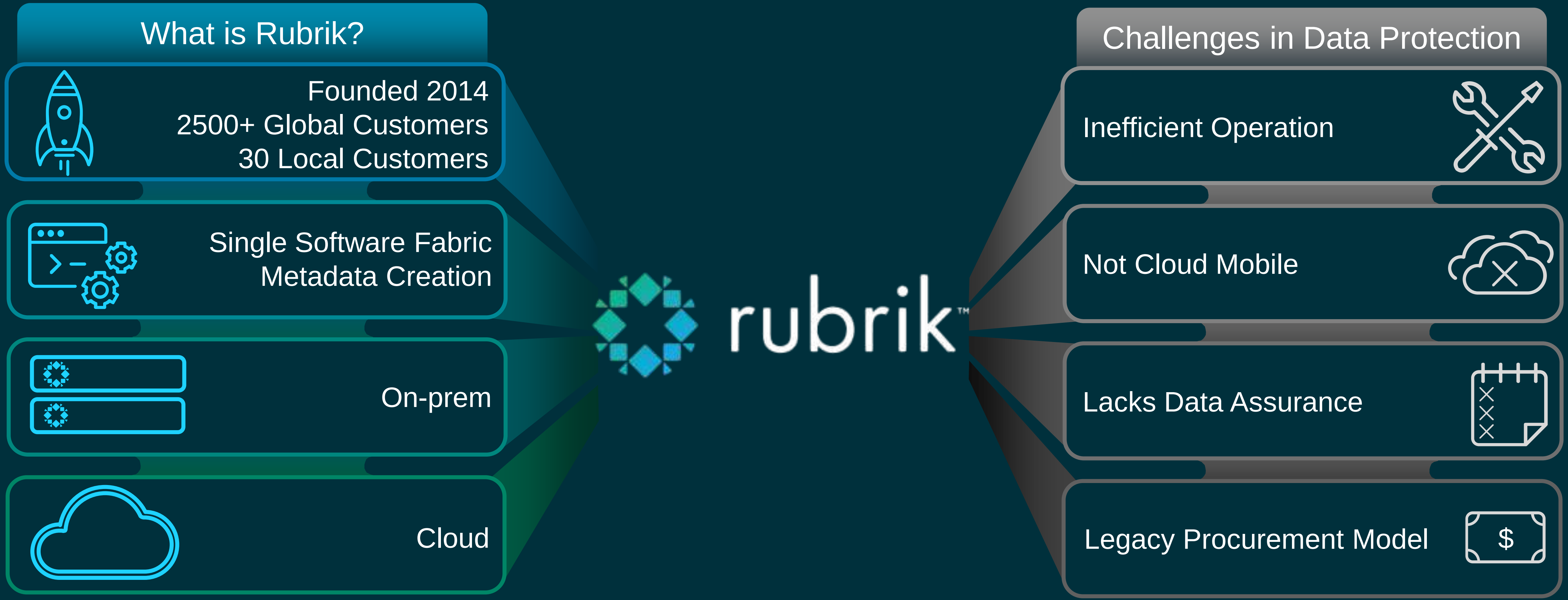
Rubrik Zero Trust Architecture

Salvatore *Buccoliero – Channel SE Nordic*
Salvatore@rubrik.com

Introduction to Rubrik



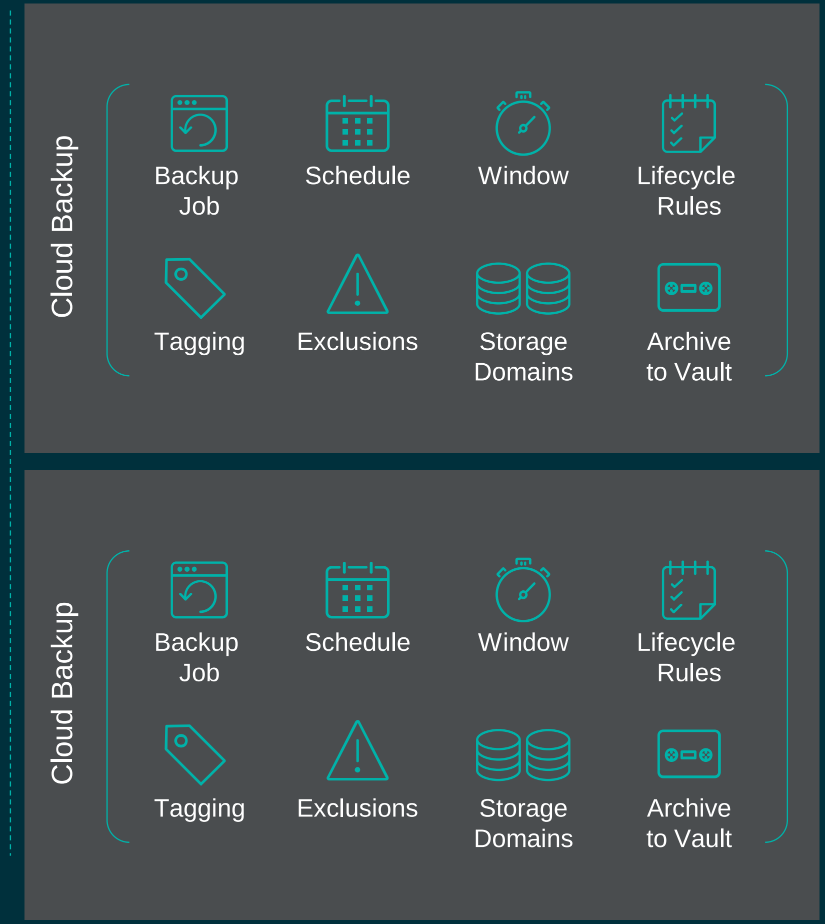
What is Rubrik?

- Founded 2014
  2500+ Global Customers
  30 Local Customers
- Single Software Fabric
  Metadata Creation
- On-prem
- Cloud

Challenges in Data Protection

- Inefficient Operation
- Not Cloud Mobile
- Lacks Data Assurance
- Legacy Procurement Model

