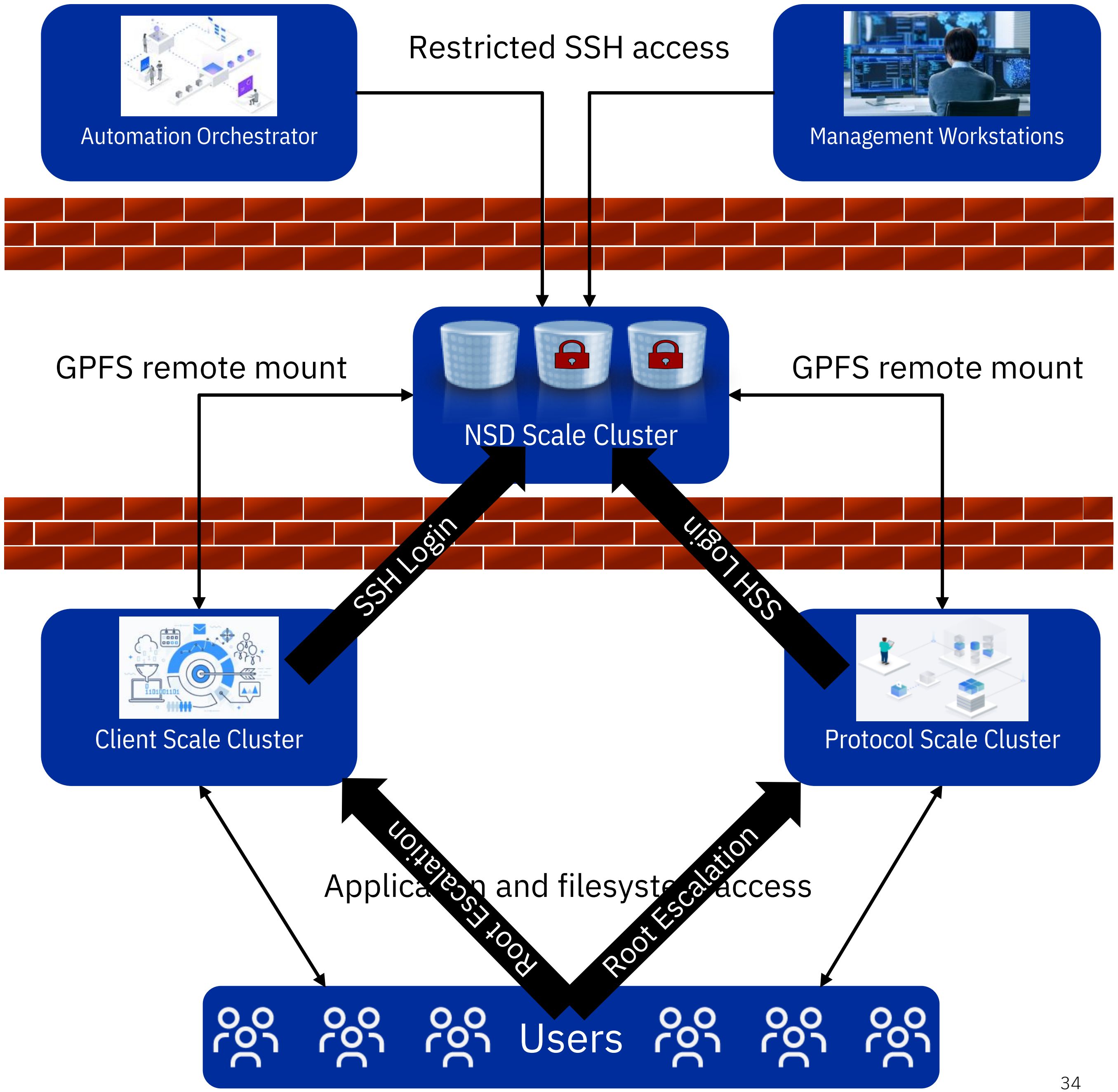
Root Privilege Escalation

- Cyber Vault core requirements properly implemented on NSD cluster:
  - Limited number of root or security admin accounts, reserved for specific tasks, not everyday use.
  - Disable direct logins as the root user on all Scale nodes.

