Cyber resiliency

rubrik

PREVENT ATTACK
DETECT ATTACK
RECOVER

rubrik

BUT I HAVE BACKUPS, RIGHT?

rubrik

IMAGINE VISITING YOUR BACKUP SERVERS AND NOTICING THAT ALL THE BACKUP VOLUMES HAVE BEEN FORMATTED.

OH NO.

rubrik

THE KEY IS IMMUTABLE BACKUPS

Once data has been written it cannot be read, modified, or deleted by clients on your network.

No security exposure can tamper with the backups.

rubrik

TECHNICAL DEEP DIVE: RUBRIK'S IMMUTABLE ARCHITECTURE

rubrik

THREE PILLARS OF IMMUTABILITY

Distributed Immutable Filesystem

Provides tight controls over which applications can exchange information, how each data exchange is transacted, and how data is arranged across physical and logical devices.

Zero Trust Cluster Design

Never assume trust with any other member of the cluster or external entity. Require certificate-based mutual authentication for secure communications.

Authenticated APIs and Tools

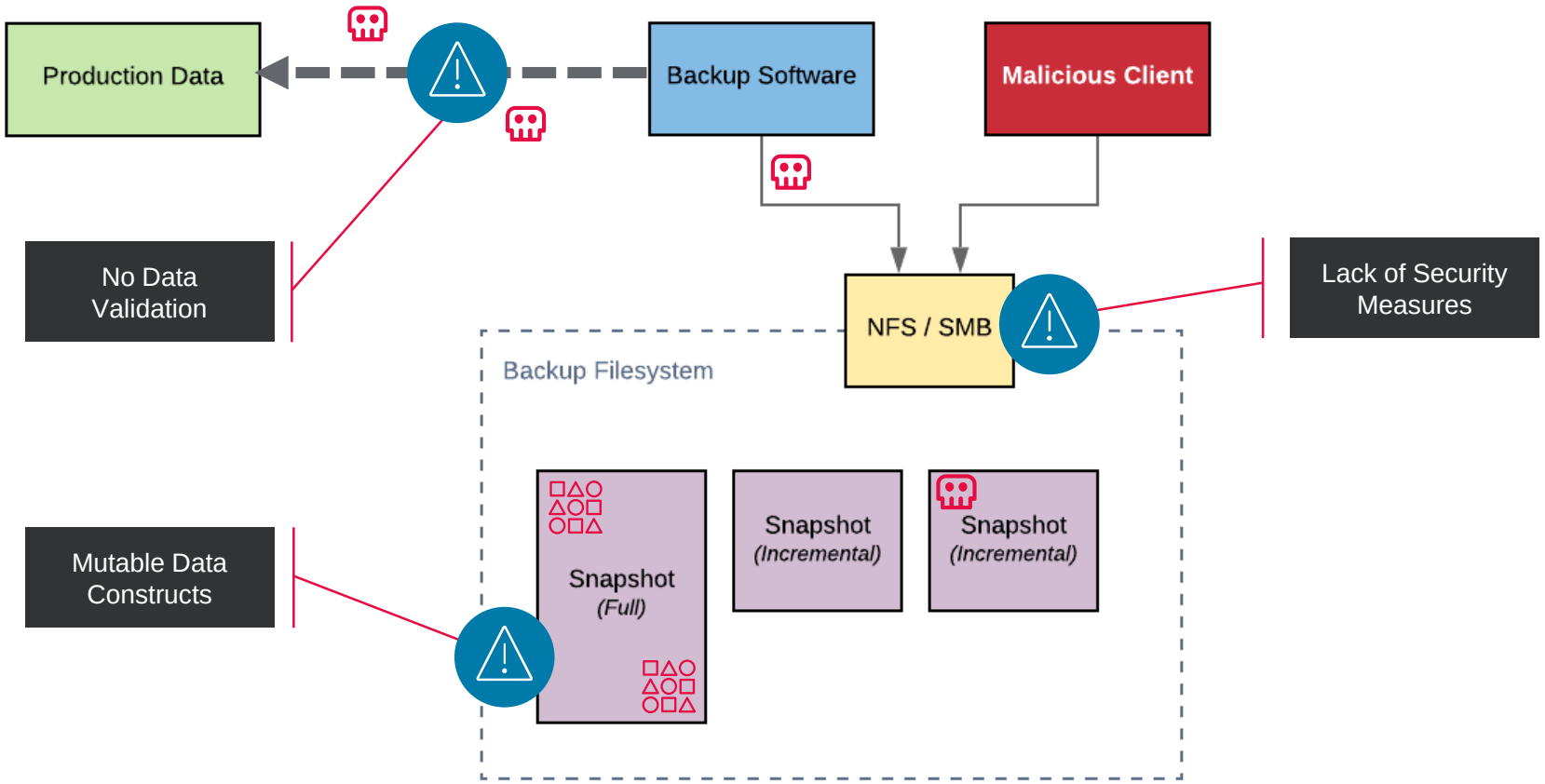
Require authentication to all endpoints that are used to operate the solution, including Role Based Access Control (RBAC) or Multi-tenancy features.