Siloed Tool Sprawl + Processes = Loss of Data Control



Cloud Backup

Backup Job

Schedule

Window

Lifecycle Rules

Tagging

Exclusions

Storage Domains

Archive to Vault

Cloud Backup

Backup Job

Schedule

Window

Lifecycle Rules

Tagging

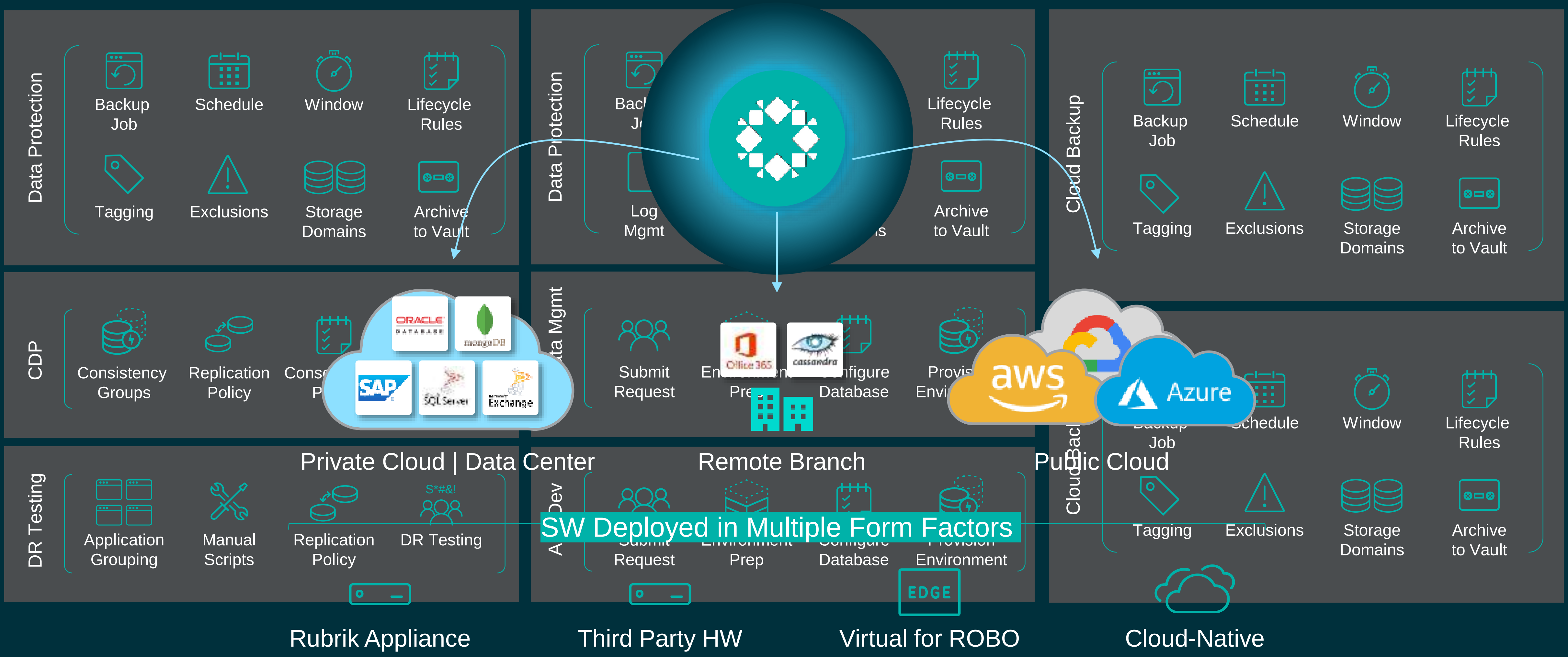
Exclusions

Storage Domains

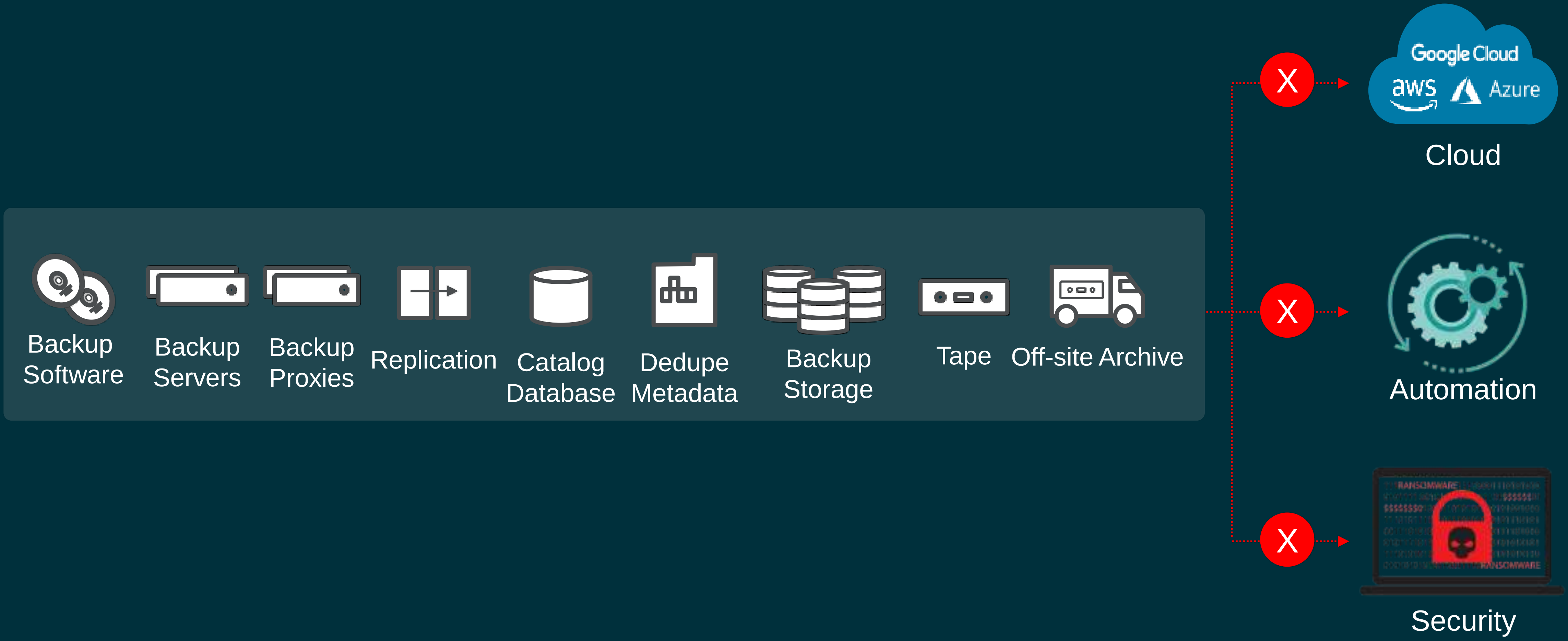
Archive to Vault

Costly, complex, and inhibits transformation

Introducing a New Approach to Data Management



Data Management: 1990s to Present



Backup Software

Backup Servers

Backup Proxies

Replication

Catalog Database

Dedupe Metadata

Backup Storage

Tape

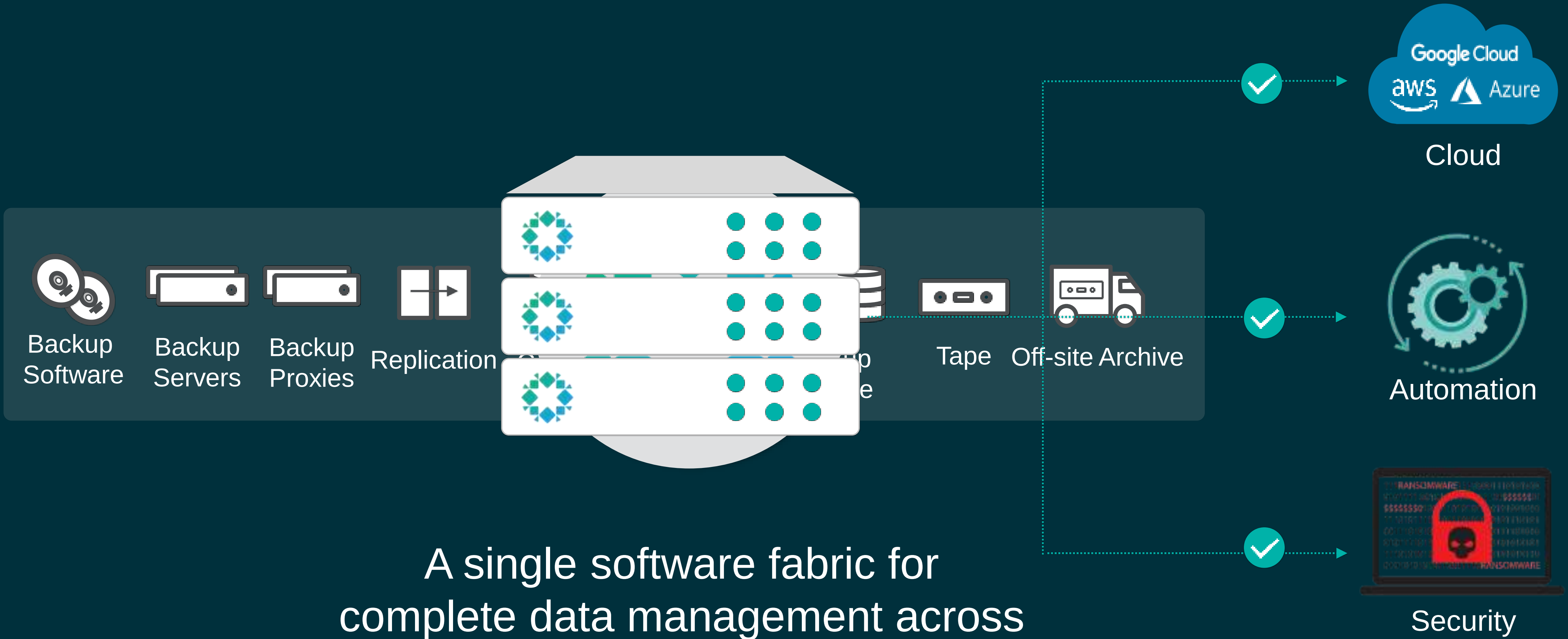
Off-site Archive

Cloud

Automation

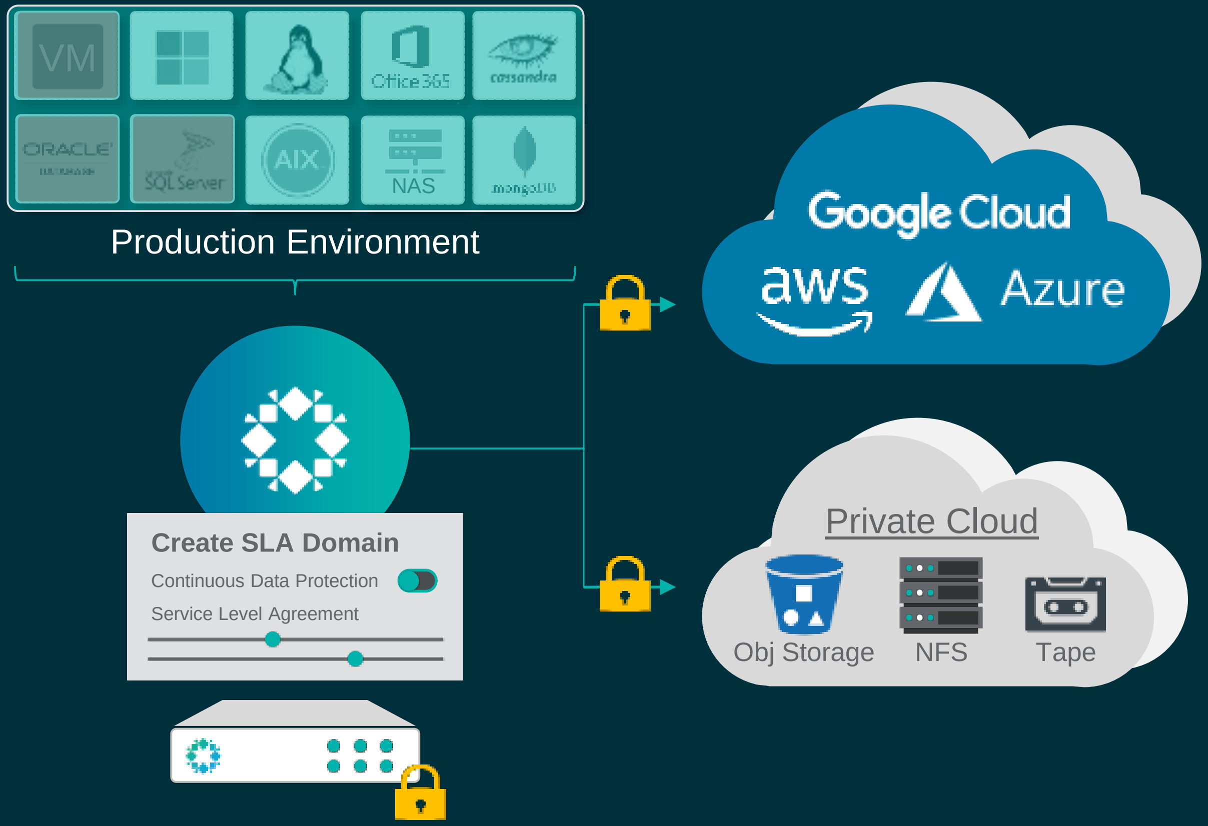
Security

Rubrik Cloud Data Management



A single software fabric for complete data management across data center and cloud

Meet Rubrik Cloud Data Management



Quick Start: Rack and go. Auto-discovery.