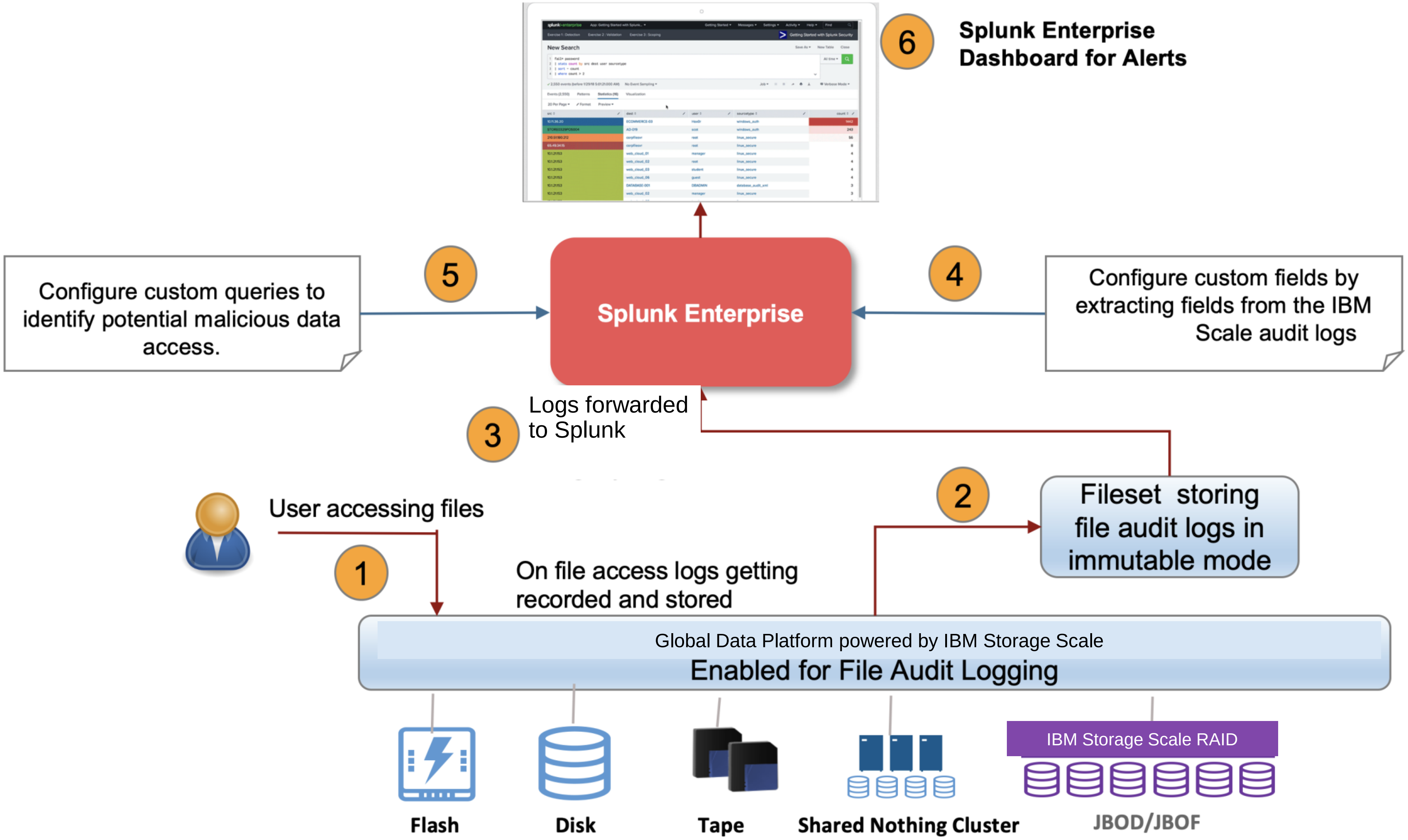
- The NSD cluster is firewalled such that client and protocol cluster may only communicate with the GPFS protocol for remote mount.

- NSD cluster remote access is limited to only management or automation and only from a limited number of specific IP addresses.

- NO SSH keys between clusters, only within cluster.