rubrik

DISTRIBUTED IMMUTABLE FILESYSTEM

rubrik

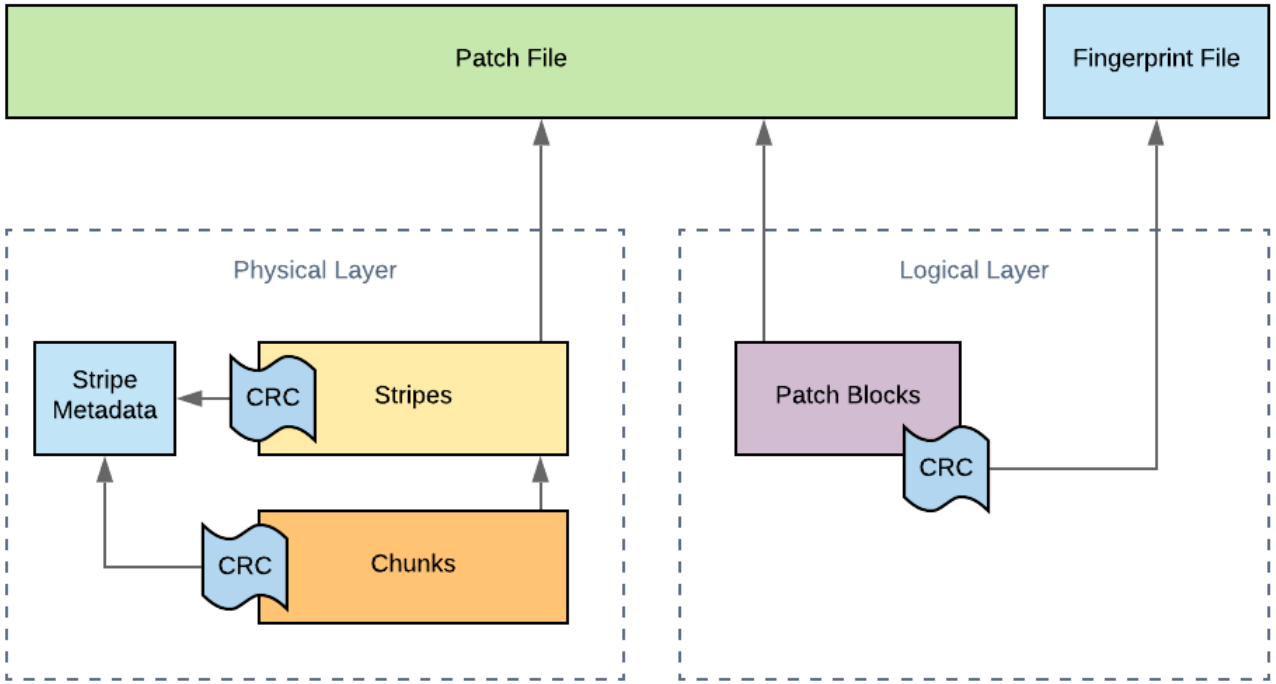
LEGACY / WANNABE-IMMUTABLE FILESYSTEMS



rubrik

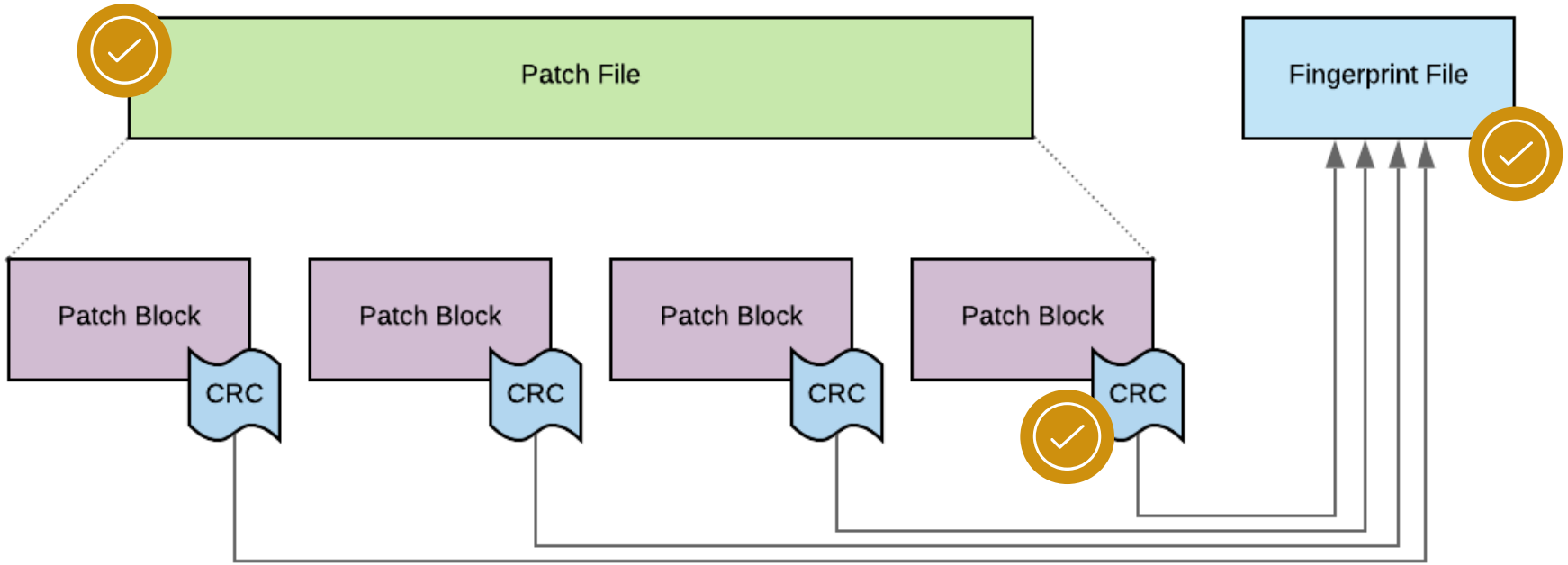
DISTRIBUTED IMMUTABLE FILESYSTEM

- Atlas, an **immutable** Filesystem in Userspace (FUSE)
- Distributed and immutable filesystem for writing and reading data for other **Rubrik services**.
- Backup data is **never exposed** to external clients through insecure methods or protocols.
- All writes are **out-of-place**, meaning that new writes will never touch data written earlier.



rubrik

CONSTRUCTING APPEND ONLY FILES (AOFs)



» Checksums (CRCs) are generated and written to a Fingerprint file.

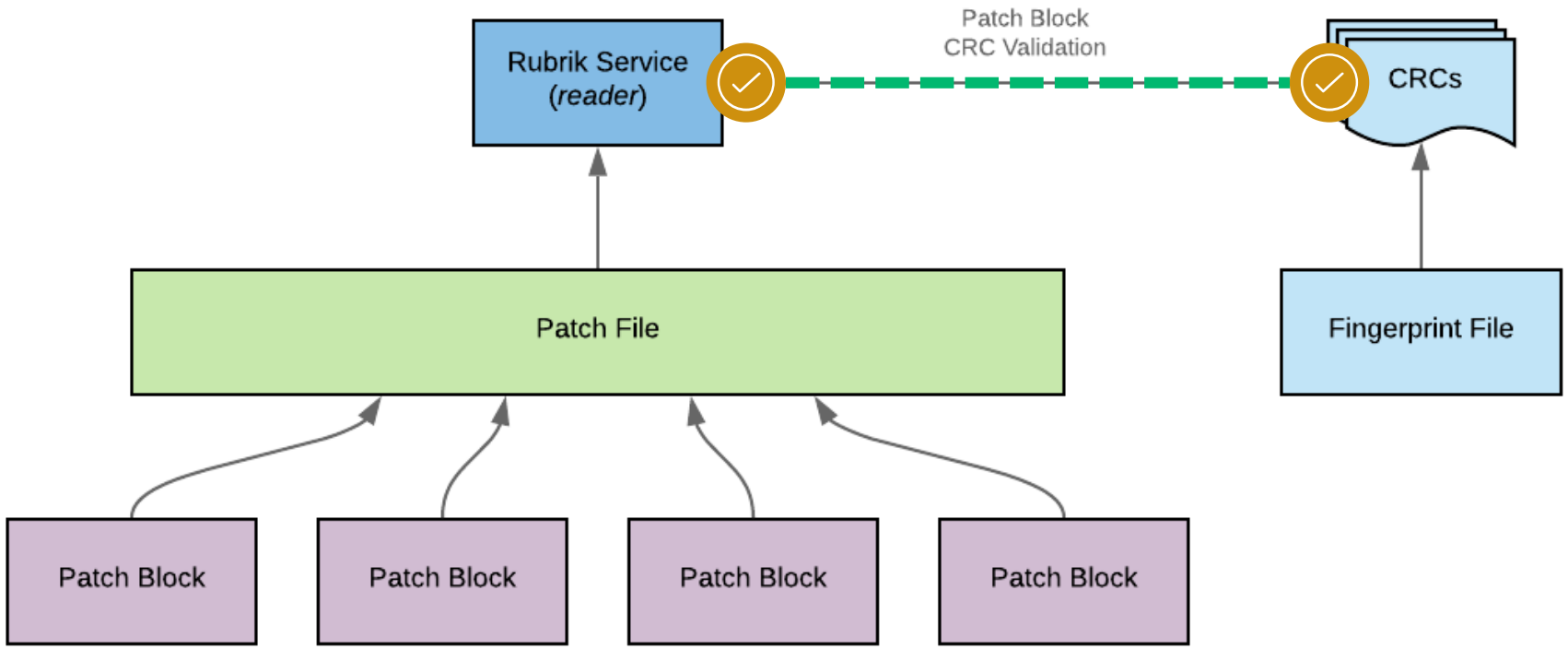
» Rubrik always does a Fingerprint check before committing any data transformations.

» Fingerprints stored along with data to ensure that once written, the data is never changed.

rubrik

IN-LINE READ VALIDATION

Files are not exposed to any external systems or customer administrator accounts.