Automate: Intelligent SLA policy engine for effortless management.

Rapid Ingest: Parallel ingest accelerates snapshots and eliminates stun.

Instant RTOs/RPOs: Live Mount VMs, SQL & Oracle databases. Google-like search. Natively integrated CDP for VMware.

Secure: End-to-end encryption. Immutable file system.

Cloud: “CloudOut” instantly accessible with global search. “CloudOn” for cloud instantiation.

rubrik

WORKING TOGETHER GETTING PRIORITIES STRAIGHT

PREVENT ATTACK (BREACH) – PALO ALTO NETWORKS

DETECT ATTACK (BREACH) – PALO ALTO NETWORKS & RUBRIK

LAST LINE OF DEFENSE (RECOVER) - RUBRIK

RESURRECTION

“Recovery is not Defense in traditional thinking – It has more resemblance with Resurrection”

Depending on the level of breach, the success rates of backups, and the used technology, recovery can take seconds, hours, days or weeks. Even **Infinitely** long time – The problem is **RTO** and most likely also **RPO**. No one can wait for infinity”

RTO
Recovery Time Objektive.
The time it takes to complete a recovery.
Seconds, Hours, Days, Weeks or never.

RPO
Recovery Point Objektive.
The last Point in Time Backup available for recovery.
Seconds, Hours, Days or none.

BUT I HAVE BACKUPS, RIGHT?

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

OH NO.

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.

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

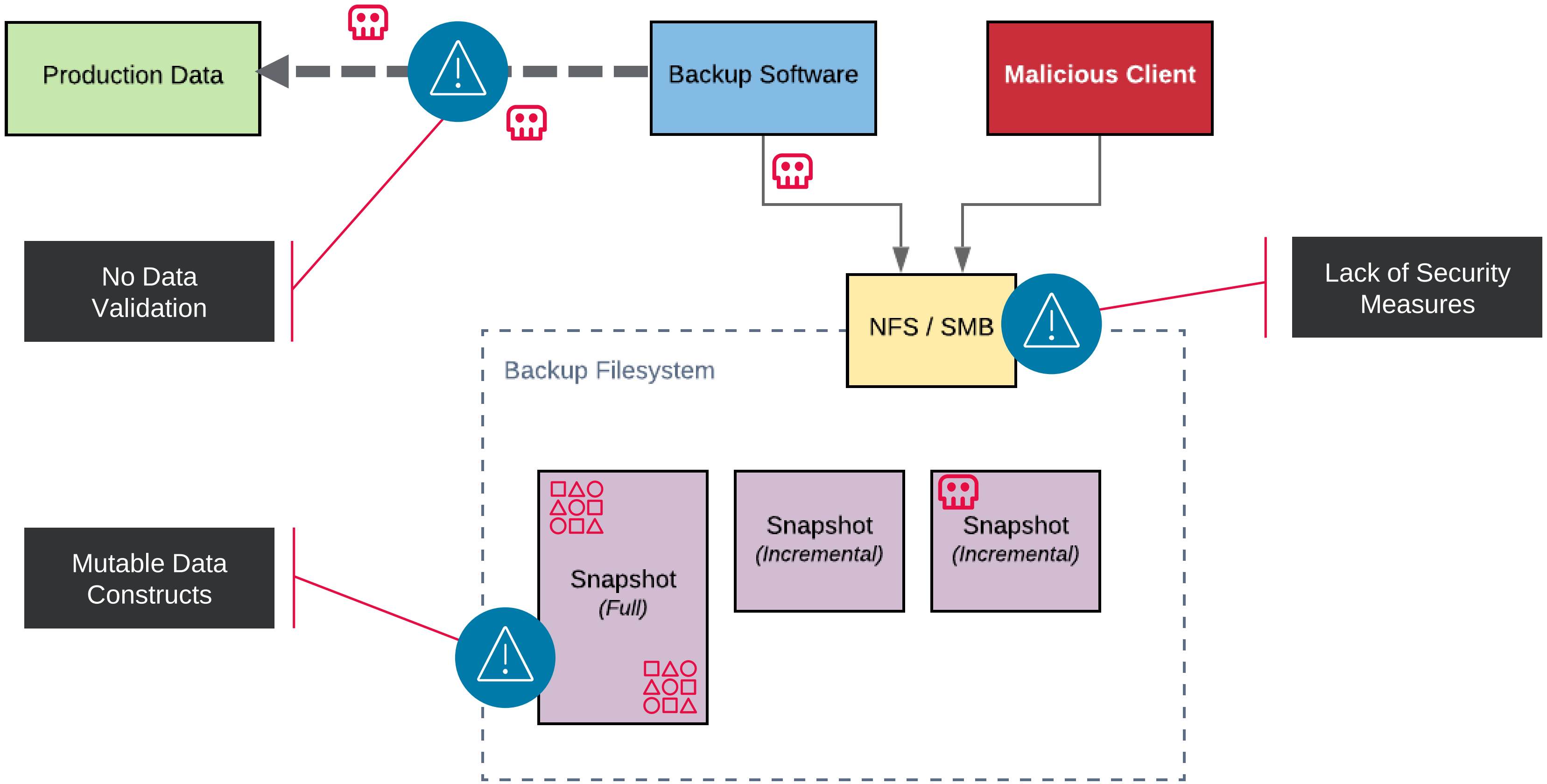
Require authentication to all endpoints that are used to operate the solution, including Role Based Access Control (RBAC) or Multi-tenancy features.

rubrik

DISTRIBUTED IMMUTABLE FILESYSTEM

rubrik

LEGACY - BACKUP ARCHITECTURES



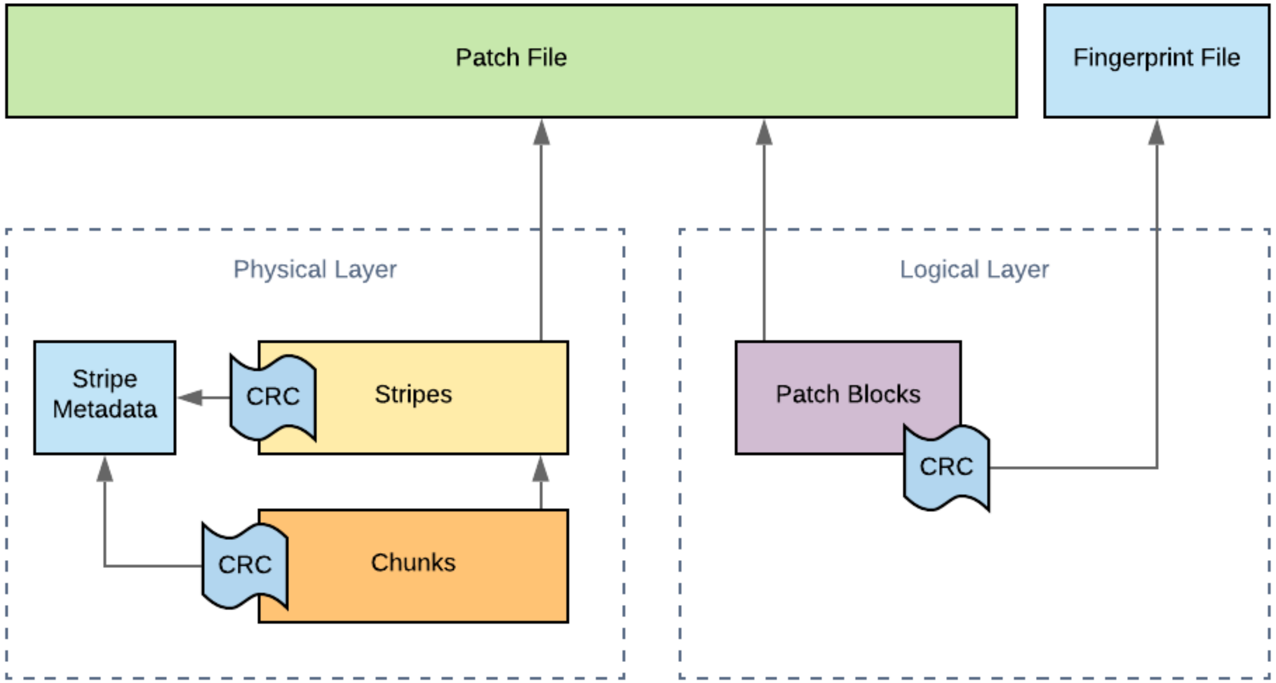
DISTRIBUTED IMMUTABLE FILESYSTEM

- Atlas, an **immutable** Filesystem in Userspace (FUSE)