IBM Storage Scale and SPLUNK : Integration Flow



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 Scale audit logs

3 Logs forwarded to Splunk

User accessing files

1 On file access logs getting recorded and stored

2 Fileset storing file audit logs in immutable mode

Global Data Platform powered by IBM Storage Scale

Enabled for File Audit Logging

Flash

Disk

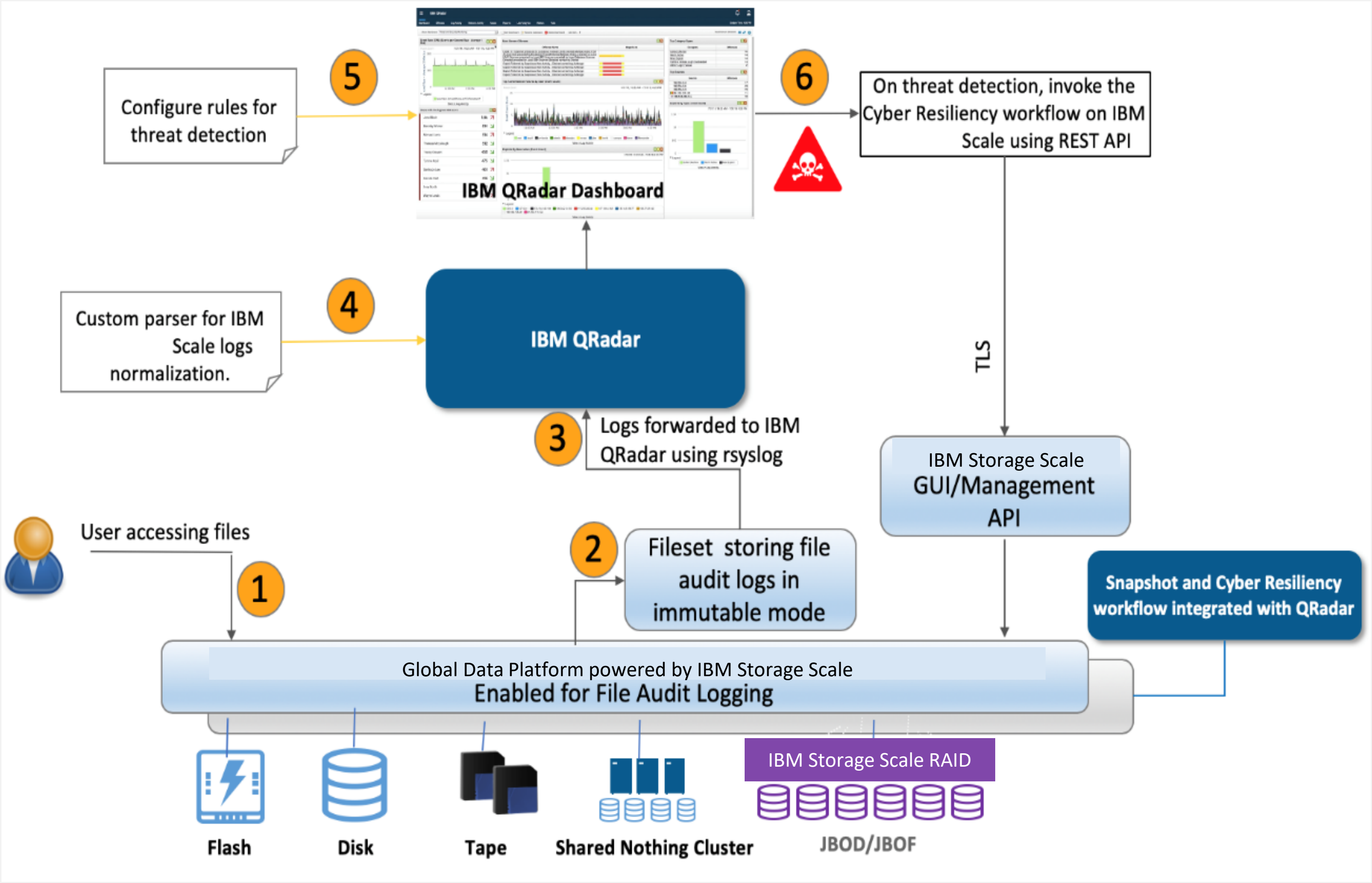
Tape

Shared Nothing Cluster

IBM Storage Scale RAID

JBOD/JBOF

Safeguarded Copy Snapshot with Storage Scale



5 Configure rules for threat detection

IBM QRadar Dashboard

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

4 Custom parser for IBM Scale logs normalization.

IBM QRadar

TLS

3 Logs forwarded to IBM QRadar using rsyslog

IBM Storage 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

Global Data Platform powered by IBM Storage Scale
Enabled for File Audit Logging