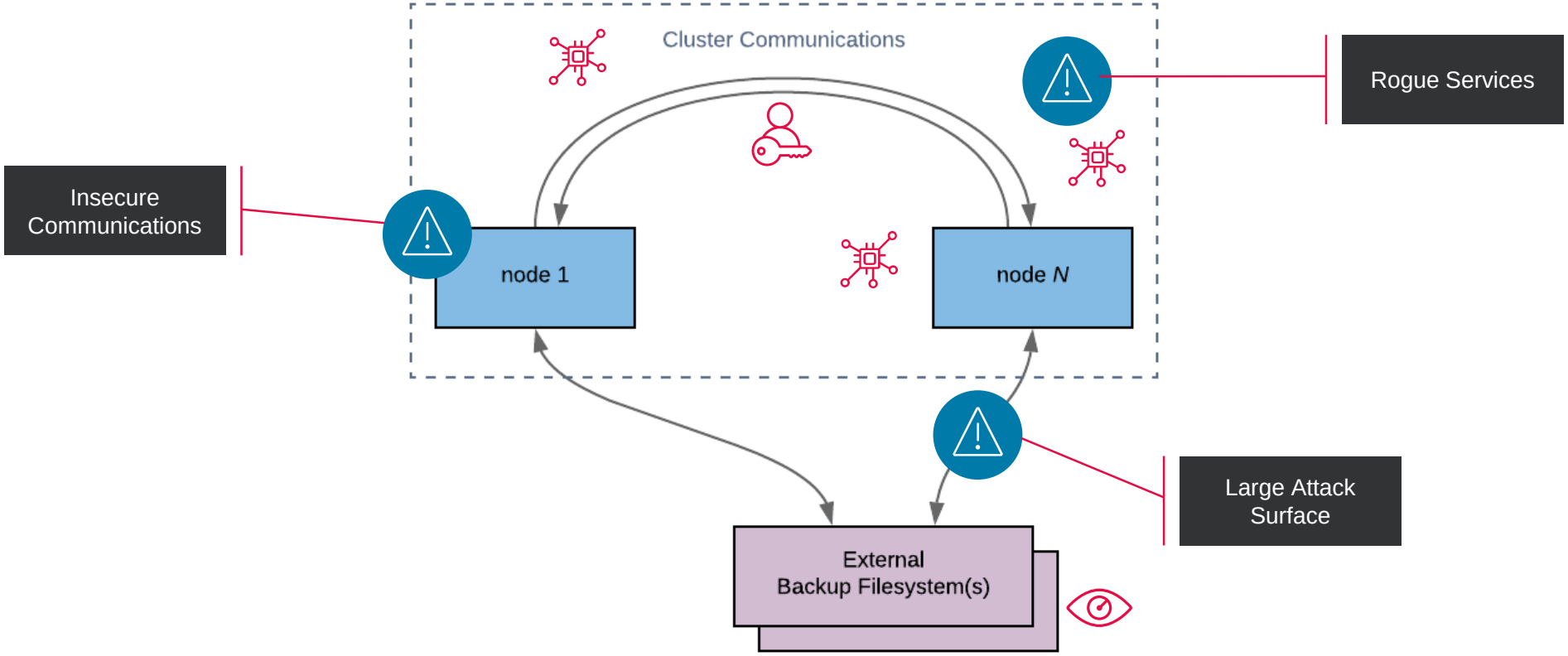


rubrik

ZERO TRUST CLUSTER DESIGN

rubrik

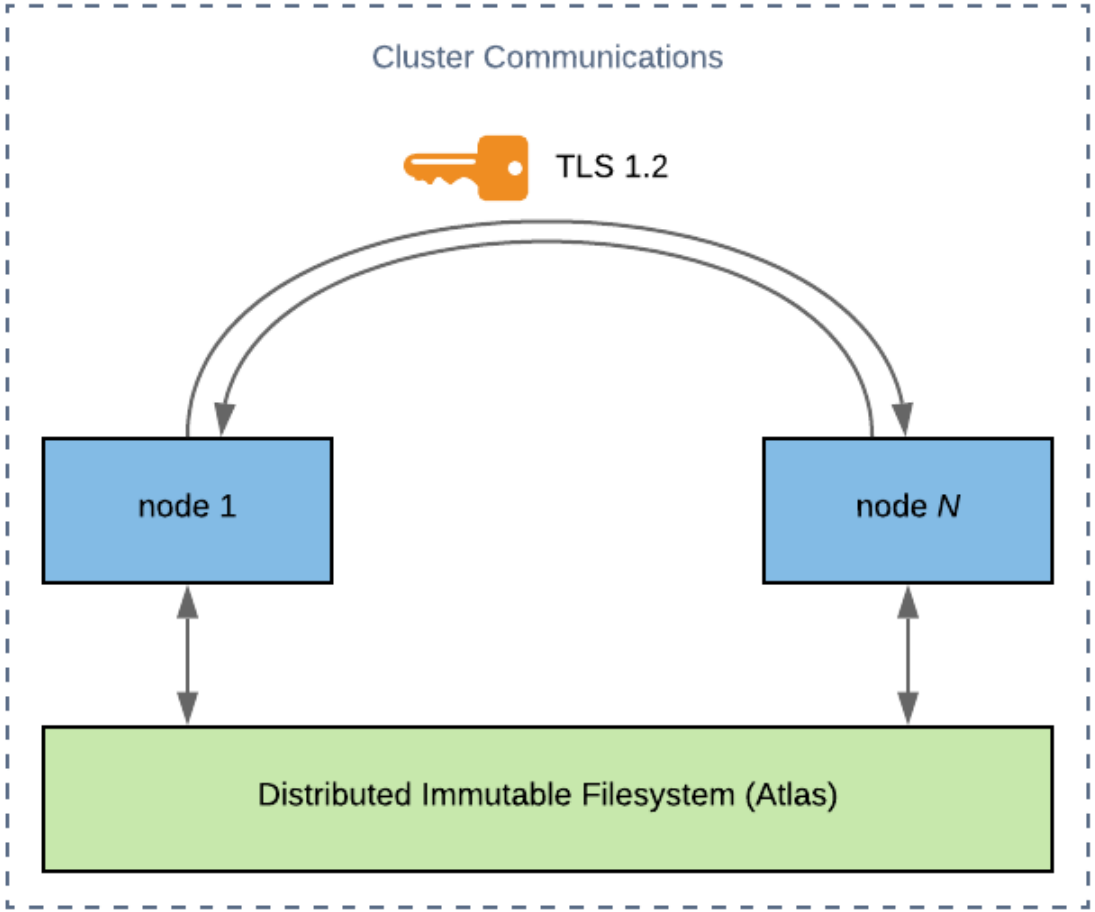
LEGACY “FULL TRUST” DESIGN



rubrik

ZERO TRUST CLUSTER DESIGN

- Validate each node that wants to exchange data.
- Rubrik requires certificate-based mutual authentication.
- Enforce TLS 1.2 with strong cipher suites and Perfect Forward Secrecy (PFS).