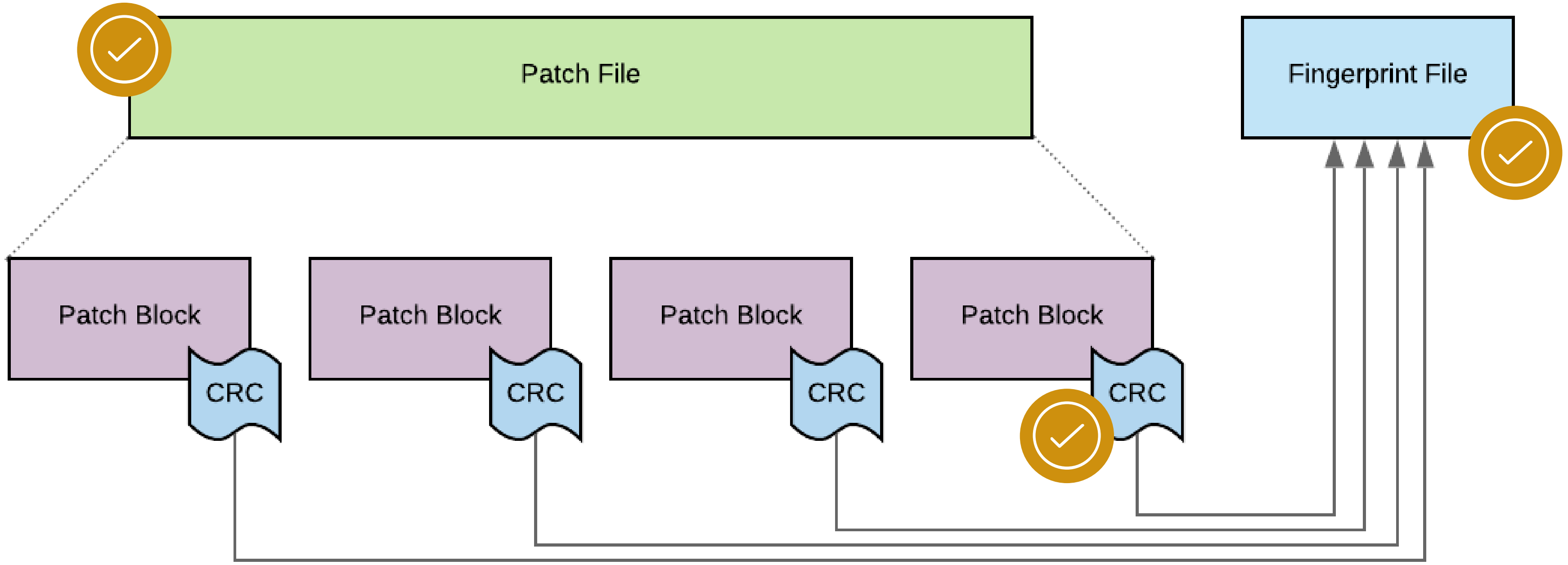
- Distributed and immutable filesystem for writing and reading data for other **Rubrik services**.

- 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.



CONSTRUCTING APPEND ONLY FILES (AOFs)



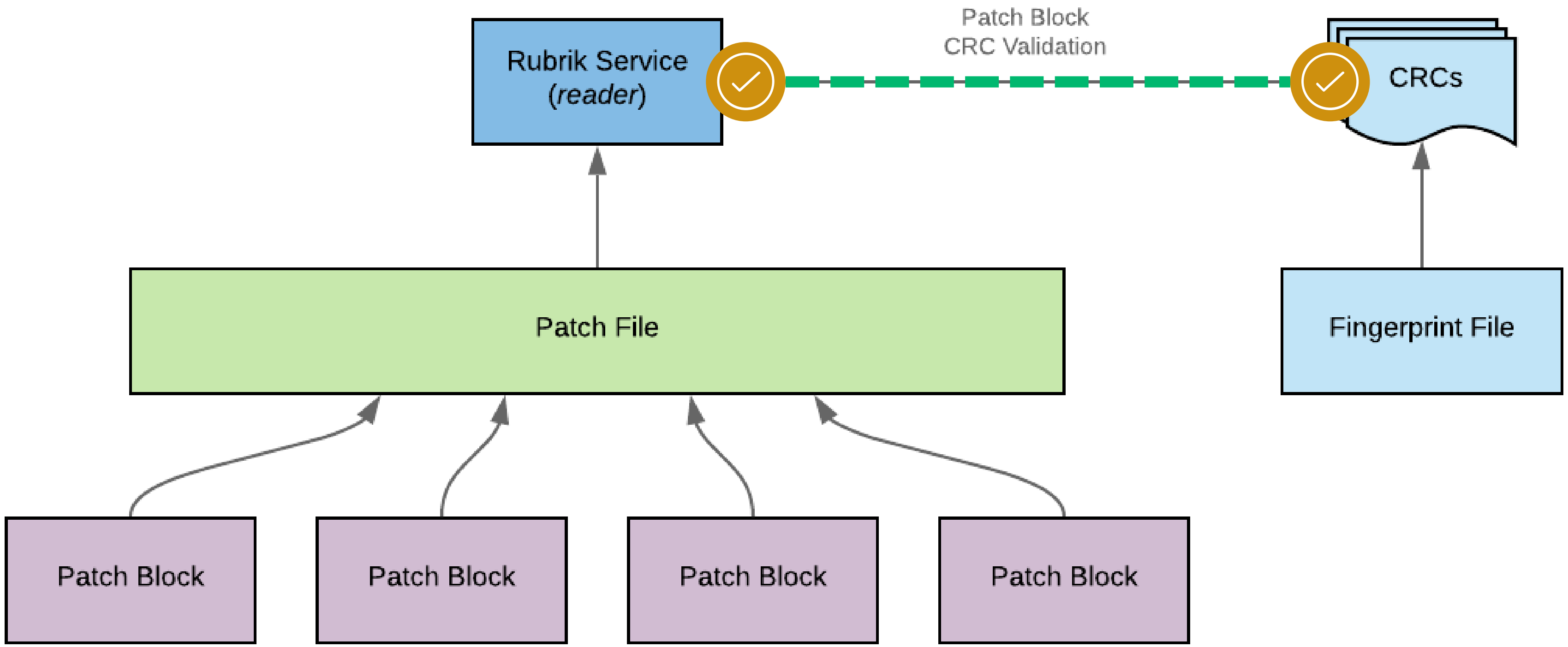
» Checksums (CRCs) are generated and written to a Fingerprint file.