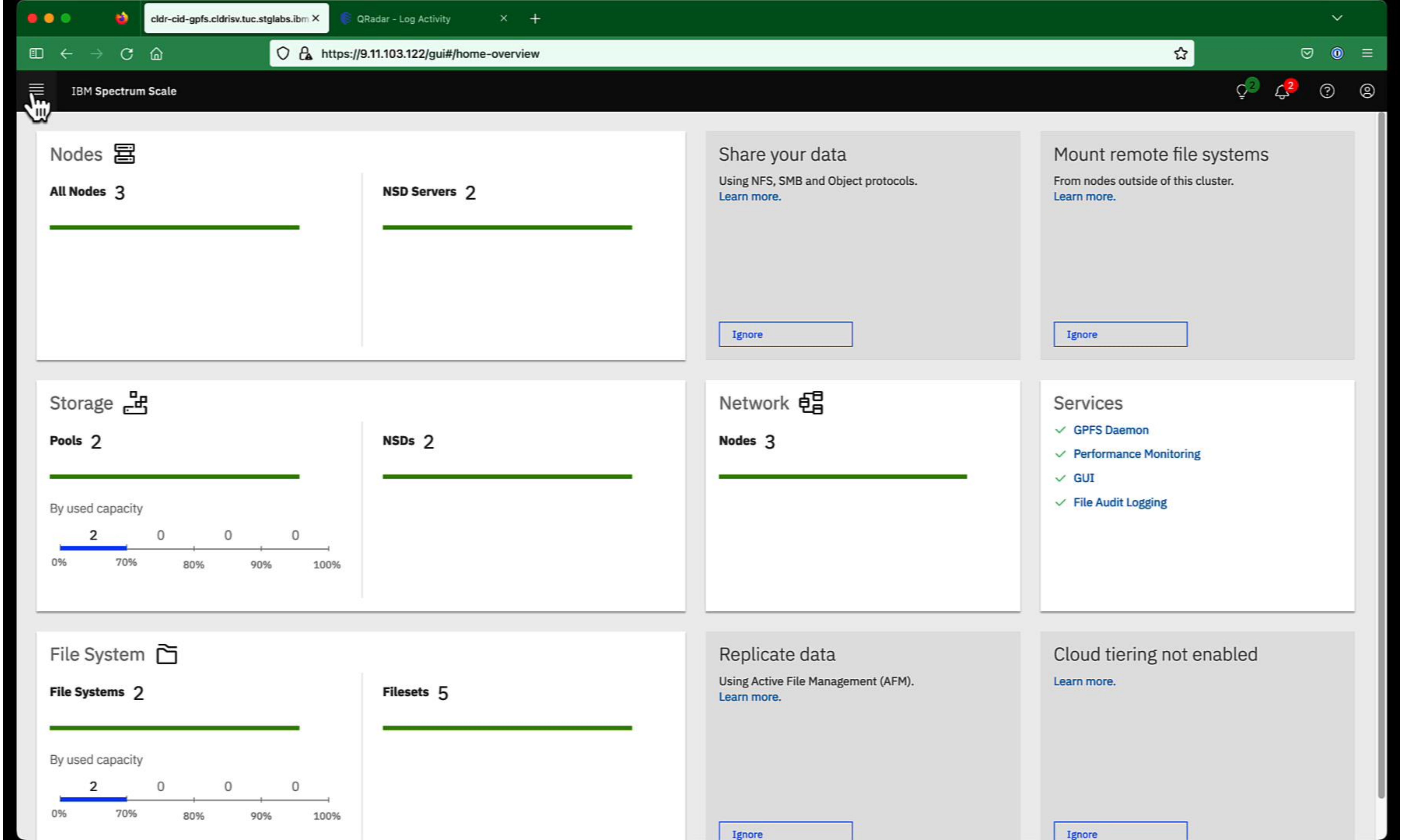
IBM Storage Scale RAID

Scenario

- User modifying confidential data outside business hours

Mitigation

- Enable filesystem audit
- Send audit events to IBM QRadar
- Define rules, actions in IBM QRadar
- Use Storage Scale Safeguarded copy feature to create immutable snapshot


cldr-cid-gpfs.cldrisv.tuc.stglabs.ibm
QRadar - Log Activity
https://9.11.103.122/gui#/home-overview
IBM Spectrum Scale
2
2

Nodes

All Nodes 3

NSD Servers 2

Share your data

Using NFS, SMB and Object protocols.
Learn more.

Mount remote file systems

From nodes outside of this cluster.
Learn more.

Storage

Pools 2

By used capacity

NSDs 2

Network

Nodes 3

Services

- ✓ GPFS Daemon
- ✓ Performance Monitoring
- ✓ GUI
- ✓ File Audit Logging

File System

File Systems 2

By used capacity

Filesets 5

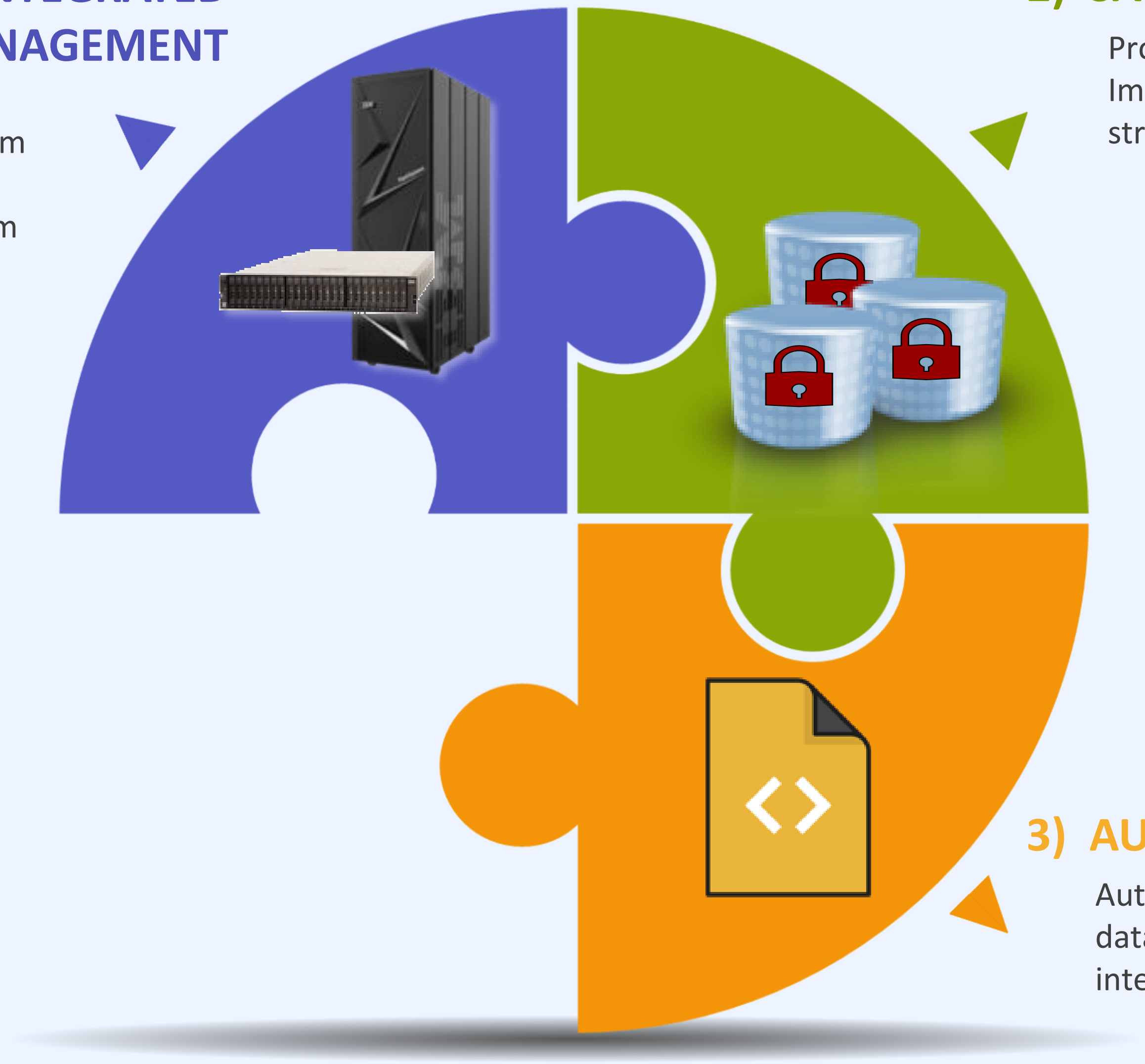
Replicate data

Using Active File Management (AFM).
Learn more.