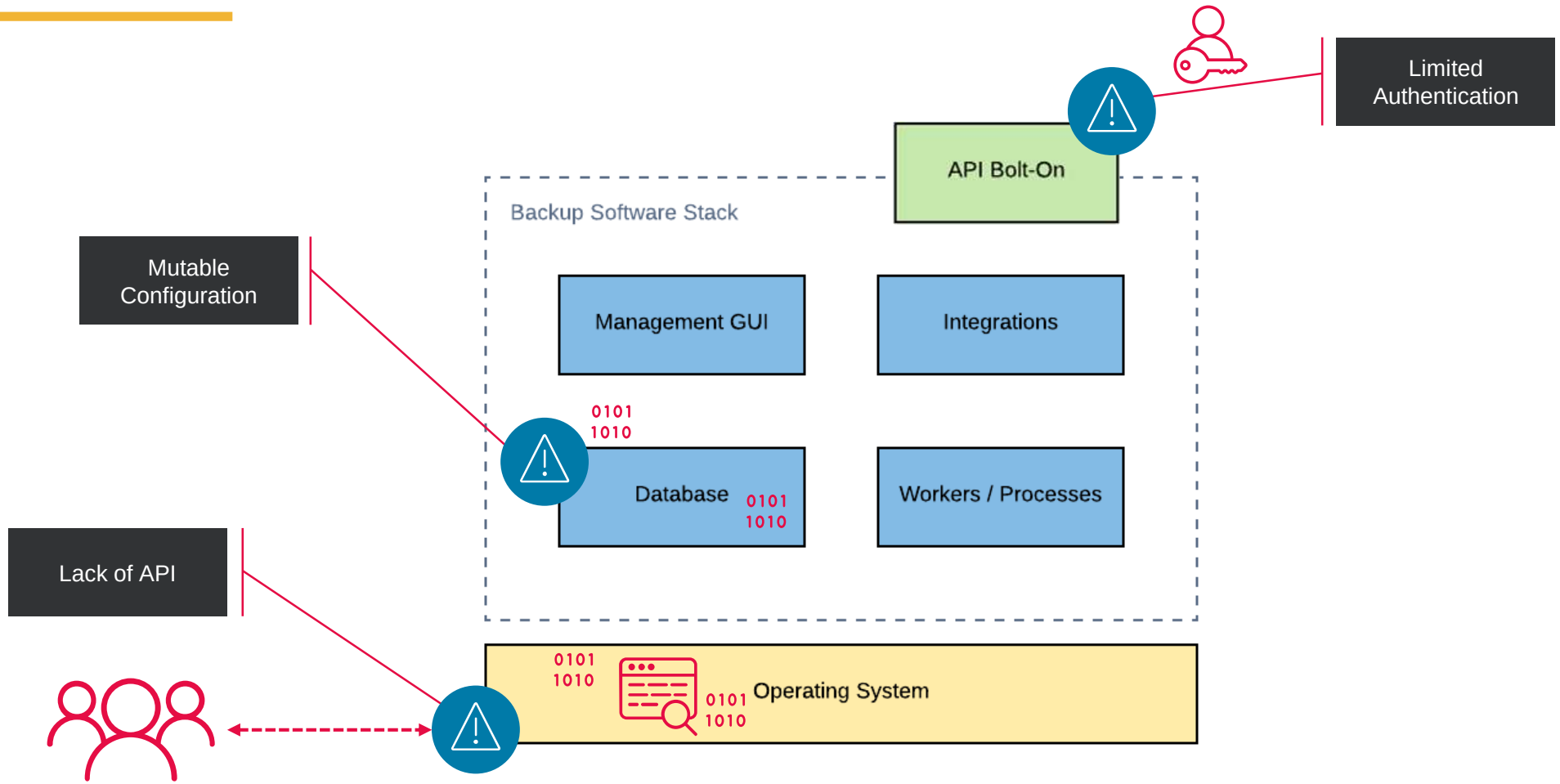


rubrik

AUTHENTICATED APIs AND TOOLS

rubrik

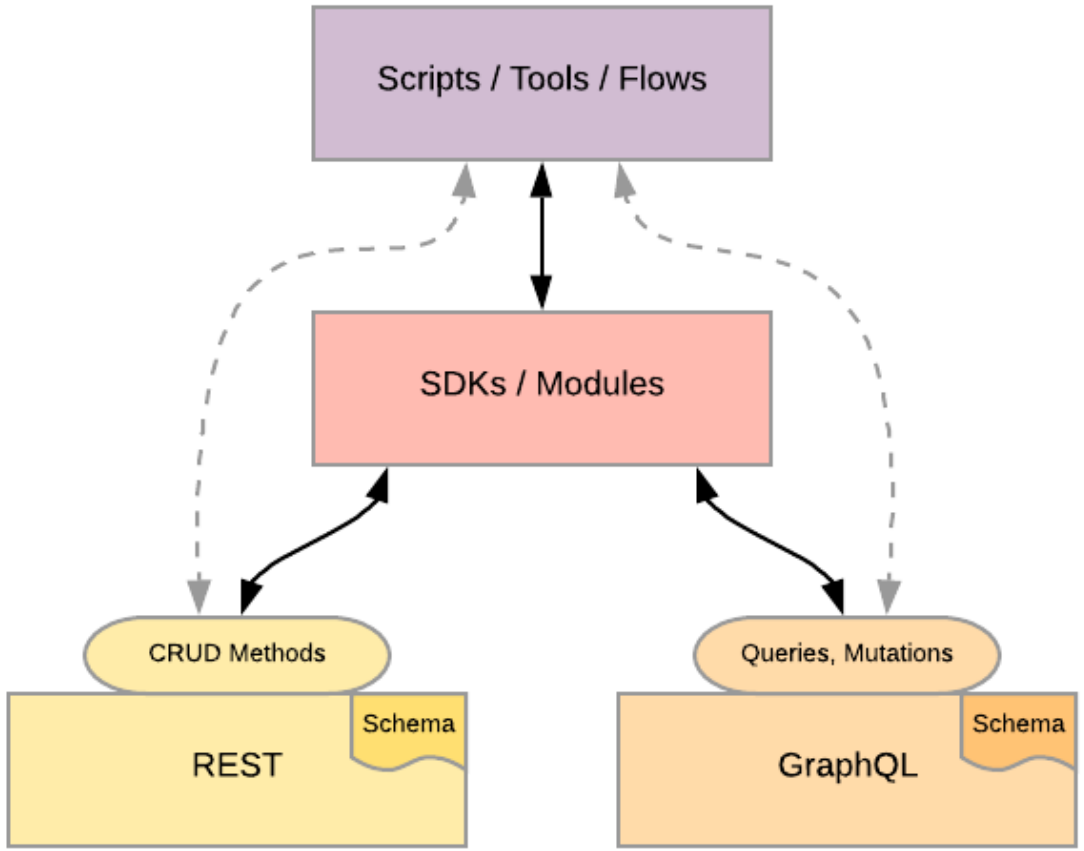
EXTENSIBILITY CONCERNS



rubrik

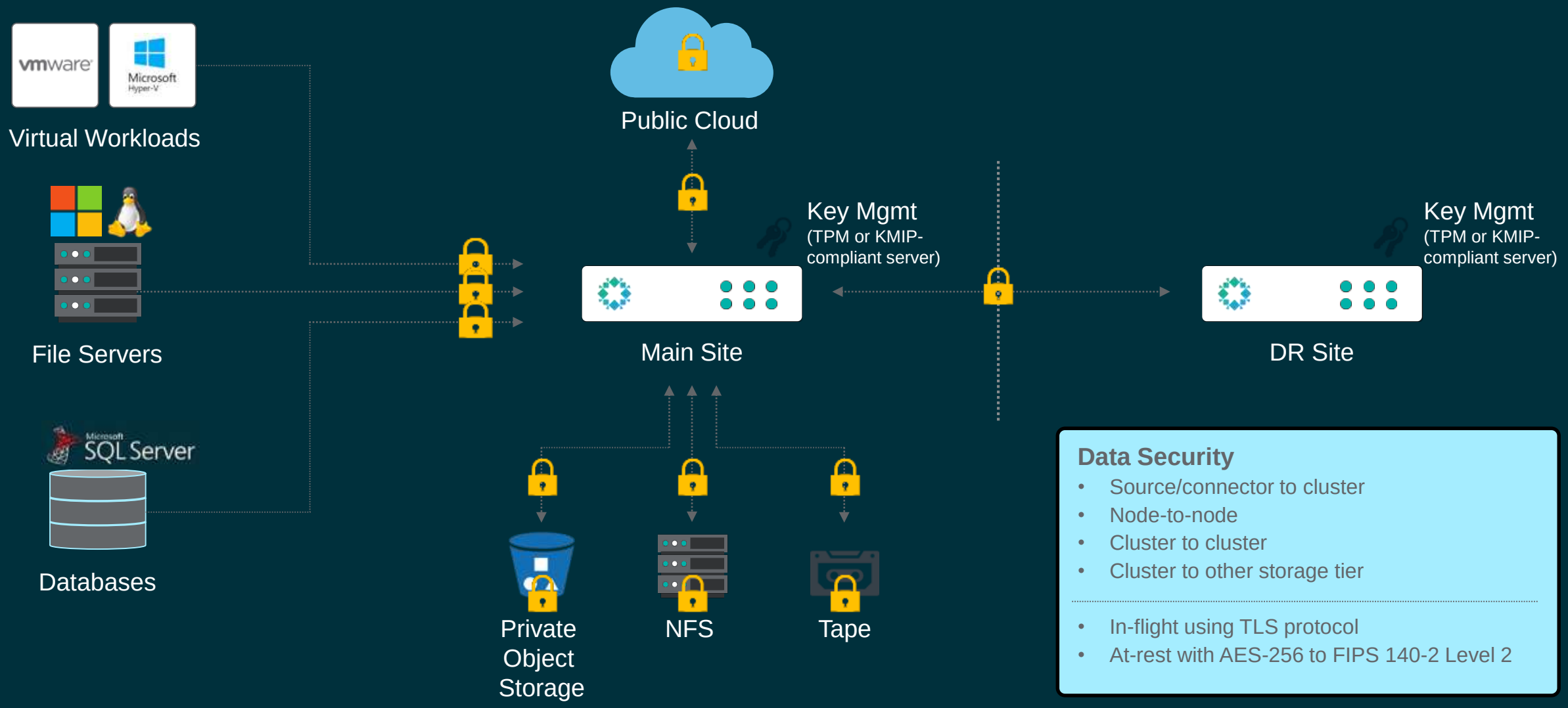
AUTHENTICATED APIs AND TOOLS

- Rubrik adopted an **API-first design** as part of the architecture.
- We require authentication to all endpoints that are used to operate the solution.
- Authentication can be handled via credentials or secure token.
- Rubrik's CLI, SDKs, and other tools consume the API and are held to the same security requirements.



rubrik

End-to-End Encryption



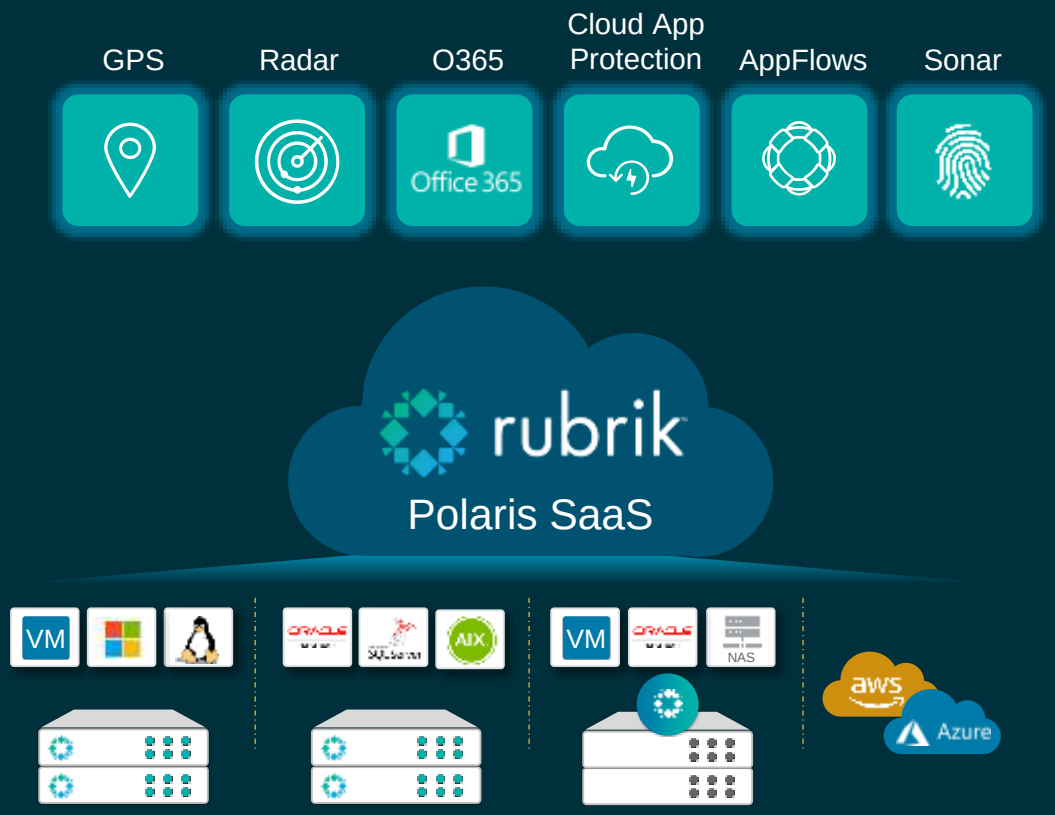
Data Security

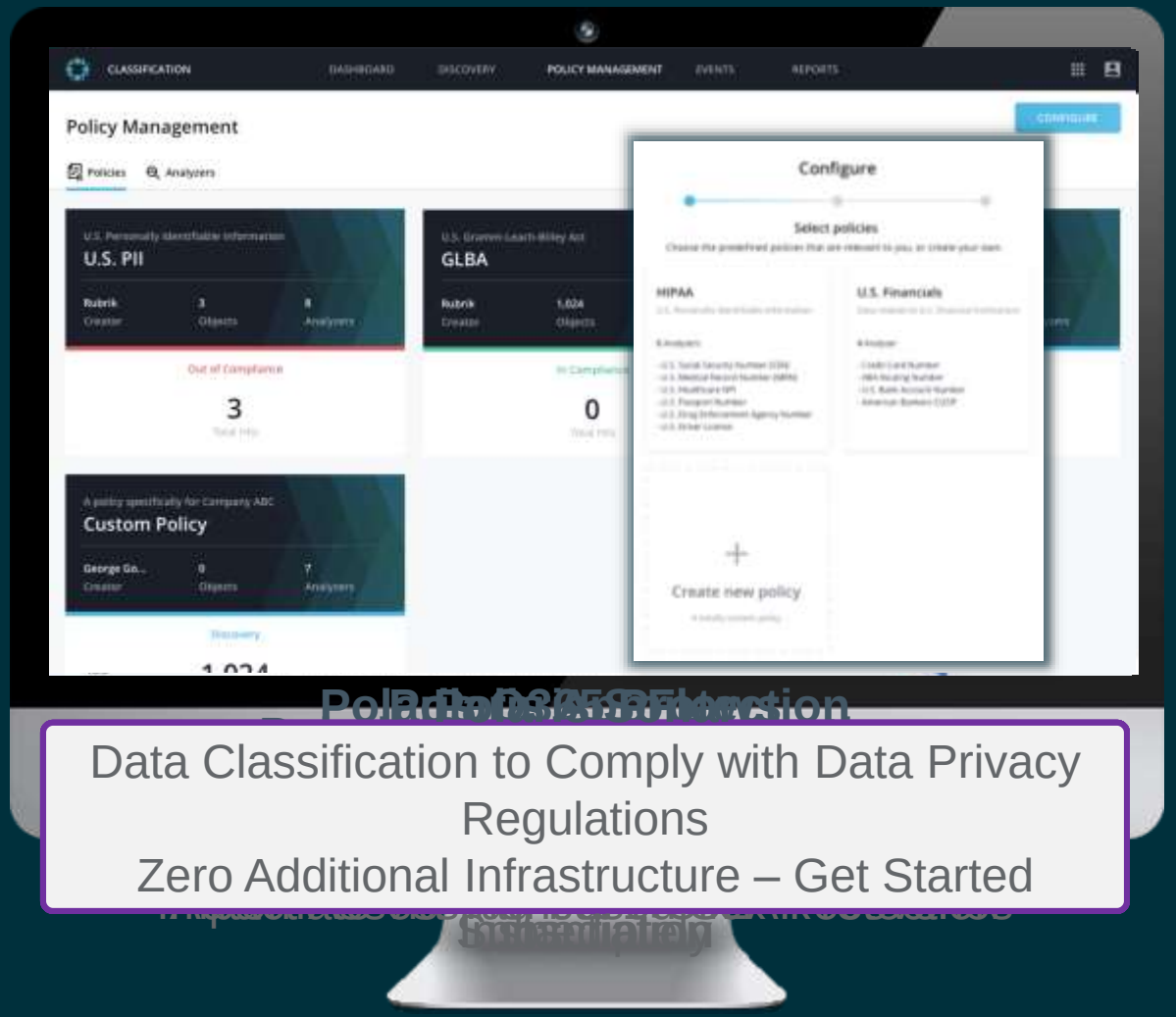
- Source/connector to cluster
- Node-to-node
- Cluster to cluster
- Cluster to other storage tier