» 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

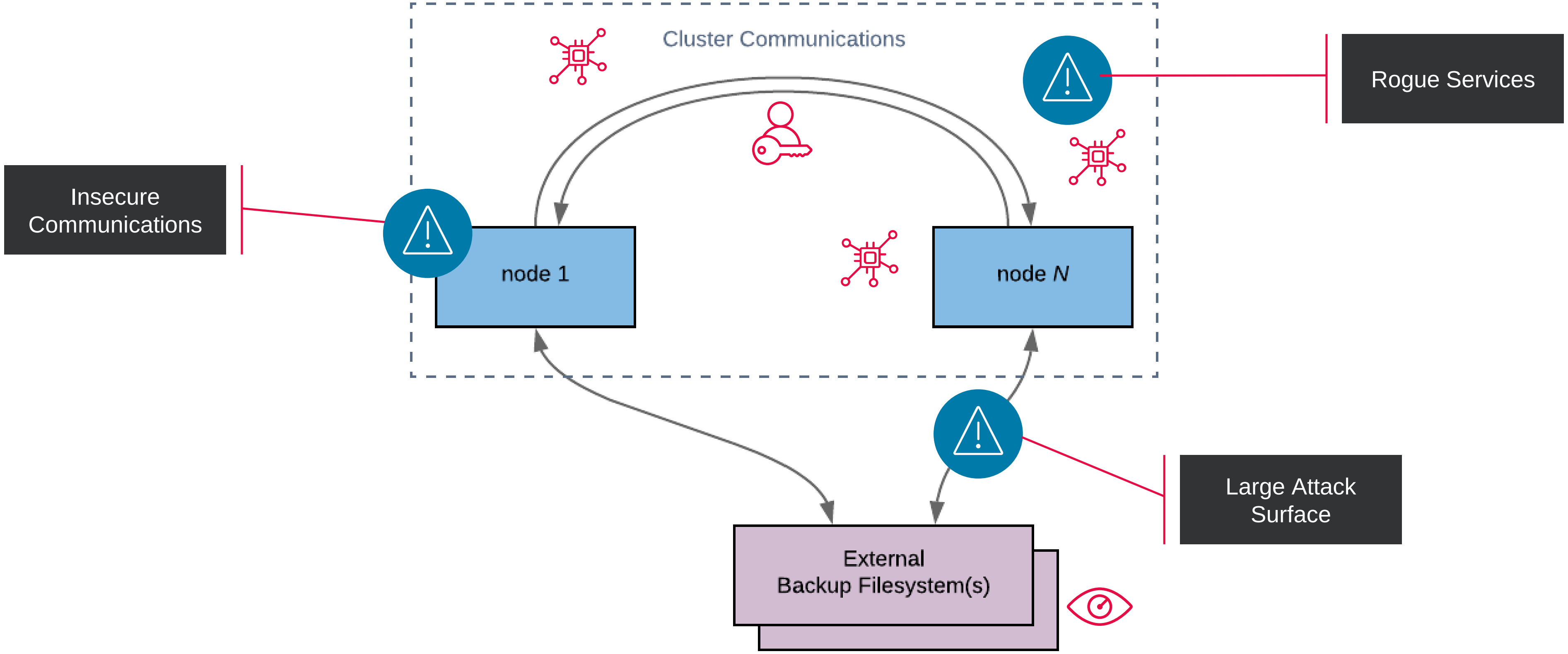
IN-LINE READ VALIDATION



ZERO TRUST CLUSTER DESIGN

rubrik

LEGACY “FULL TRUST” DESIGN



Rogue Services

Insecure Communications

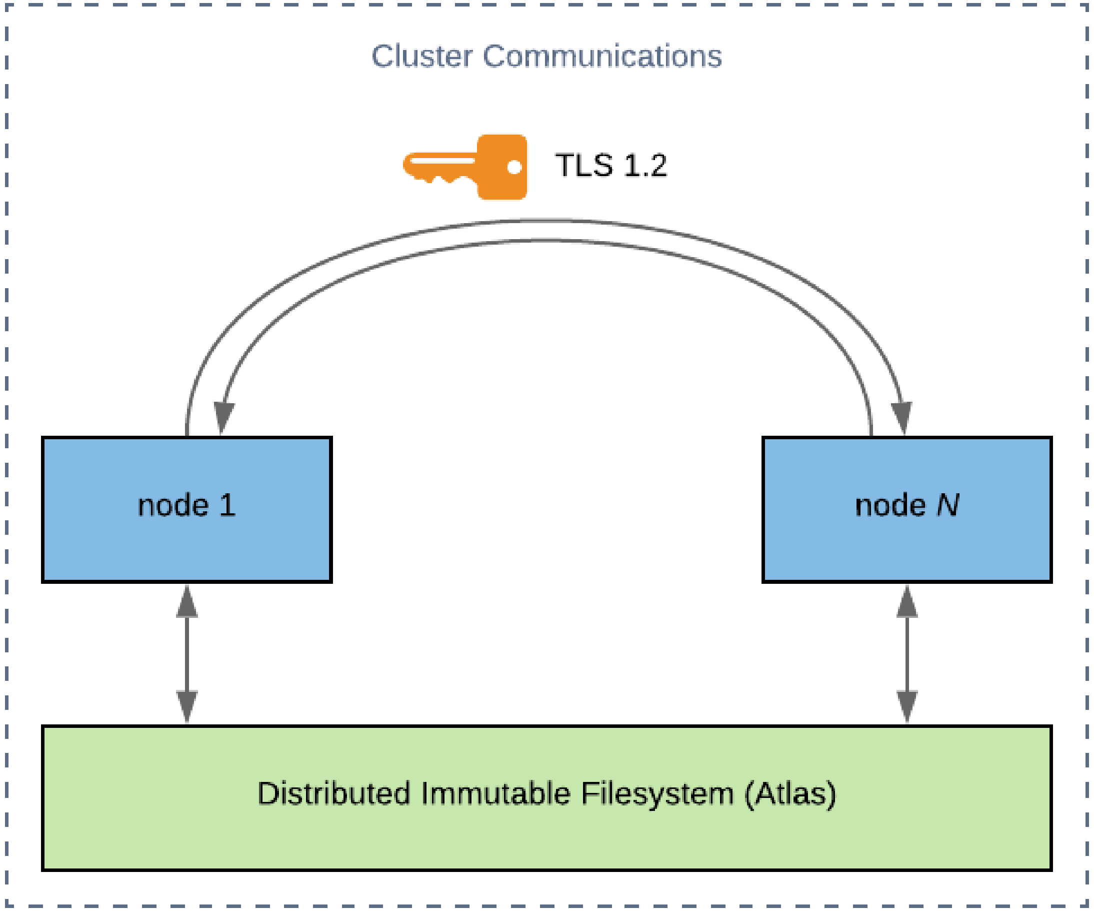
Large Attack Surface

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).