Cloud tiering not enabled

Learn more.

Cyber Vault framework: significantly reduce the impact of breaches



1) IBM STORAGE WITH INTEGRATED COPY MANAGEMENT

- IBM Storage Scale
- IBM Storage Scale System
- IBM Storage Virtualize
- IBM Storage FlashSystem

2) SAFEGUARDED COPIES

Protected PIT copies:
Immutable and Isolated with stringent RBAC's

3) AUTOMATION

Automated data validation, data recovery and application integration

Automation Processes

Quiesce

Application integration to provide application-consistent recovery points.

- Could be specific to the application(s)
  - **mmcrsnapshot/REST/GUI** call does this
- Requests the application flush memory to disk and hold further file updates until released.
- May impact running operations, testing is needed to determine.
- Not always needed, crash-consistent is acceptable for many applications.
- Databases may have a hot-backup capability to minimize affect.
  - Flushes records out the DB files.
  - Plays all updates into DB files after resume.
  - Stops writing to DB files and writes to log journal during quiesce.
  - DB files and logs should be in different volume groups, and protected separately, to allow log journal to update during DB file quiesce.

Automation Processes

Validate

Scan the Safeguarded copy integrity prior to restoring data.

- Can be performed at one, or several, stages to provide integrity check:
  - After the Safeguarded copy is performed.
    - Provides good/bad state prior to recovery.
    - Requires a data location to hold the statuses.
  - During the restore process, prior to restoring.
    - Slows the recovery while data is scanned.
    - All scans are based on most recent patterns.
  - At a regular interval and as detection parameters evolve.
    - Confirms integrity against most recent patterns
    - Requires more processing to rescan as patterns change.

- Example tools and methodologies:
  - Server/VM and application startup check
  - Structure checking like IBM Sentinel uses in the Scanning Engine.
  - Pattern matching like conventional antivirus and malware detectors.
  - Custom report validation based on inside knowledge.
  - Verification of Honeypot / Canary records remaining unchanged.
  - Monitoring of file access patterns.

Automation Processes

Recover/Restore

Start and Stop applications and revert the data set to the Safeguarded Copy point-in-time.

- Surgical recovery methodology.
  - A copy of the data from the Safeguarded Copy point-in-time is presented to a server/VM out-of-band in a recovery / clean-room environment.
  - Data to be recovered is manually moved between recovered system and protected system to merge older data from the point-in-time back into the protected environment.

- Full time-warp of data back to Safeguarded Copy point-in-time.
  - The volumes revert to the data state they were in when the Safeguarded copy was taken.
  - No need to manually move data to the protected server.
  - All data modified since the Safeguarded Copy point-in-time is lost unless manually extracted prior to restoring.

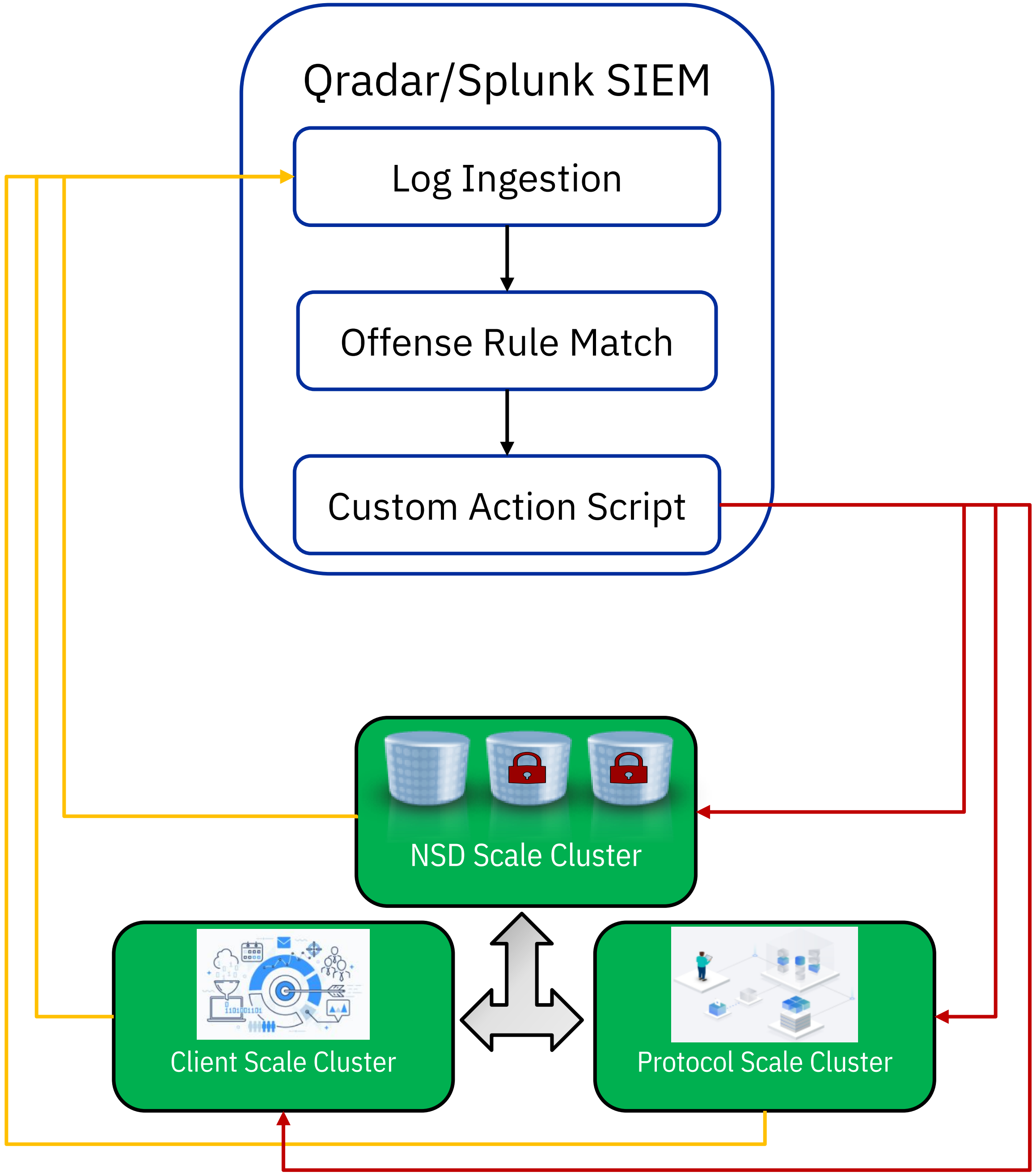
- Stopping the application beforehand is advised to clean the environment and provide better sanity.
- Starting the application would be required after the data is reverted.
- Needs to be configured / planned per application to verify procedure and prior dependencies are met.