- In-flight using TLS protocol
- At-rest with AES-256 to FIPS 140-2 Level 2

DETECT ATTACK
ALERT
RECOVER

Rubrik add-on security functions





Data Classification to Comply with Data Privacy Regulations
Zero Additional Infrastructure – Get Started

rubrik

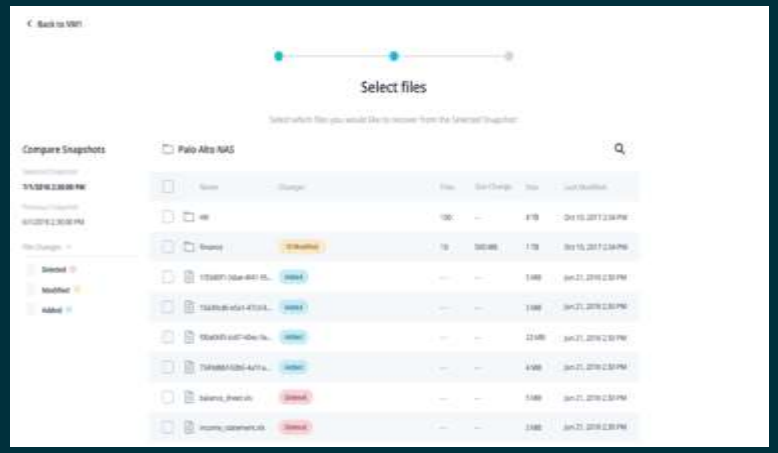
Our Approach: Recovery Accelerated and Simplified

The Rubrik Difference

Identify Abnormal Behavior

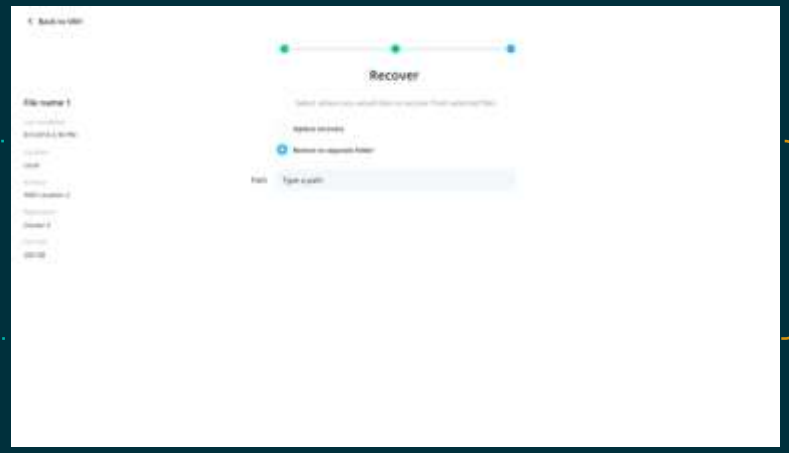
- ML-based anomaly detection on existing backup data for last line of defense
- Neural Network: 99.9% Accuracy
- API-first platform to plug into automation frameworks and SEIM tools

Granular Impact Assessment



- Automated assessment of blast radius
- Clear view into what applications and files were impacted and where
- Filter and choose recovery level

Immutability + Instant Recoveries



- Data is never available in read/write mode means it can't be overwritten
- 1-click recovery to most recent clean version (Restore/Live Mount/File-level)
- RTO down from Days to Minutes

rubrik

“

AFTER THE INCIDENT, WE WERE SO IMPRESSED THAT WE MOVED MORE OF OUR LEGACY SYSTEMS TO RUBRIK AND ARE FULLY CONFIDENT THAT

RUBRIK’S IMMUTABLE BACKUPS WILL PROTECT US FROM FUTURE INCIDENTS.

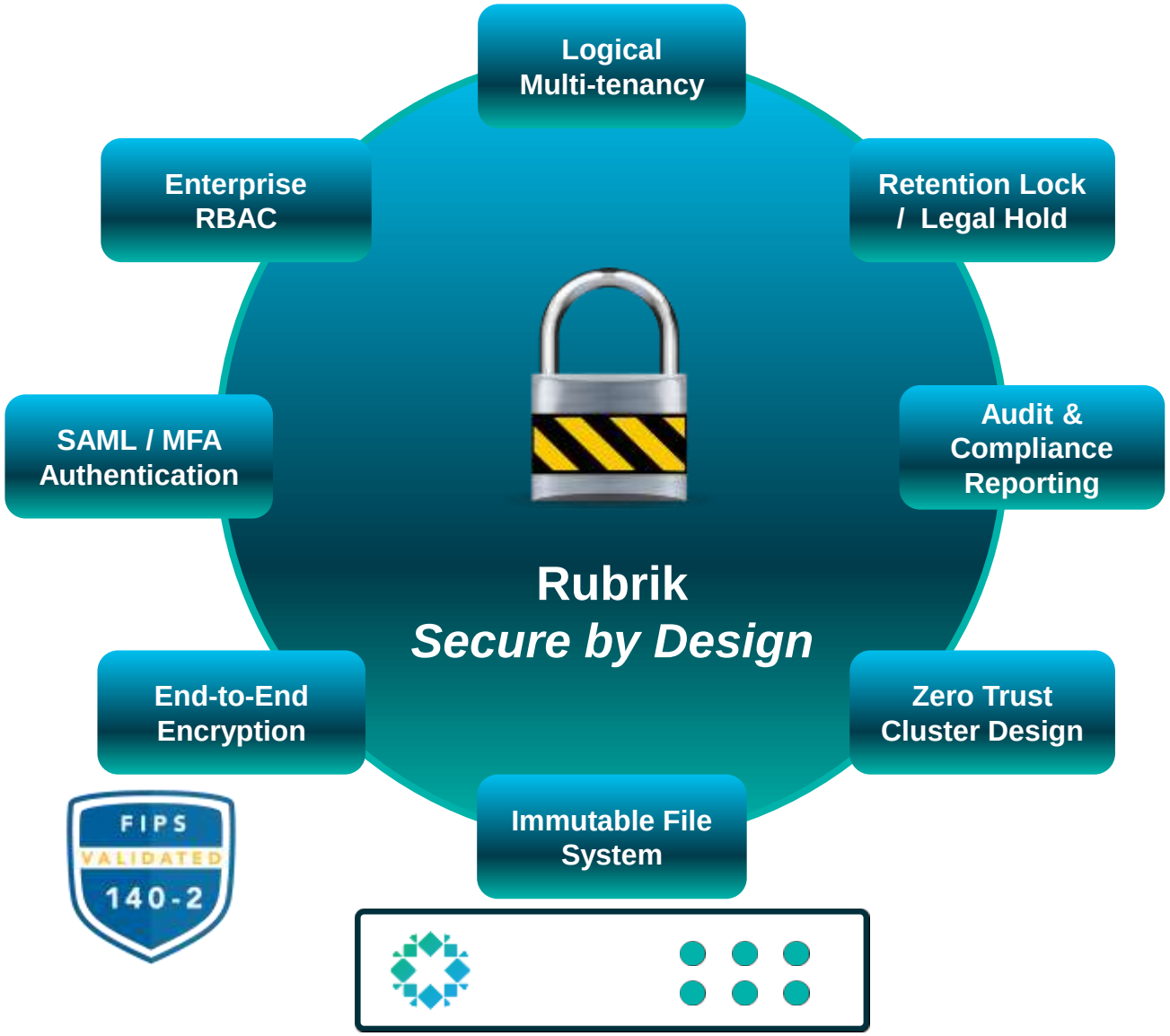
Craig Witmer, CTO at Kern Medical Center

Rubrik Security Hardening
Best Practices

August 2020

rubrik

The Rubrik Security Framework



SOC 2 TYPE 2

ISO 27001 Certified

FIPS VALIDATED 140-2

Rubrik Hardening Standard

No customer snapshot data held in Atlas is exposed in a readable format via the filesystem.	No way to “mount” snapshot data directly from the filesystem.
Only Rubrik certified services can run within the platform.	Provides no attack surfaces for malicious code, human error, or other pain points.
Rubrik pre-configures the iptables of the underlying operating system to whitelist services that can access each other.	Eliminates external access to internal services. Using a whitelist greatly reduces the attack surface area.
All Rubrik software images are signed by authorized personnel. The signature is verified during the boot process.	Ensures software retrieved matches what was generated by the development team. Software upgrades will fail if the signature does not match.
All unused ports are disabled on the product.	Ports that are not needed for the production to function are no longer potential intrusion points for attackers.