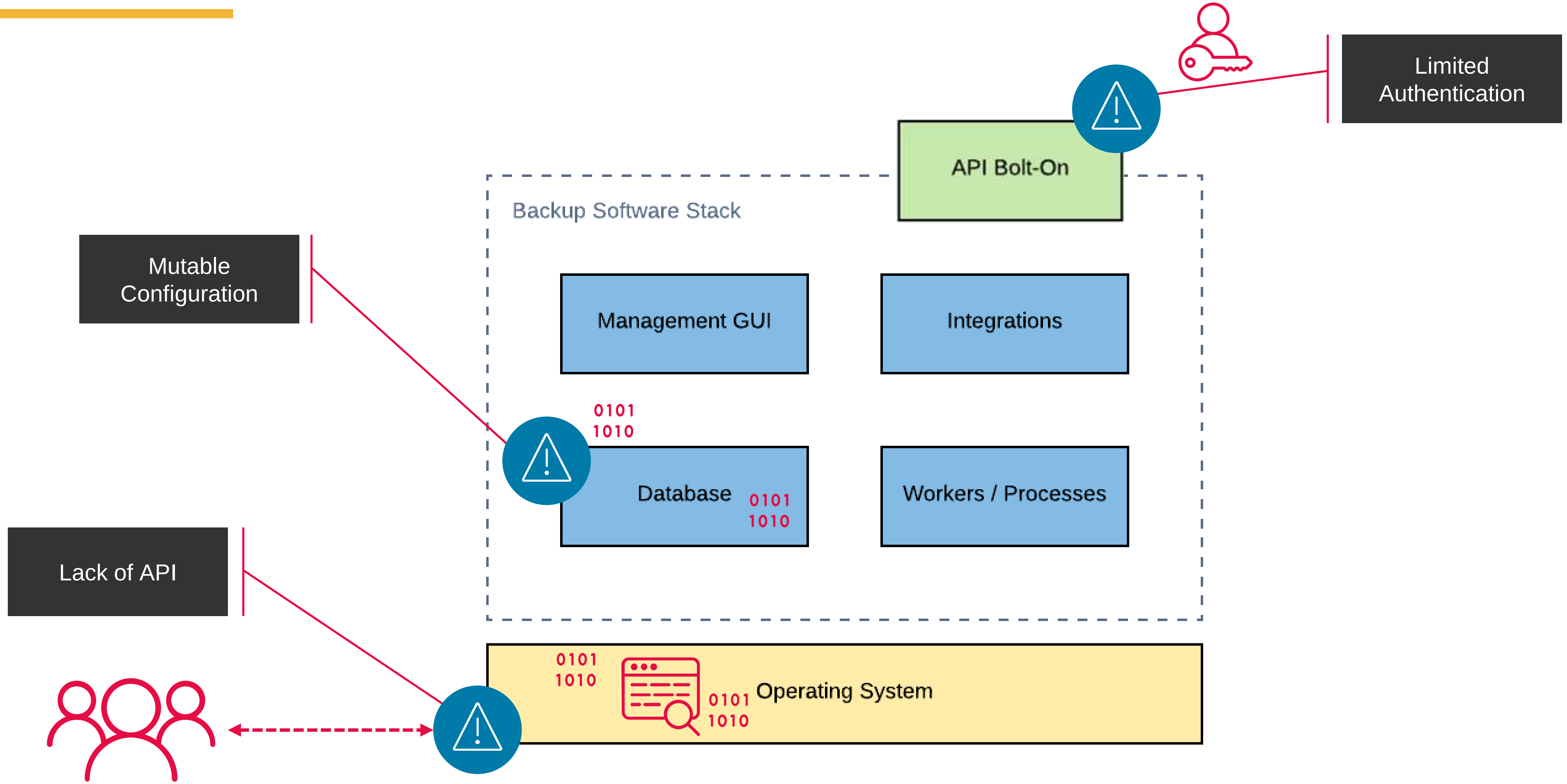


rubrik

AUTHENTICATED APIs AND TOOLS

rubrik

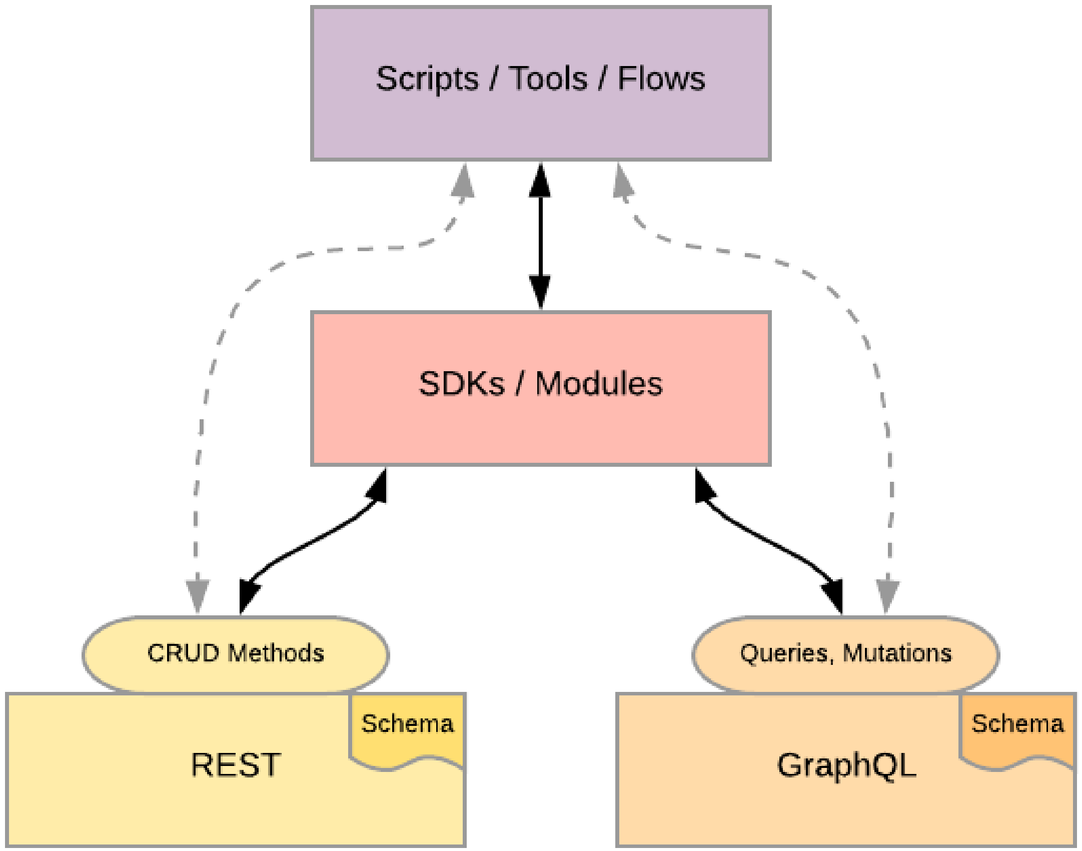
EXTENSIBILITY CONCERNS



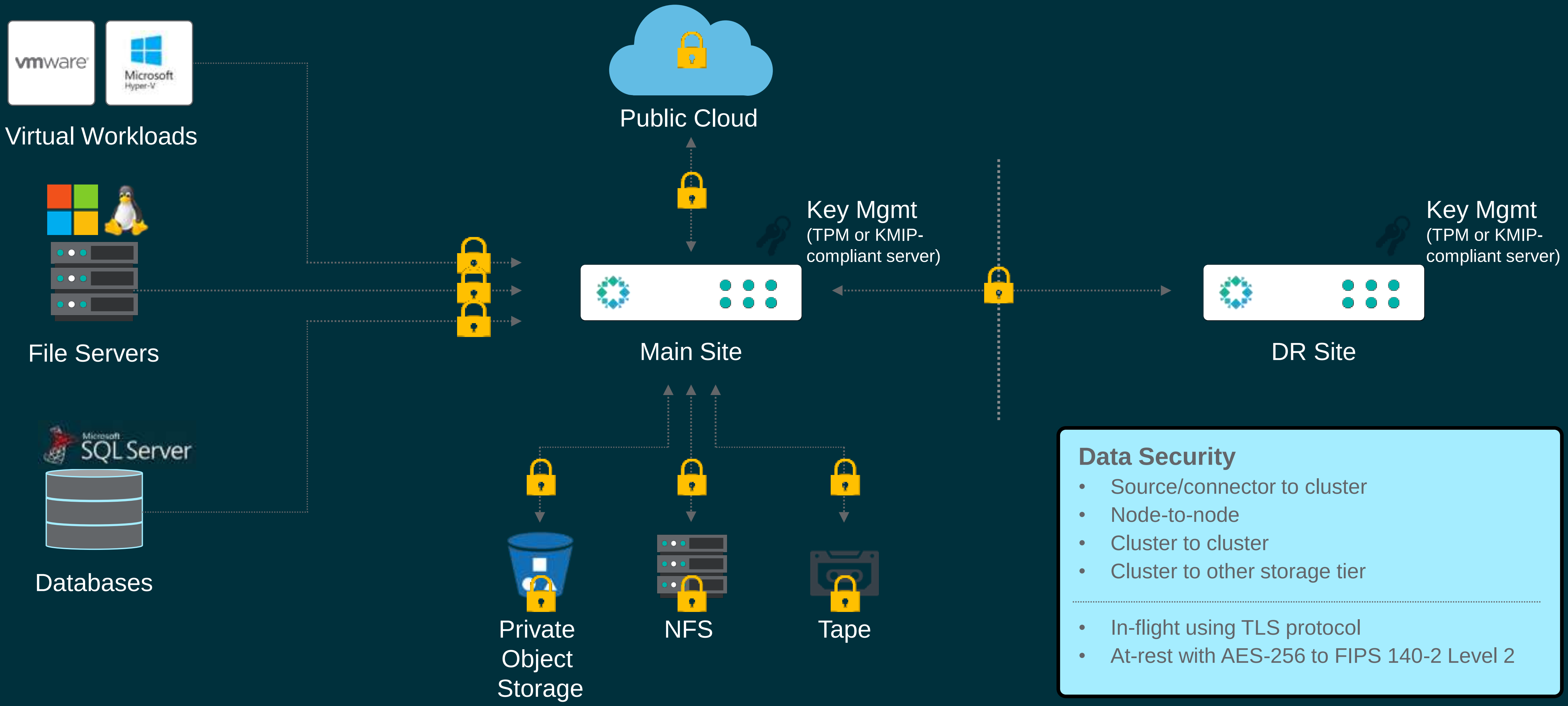
© 2020 Rubrik. All rights reserved.

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.



End-to-End Encryption



Data Security

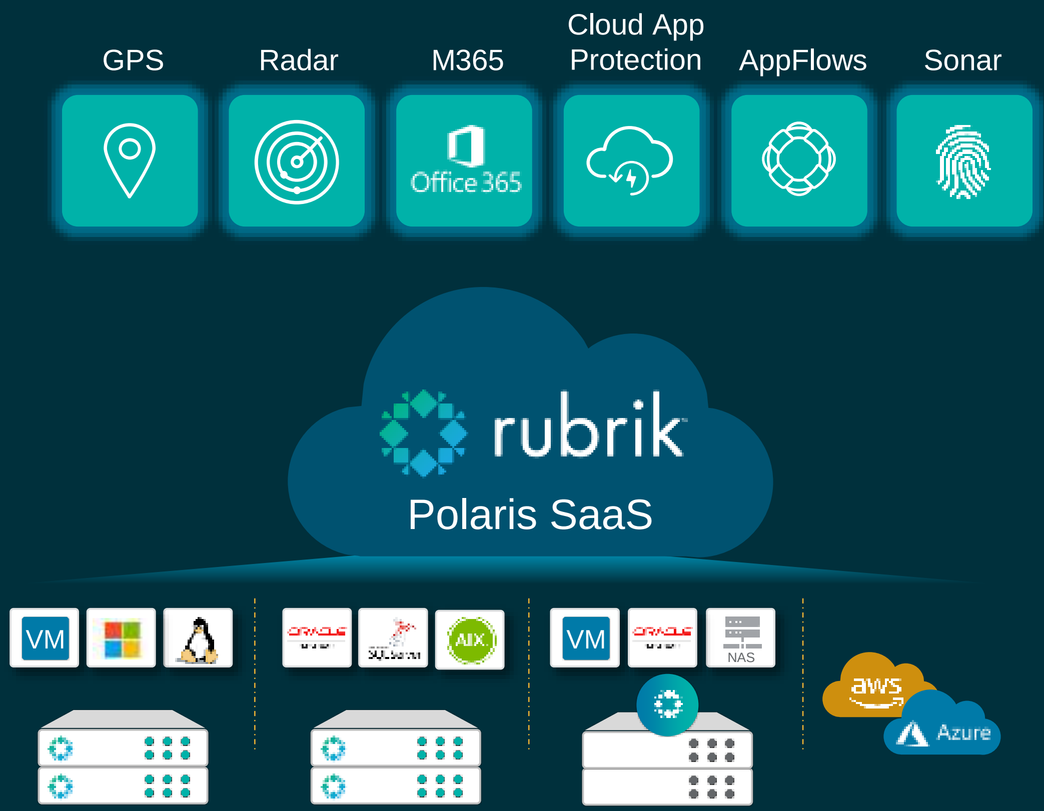
- Source/connector to cluster
- Node-to-node
- Cluster to cluster
- Cluster to other storage tier

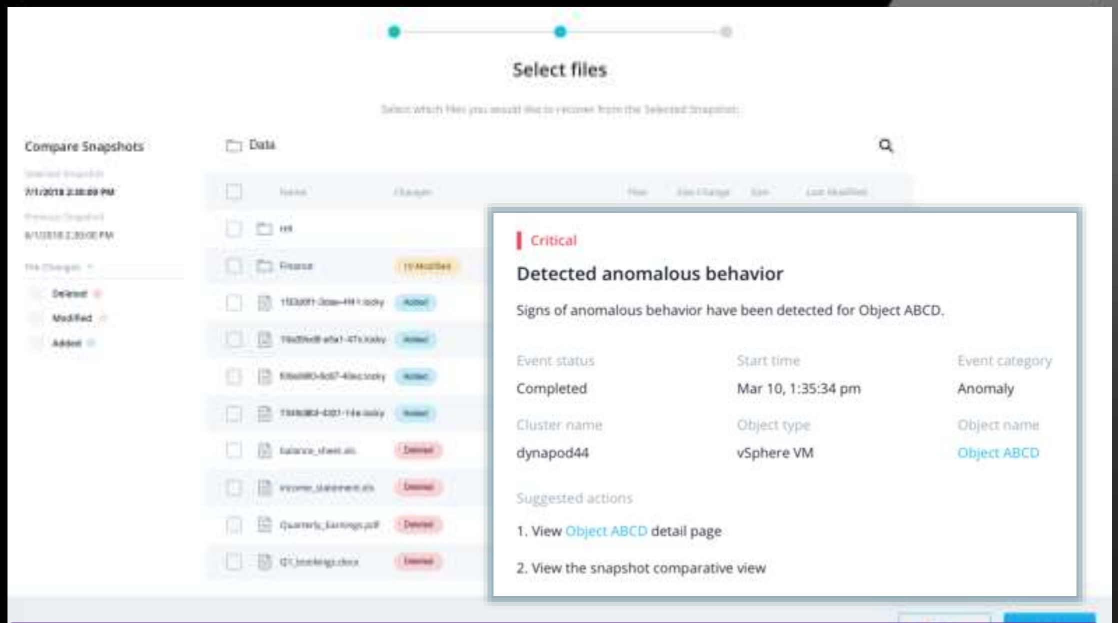
- In-flight using TLS protocol
- At-rest with AES-256 to FIPS 140-2 Level 2

GETTING PRIORITIES STRAIGHT PART II - IN CASE OF BREACH

DETECT ATTACK (BREACH)
ALERT
STOP ATTACK
RECOVER

Rubrik add-on security functions





Critical

Detected anomalous behavior

Signs of anomalous behavior have been detected for Object ABCD.