Automation Methods

Qradar/Splunk SIEM

- No additional orchestrator or server/VM(s) needed.
- Fastest response to an event detection.

- Timeout limitation, seconds to process, not minutes.
- Lacks interactive decision making, always performs action when event is detected.
- Runs in a chrooted environment with limited scripting / programming language support.

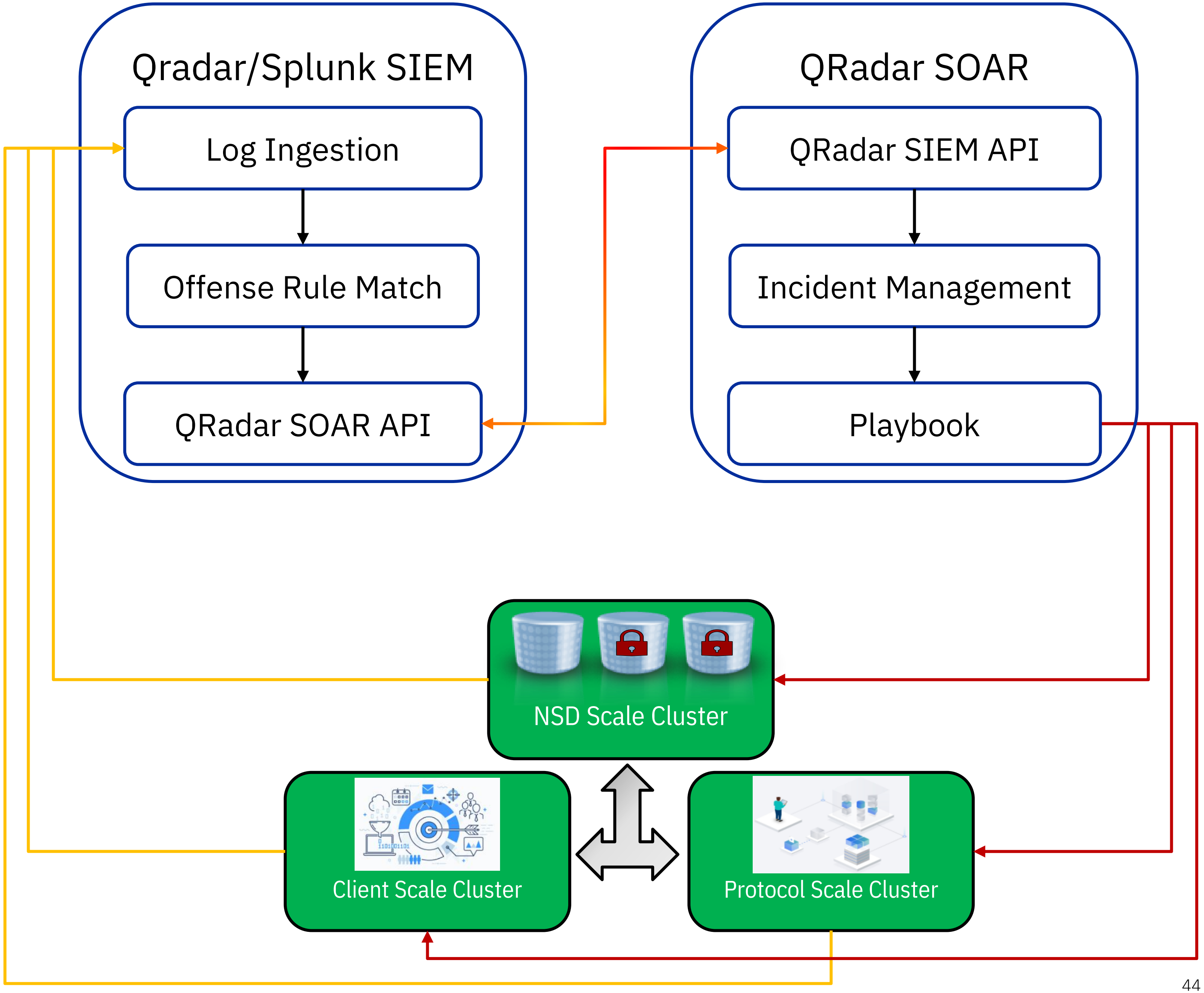


Automation Methods

QRadar SOAR

- Ticket management system to notify/involve appropriate people and track compliance.
- Able to orchestrate automated tasks without a detected event.
- Plugins to collect and correlate additional data sources.
- Wide variety of scripting / programming languages.