Security Review Checklist

- [ ] Local Account Security
- [ ] Domain Account Security
- [ ] Automation Security
- [ ] Roles and Permission Review
- [ ] System Reset Protection
- [ ] Enabling Auditing / Syslog
- [ ] Securing NTP Servers
- [ ] Login Banners
- [ ] SMB / NFS Security Review
- [ ] S3 / Archive Security Review
- [ ] SLA / Object Protection
- [ ] Physical Site Security
- [ ] Deliver copies of technical whitepapers on best practices

rubrik

Local Account Security

DO's

Best Practices

1. Use unique and strong passwords
2. Rotate passwords frequently (30-90 days)
3. Admin access should be the exception not the rule
4. Syslog / Alert on admin level login attempts / failures
5. Enable MFA on local admin accounts
   If MFA isn't available, physically shard password to give additional protection of control
6. Store credentials in encrypted vault or key store
7. Separate primary and secondary credential storage in separate encrypted vaults

DONT's

Best Practices

1. No password re-use across clusters or instances

➔ Users (under Access Management) ➔ Select the Ellipsis (...) ➔ Password Requirements.

Domain Account Security

DO's

Best Practices

1. Only use domain accounts for application or end-user level accounts where possible
2. Align RBAC permissions by need and enforce principle of least privilege access
3. Enable MFA for all domain accounts
4. Enable upstream MFA with SSO provider via SAML

DONT's

Best Practices

1. Do not enroll target replication clusters in same AD / LDAP domains

Microsoft Active Directory

LDAP

RSA SecurID

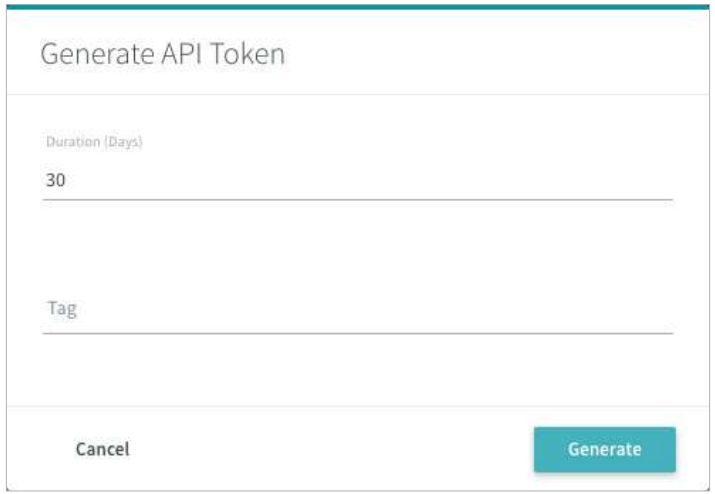
SAML

Automation Security

DO's

Best Practices

1. Create new user account for each automation task
2. Enforce limited scope of privileges via RBAC
3. Ensure automation account **does not** have data expiry or SLA change permissions unless necessary
4. User `TOKEN` authentication over `Basic` authentication when programmatically connection to Rubrik cluster
5. Store `TOKEN` and access keys in secure vault or key store system

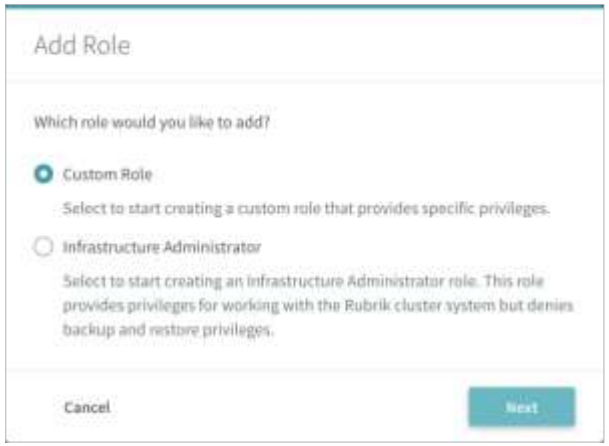


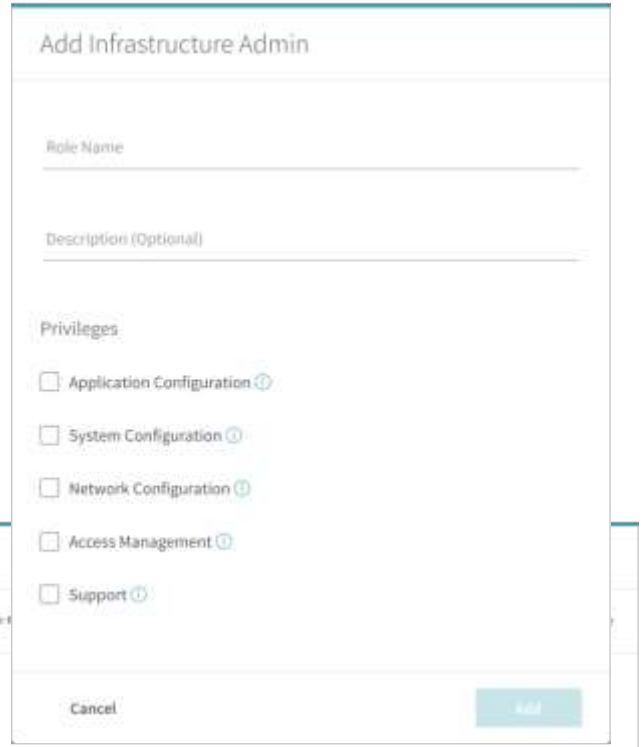
DONT's

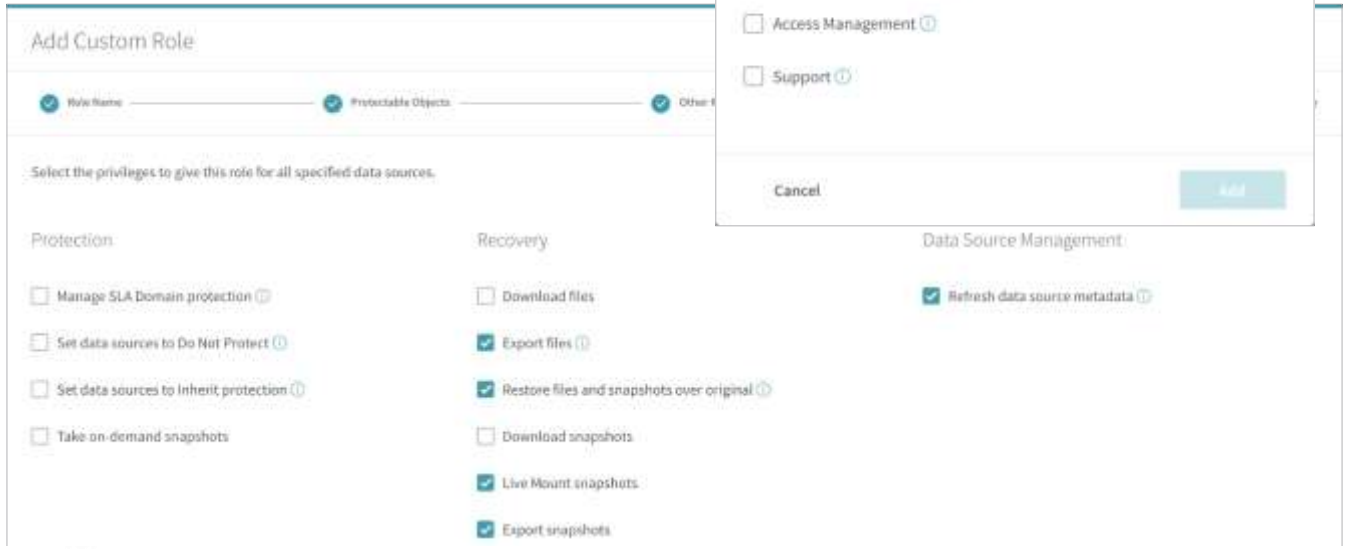
Best Practices

1. Never store any credentials directly in your automation code

Granular Role-Based Access Controls







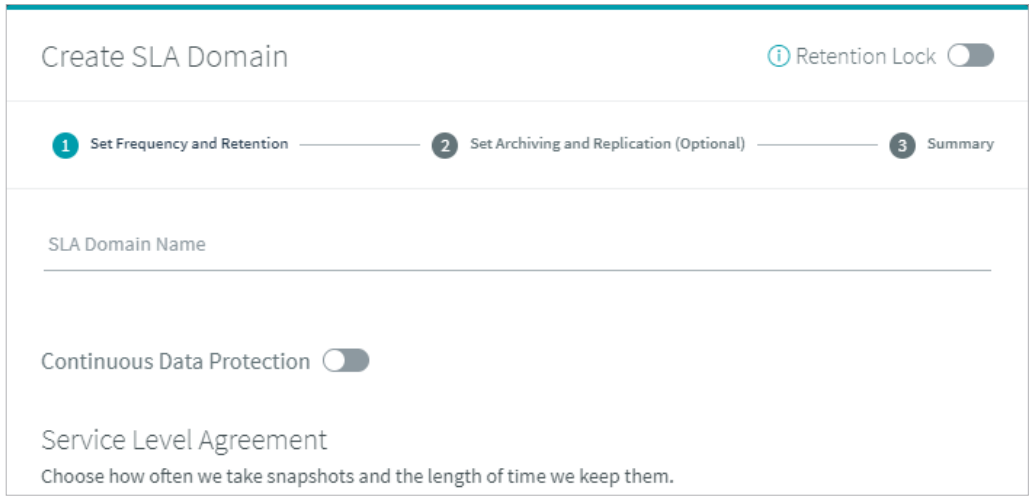
<u>Infrastructure Admin Role</u> - The Infrastructure Admin role template provides privileges for working with the Rubrik cluster system but denies backup, restore, and policy creation / deletion privileges.