Event status	Start time	Event category
Completed	Mar 10, 1:35:34 pm	Anomaly
Cluster name	Object type	Object name
dynapod44	vSphere VM	Object ABCD

Suggested actions

1. View Object ABCD detail page
2. View the snapshot comparative view

Polaris Radar

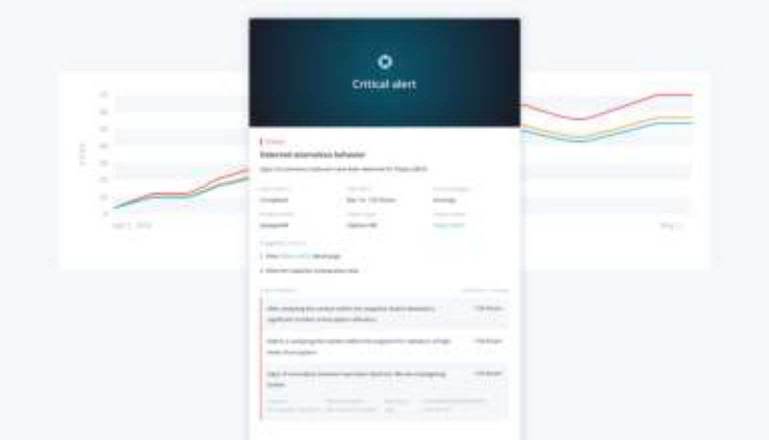
Automated Ransomware Detection & Remediation

Impact Assessment & 1-Click Recoveries

Our Approach: Recovery Accelerated and Simplified

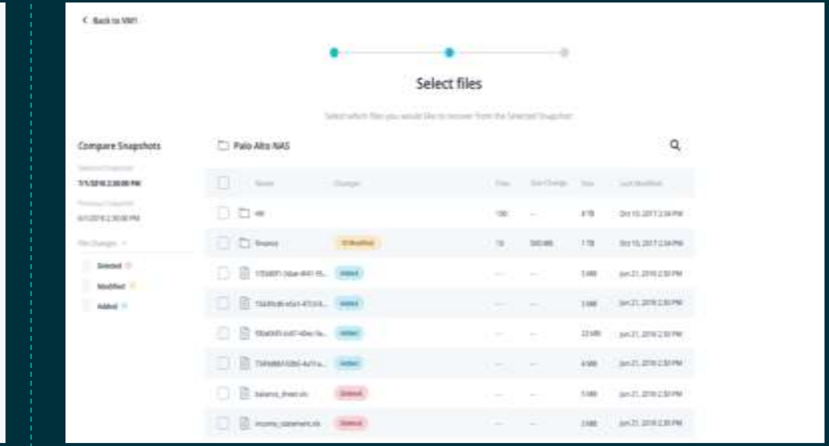
The Rubrik Difference

Identify Abnormal Behavior



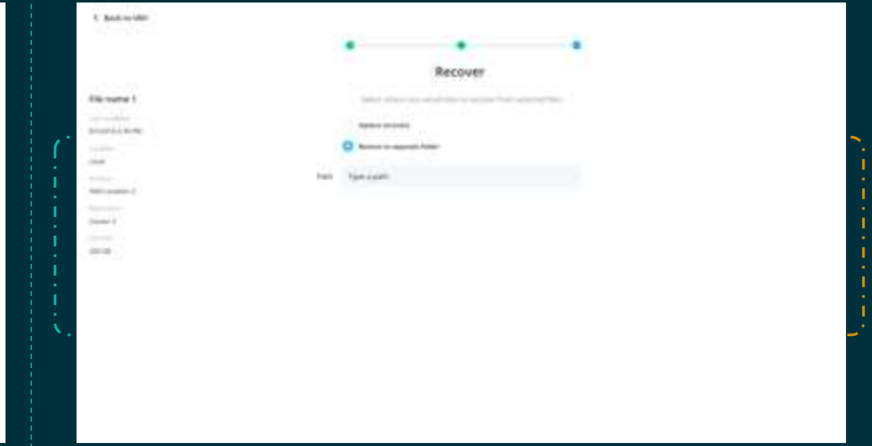
- ML-based anomaly detection on existing backup data for last line of defense
- Neural Network: 99.9% Accuracy
- API-first platform to plug into automation frameworks and PALO ALTO XSOAR

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

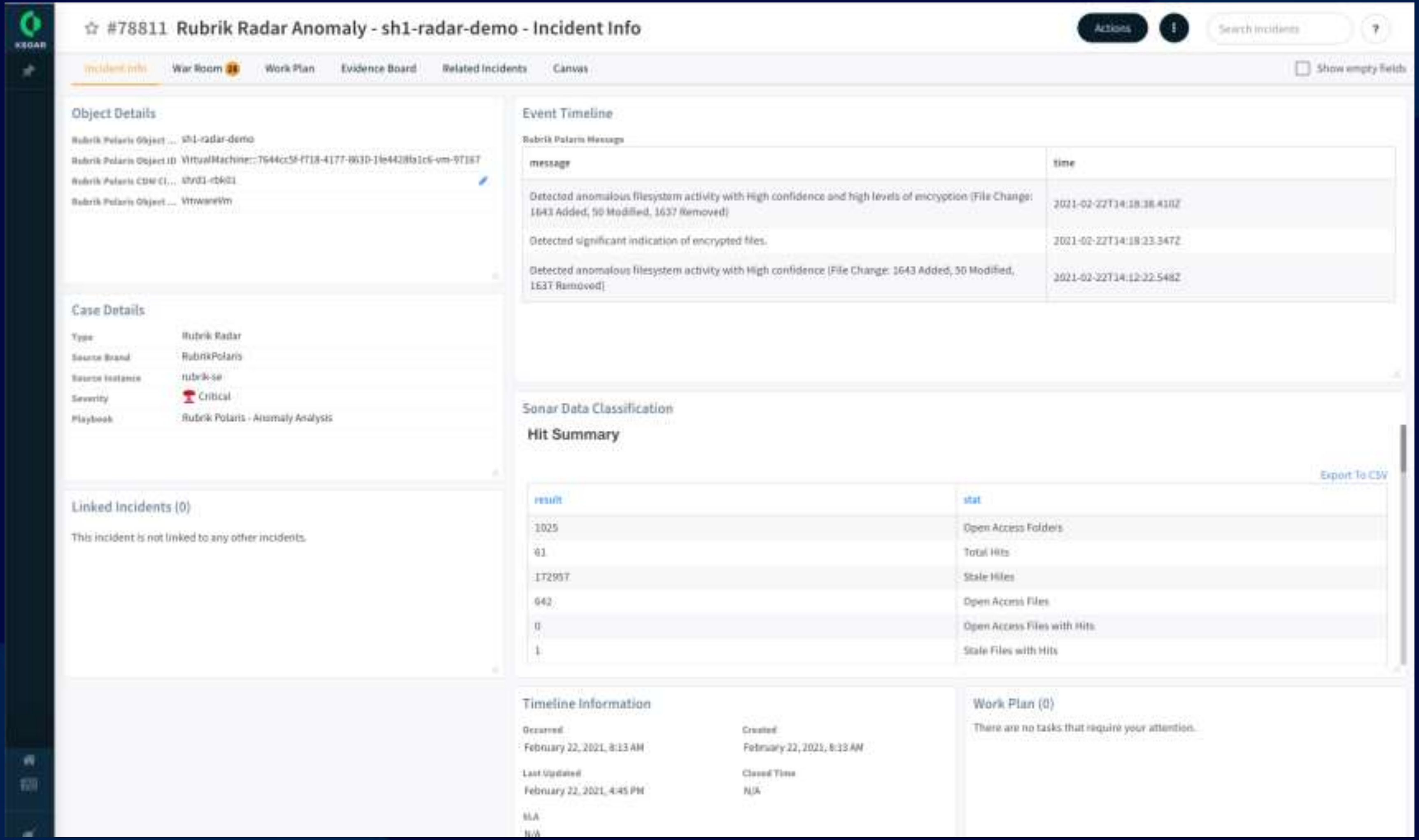


- Data is never available in read/write mode means it can't be overwritten
- 1-click recovery to most recent clean version (Restore/Live Mount/File-level)
- RTO down from Days to Minutes

rubrik

Working together

- Rubrik plugs in to Palo Alto XSOAR platform
- Reports on security anomalies



☆ #78811 Rubrik Radar Anomaly - sh1-radar-demo - Incident Info

Object Details

Rubrik Polaris Object ...	sh1-radar-demo
Rubrik Polaris Object ID	VirtualMachine:::7644cc5f-f718-4177-8630-14e4428fa1c6-vm-97167
Rubrik Polaris CDM Cl...	shrd1-rbk01
Rubrik Polaris Object ...	VmwareVm

Case Details

Type	Rubrik Radar
Source Brand	RubrikPolaris
Source Instance	rubrik-se
Severity	Critical
Playbook	Rubrik Polaris - Anomaly Analysis

Linked Incidents (0)

This incident is not linked to any other incidents.