- Requires additional server(s)/VM(s).
- Licensing not part of the QRadar SIEM.
- Slightly slower response due to incident hand-off.

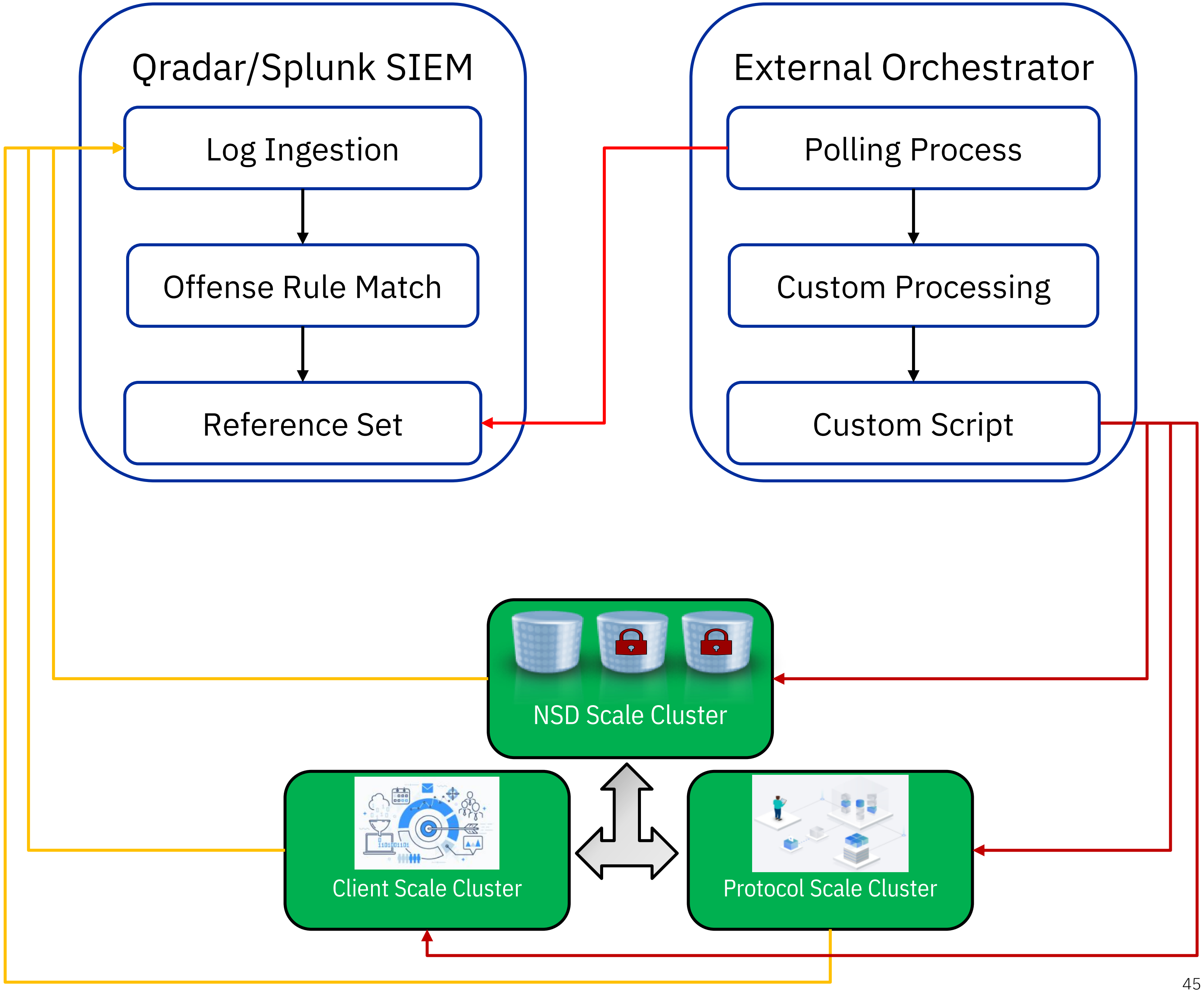


Automation Methods

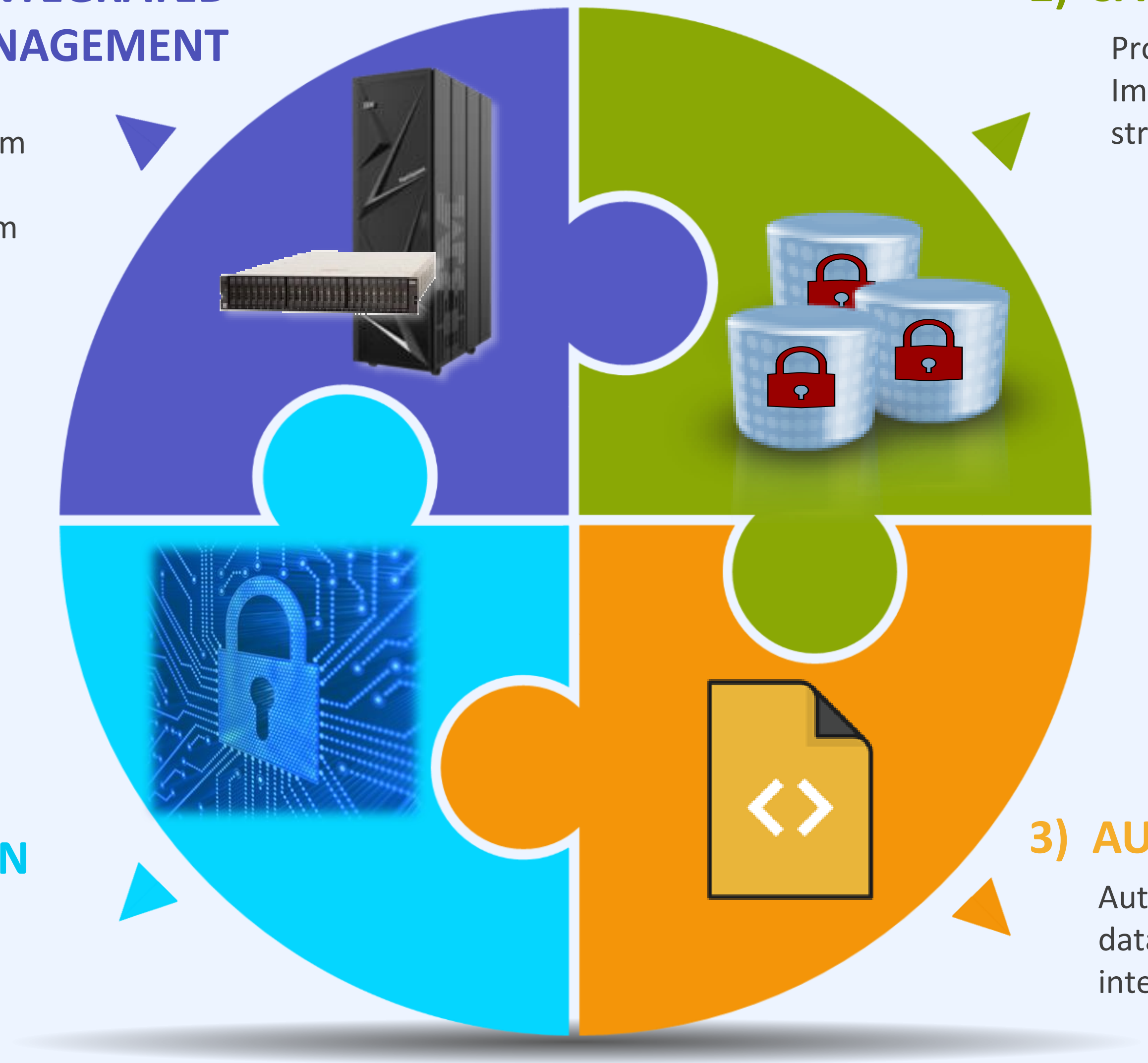
External Orchestrator

- Customized to specific needs and requirements.
- Able to provide orchestration of automated tasks without a detected event.
- Wide variety of scripting / programming languages.

- Requires custom coding to interface with APIs.
- Requires additional server(s)/VM(s).
- Polls the QRadar SIEM for events, not event driven.
- Potentially slower response to incident.



Cyber Vault framework: significantly reduce the impact of breaches



1) IBM STORAGE WITH INTEGRATED COPY MANAGEMENT

- IBM Storage Scale
- IBM Storage Scale System
- IBM Storage Virtualize
- IBM Storage FlashSystem

2) SAFEGUARDED COPIES

Protected PIT copies:
Immutable and Isolated with stringent RBAC's

3) AUTOMATION

Automated data validation, data recovery and application integration

4) SECURITY INTEGRATION

Detect and respond to threats real-time from a wide variety of data sources.

Security Tool Integrations

- Qradar/Splunk SIEM analyzing Scale node OS logs
  - Logins as root, should not happen in sudo environment
  - Privilege escalations
  - Multiple failed login attempts
  - User Behavior Analytics

- Qradar/Splunk SIEM analyzing GPFS audit logs
  - Ransomware access patterns
  - Windows ACL changes
  - Extended file attribute changes
  - Sudden deletes

- Guardium analyzing Database(s) on client clusters
  - Access of sensitive/critical data
  - Vulnerability assessments
  - Database change controls
  - Privileged actions

- AV / Integrity scan with reporting to QRadar on client/protocol cluster(s) or user endpoints.
  - Malware pattern detection
  - Changes to file extensions or structure

ADDITIONAL INFORMATION

- Safeguarded copy
  https://www.ibm.com/docs/en/Storage-scale/5.1.5?topic=administering-protecting-file-data-Storage-scale-safeguarded-copy
- sudo-wrapper set up and configuration
  https://community.ibm.com/community/user/storage/blogs/nils-haustein1/2020/12/17/Storage-scale-sudo-wrappers