This role should be leveraged for separating the infrastructure operations from data plane operations for scoping limited access accounts.

<u>Custom Role</u> - The custom role provides for defining access to data plane operations for managing Protection, Recovery, and Data Source Management**<u>.</u>**

⚙ **➔ Users (under Access Management) ➔ Select the Ellipsis (...) ➔ Roles ➔ +Add Role (*wizard*)**

Retention Locked SLA Protection



1. A Factory Reset of the cluster/node cannot be performed once Retention Lock has been enabled by Rubrik Support:
   A common attack vector is an immediate attempt to perform a factory reset on the appliance in order to instantly wipe out backup data. This becomes impossible to do without the intervention of Rubrik Support when the Retention Lock feature is globally enabled. Below is the messaging that an administrator is presented with when trying to perform a reset through conventional means:

```
Node reset is disallowed
This Rubik cluster has Retention Lock policies that prevent reset. Contact Support to enable reset.
```

   If a reset absolutely has to be performed for any reason, please contact Rubrik Support.

2. The only modifications allowed on SLA Domains are for "stronger" and "more secure" configurations:
   Any attempt now to reconfigure the SLA Domain that might contribute to a weaker configuration or contribute to the expiration of existing data is prohibited. This is specifically designed to prevent the accidental or malicious attempts at modifying the SLA that causes expiration/pruning of existing data. There are also restrictions in place to prevent the removal or any archival locations or replication targets associated with the SLA. Additional details about the specific restrictions involved here can be found in the Rubrik CDM User Guide.

3. An external time source is required:
   A local time source is no longer allowed with Retention Lock enabled. When combined with using secure time sources in the manner mentioned above, this can be leveraged to prevent rogue time source attacks used to prematurely expire data by fast forwarding past the retention period.

IMPORTANT: Retention Lock is globally disabled on the cluster by default. Rubrik Support must be contacted and a case must be opened in order to have Retention Lock enabled and configurable within the Rubrik UI. There is also a special authorization step that includes setting up particular customer authorized contacts that the support team will walk through prior to enabling Retention Lock into the Rubrik UI of the cluster.

Enhanced System Reset Protection

*Beginning with Rubrik CMD versions (5.1.3.-p3, 5.1.4, 5.2.1, and 5.3EA2) a system level patch is being integrated into the CMD platform to remove admin access to invoke **sdreset** at the Rubrik CLI.*

DO's

Best Practices

1. Consider upgrading to a patched version of Rubrik CDM to gain protection against accidental or adversarial system level reset as soon as possible

```
Node reset is disallowed
This Rubik cluster has Retention Lock policies that prevent reset. Contact Support to enable reset.
```

Important: *Rubrik support engagement will be required for any reset of nodes or clusters once systems are running on the reset restricted code versions. This includes at the completion of a **proof of concept** test to factory reset.*

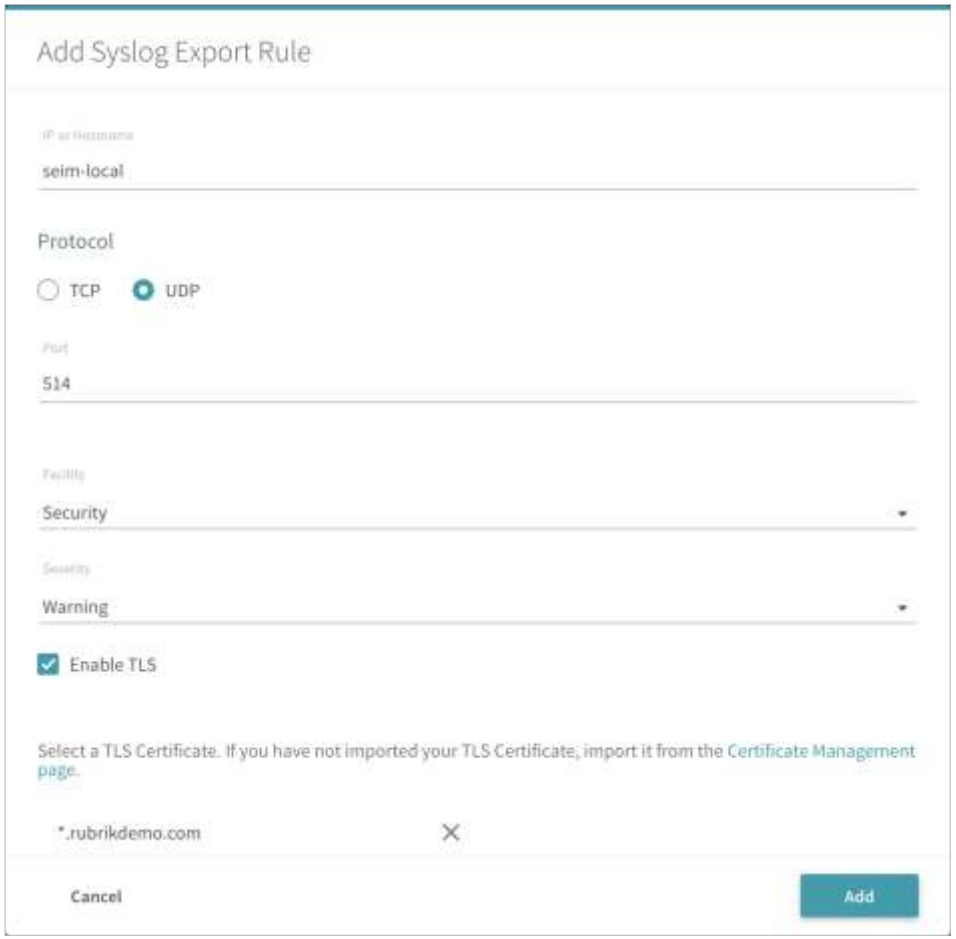
Auditing / Syslog

DO's

Best Practices

1. Enable auditing via Syslog for off appliance and out of band recording of activity
2. Refer to Rubrik CDM User Guide for facility and severity level descriptions
3. Enable TLS support encrypted syslog traffic with imported certificate
4. Leverage Polaris GPS for federated reporting and auditing of events and activity logs

Important: *Rubrik CDM keeps approximately 90 days of activity in a rolling log on each cluster. Activity and logging volume impacts actual retention. Polaris GPS maintains 12 months of rolling activity logs from managed Rubrik clusters.*



➔ Notification Settings ➔ Add Syslog Export Rule.

Securing NTP Time Sources

The Network Time Protocol (NTP) is an Internet protocol built to distribute precise time around a computer network. NTP makes use of UDP over TCP/IP to synchronize network time clients to a precise time reference. The NTP protocol can make use of encryption keys to authenticate a timeserver.

DO’s

Best Practices

1. Leverage an encrypted NTP Stratum-1 time source where available
2. Enable primary and secondary NTP time sources for redundancy

➔ **Network Configuration (Network Settings) ➔ NTP Servers**

Rubrik Solution for External Threats (Malicious Software)

1. **Rubrik's Architecture:**
   - Rubrik is a "Master-less" web-scale architecture that does not rely on a master server or proxy infrastructure - No attack vectors in the platform that are commonly seen in legacy architectures (i.e., Master server running on windows and and media agents running on Windows/Linux OS with attack vectors to libraries and de-deduplication databases

2. **Rubrik's Immutable File System:**
   - Integrity of data cannot be compromised once committed to Rubrik's proprietary "Atlas" file system.
     - Malicious actors are not able to modify snapshot data held within the Rubrik cluster due to the nature of its filesystem design.
   - Existing snapshots on Rubrik are immune to ransomware on production environment

3. **Recoverability in Event of Attack:**
   - Quickly and efficiently restore data to a known-good state. Rubrik relies on the immutable nature of its filesystem to execute this restore.
   - "Live Mount" Operation allows applications to leverage Rubrik's resources to instantly restore from last clean copy

Rubrik Solution for Internal Threats (Rogue Admin)

Rogue Administrator/Compromised Administrator Protection:

1. Rubrik's Retention Lock (WORM SLA) feature enables the protection against malicious or accidental modifications of SLA policy resulting in loss or destruction of data. Retention lock can be able with engagement of the Rubrik support organization. Retention Lock is a FINRA (SEC 17a-4) compliant security feature.

   Once enabled on the cluster, only the global admin with appropriate access control can create and edit these SLA's. The following safeguard conditions apply once Retention Lock is enabled:

   - Edits are limited to an increase in retention time but cannot be decreased.
   - Frequency can be increased but cannot be decreased.
   - Retention on any location can be increased but cannot be decreased. This includes local, replication and archival retention.
   - Retention Lock SLA Domains cannot be deleted without engagement by Rubrik support with appropriate management approvals.

2. Enterprise Role Based Access Controls allow for granular separation of permissions and data access to confirm to the principle of least privileged access.

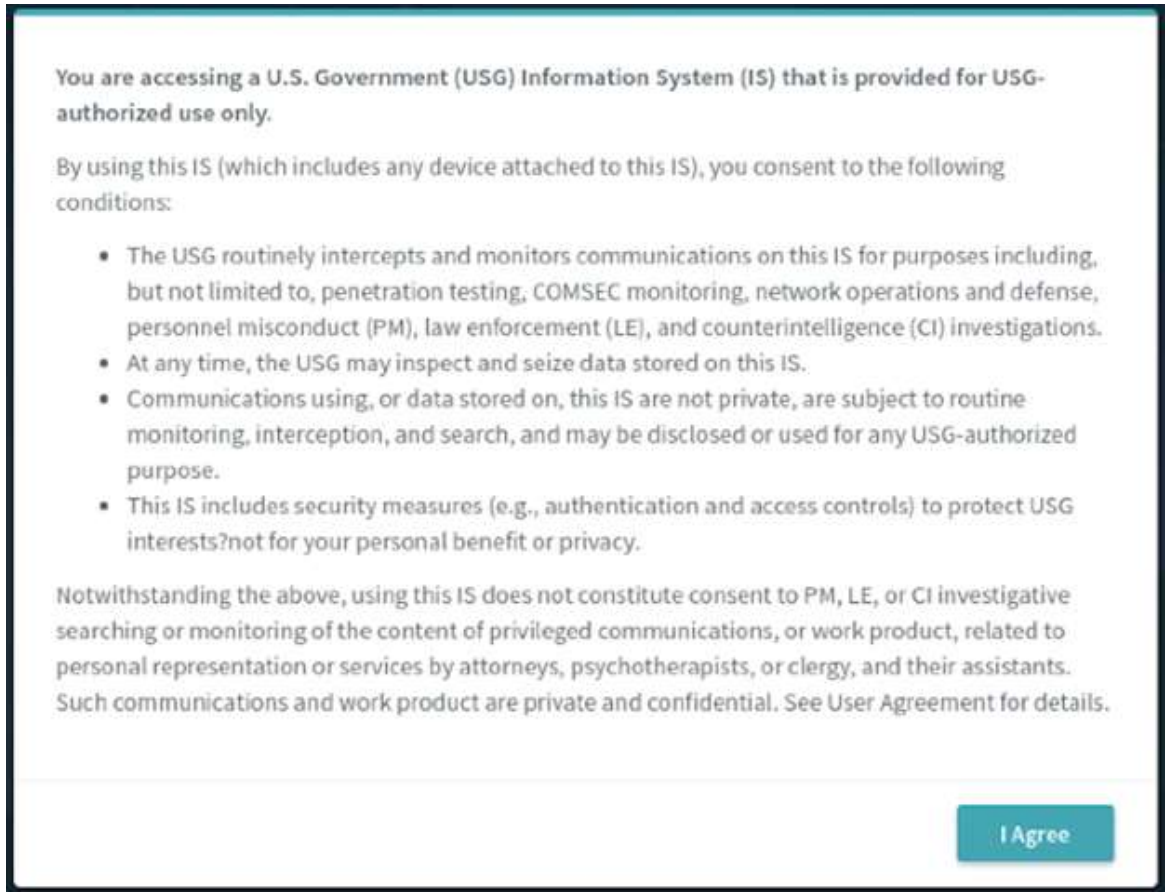
3. MFA / 2FA integration via SAML or RSA SecurID support for secondary authentication on admin and end-user accounts

Login Banners

DO's

Best Practices

1. Enable pre-login banners where desired or required
2. Set security classification notification banners if desired or required



You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- At any time, the USG may inspect and seize data stored on this IS.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests?not for your personal benefit or privacy.

Notwithstanding the above, using this IS does not constitute consent to PM, LE, or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

I Agree

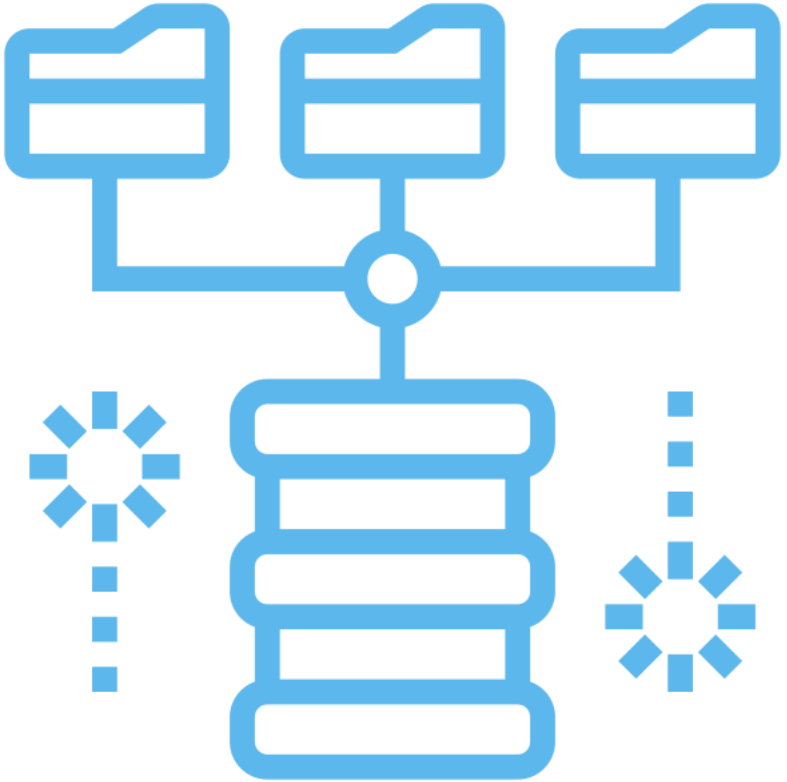
➔ Cluster Settings ➔ Select the Login Banner Text ➔ Enter notice text

NFS / SMB Security

DO's

Best Practices

1. Use secure SMB for SMB shares
2. Use IP allow-lists for all NFS archival locations and clients
3. Use Kerberos for NFS archival locations
4. User Username / Password authentication for NFS Filesets
5. Use Client Patterns with Managed Volumes



S3 / Archive Security

DO's

Best Practices

1. Leverage the principal of least privileged access
2. Store archival location credentials securely
3. Store the archival location encryption key securely / AWS CloudKMS
4. Leveraging auditing tools for continuous monitoring

OPTIONAL

Best Practices

1. Leverage versioning for bucket / blog protection

WARNING: Rubrik CDM does not integrate directly any versioning features with any of the major cloud providers today. What this means is that Rubrik CDM will not be aware of the versioning that is happening in the background. This can lead to excess capacity being used within the archives as when CloudOut deletes expired data in the archive, the data won't be deleted on the backend even though CDM will think it has been purged.

ADDITIONAL RESOURCES

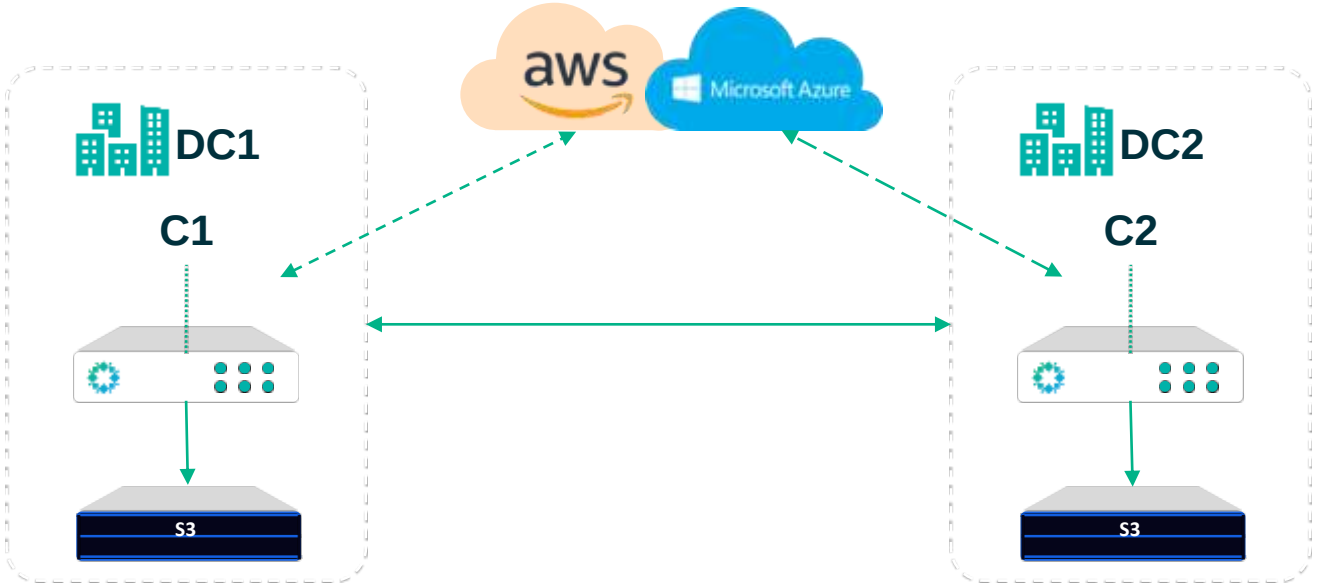
- Security Hardening Rubrik CloudOut for AWS (RWP-0517)
- Security Hardening Rubrik CloudOut for Azure (RWP-0518 *(coming)*

Physical Site Security Protection

DO's

Best Practices

1. Secure Rubrik nodes in locked racks or cages where possible
2. Limit physical access to only authorized personal to when access is required
3. Enforce principle of 3-2-1 for data protection (3 copies of data, 2 different locations, 1 offsite) by leveraging Rubrik site-to-site replication or CloudOut



Security Review Checklist

- ☑ Local Account Security
- ☑ Domain Account Security
- ☑ Automation Security
- ☑ Roles and Permission Review
- ☑ System Reset Protection
- ☑ Enabling Auditing / Syslog
- ☑ Securing NTP Servers
- ☑ Login Banners
- ☑ SMB / NFS Security Review
- ☑ S3 / Archive Security Review
- ☑ SLA / Object Protection
- ☑ Physical Site Security
- ☑ Deliver copies of technical whitepapers on best practices

rubrik

Don’t Backup. Go Forward.