Event Timeline

Rubrik Polaris Message

message	time
Detected anomalous filesystem activity with High confidence and high levels of encryption (File Change: 1643 Added, 50 Modified, 1637 Removed)	2021-02-22T14:18:38.410Z
Detected significant indication of encrypted files.	2021-02-22T14:18:23.347Z
Detected anomalous filesystem activity with High confidence (File Change: 1643 Added, 50 Modified, 1637 Removed)	2021-02-22T14:12:22.548Z

Sonar Data Classification

Hit Summary

result	stat
1025	Open Access Folders
61	Total Hits
172957	Stale Files
642	Open Access Files
0	Open Access Files with Hits
1	Stale Files with Hits

Timeline Information

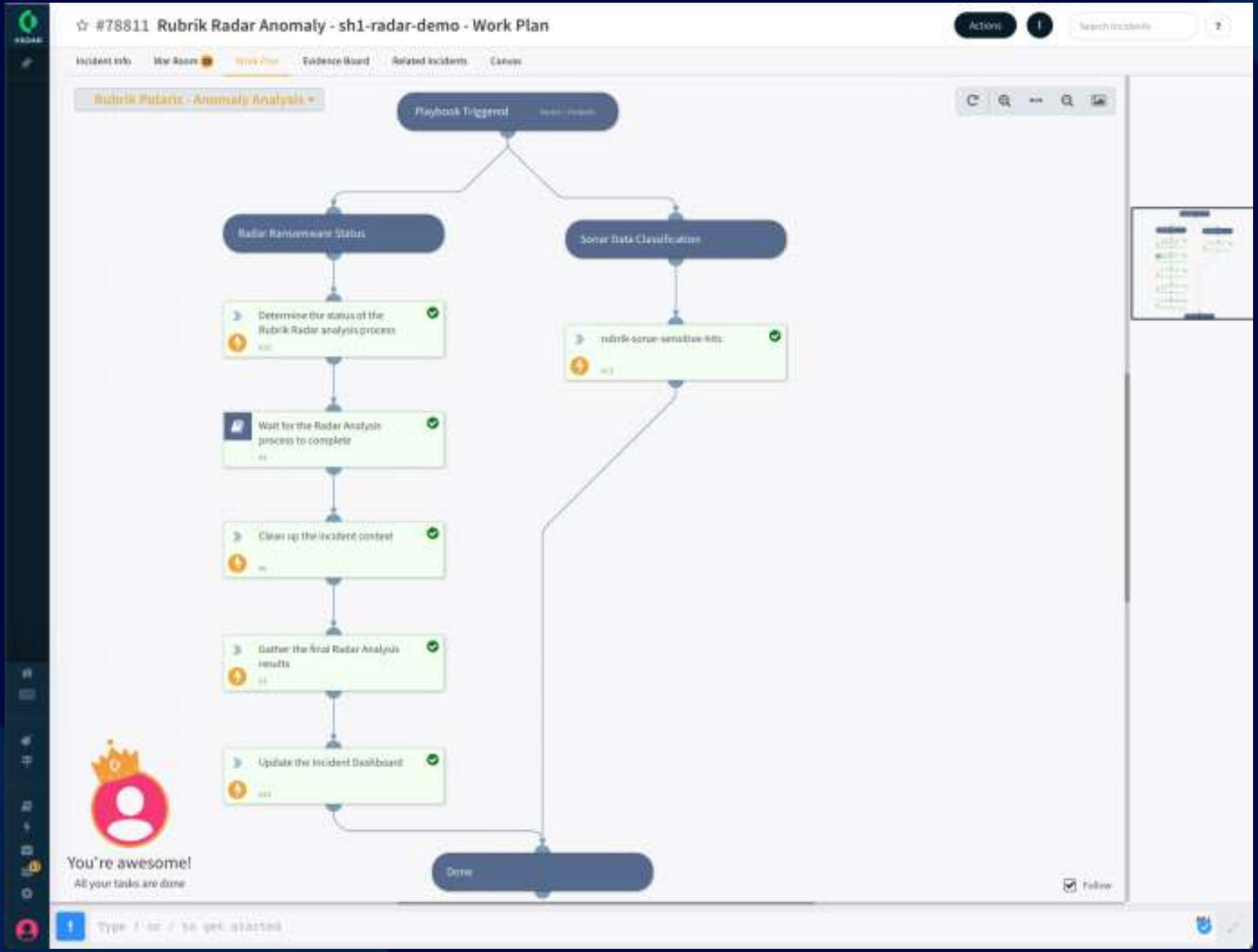
Occurred February 22, 2021, 8:13 AM	Created February 22, 2021, 8:13 AM
Last Updated February 22, 2021, 4:45 PM	Closed Time N/A
SLA N/A	

Work Plan (0)

There are no tasks that require your attention.

Plan of emergency

- Which steps should happen?
- Define workflow to help in disaster

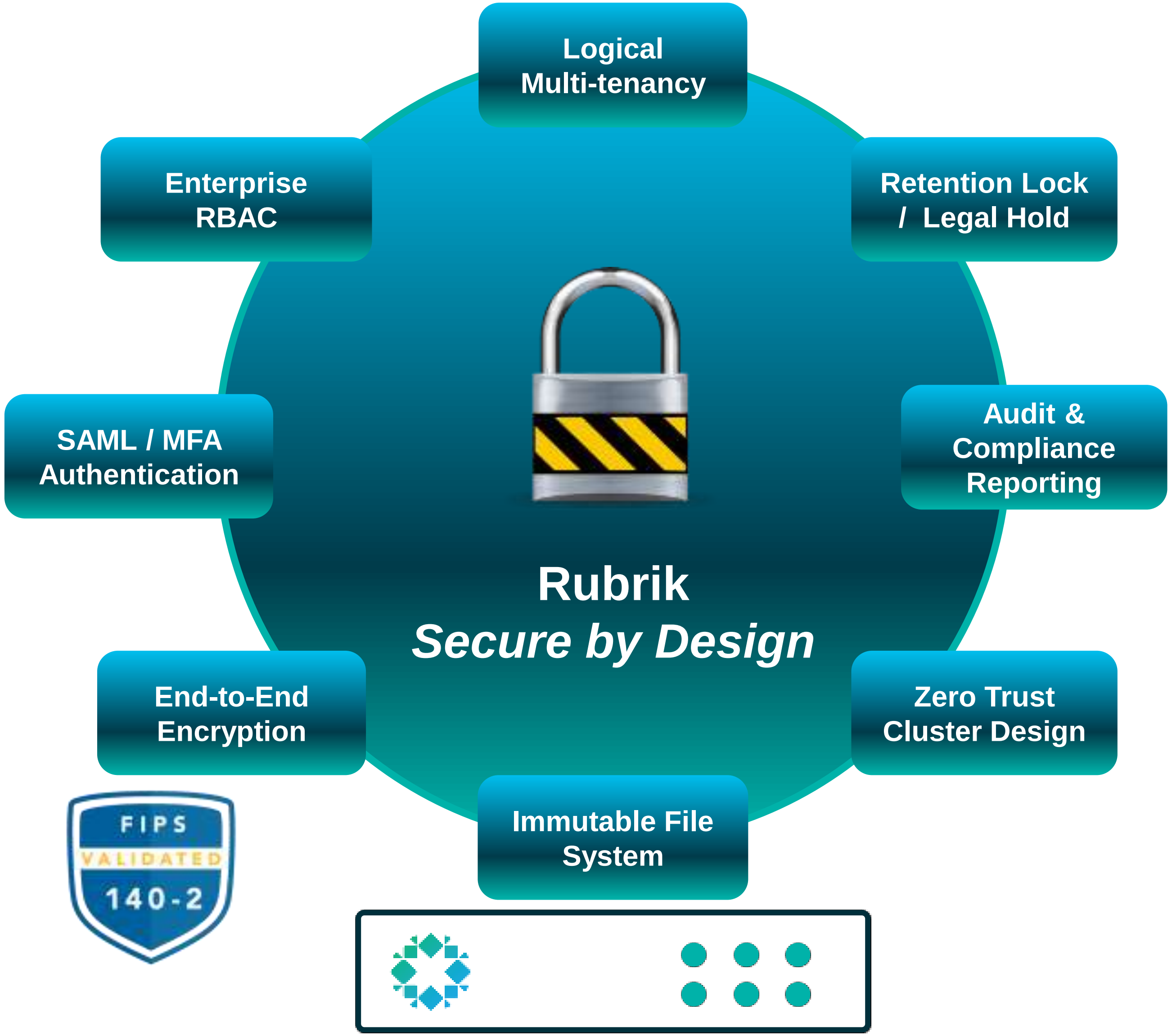


☆ #78811 Rubrik Radar Anomaly - sh1-radar-demo - Work Plan

Actions
Search Incidents
Incident Info
War Room
Work Plan
Evidence Board
Related Incidents
Canvas
Rubrik Polaris - Anomaly Analysis ▾
Playbook Triggered
Radar Ransomware Status
Sonar Data Classification
Determine the status of the Rubrik Radar analysis process
Wait for the Radar Analysis process to complete
Clean up the incident context
Gather the final Radar Analysis results
Update the Incident Dashboard
rubrik-sonar-sensitive-hits
Done
You're awesome!
All your tasks are done
Follow
Type ! or / to get started

> “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

The Rubrik Security Framework



Logical Multi-tenancy

Enterprise RBAC

Retention Lock / Legal Hold

SAML / MFA Authentication

Audit & Compliance Reporting

Rubrik
Secure by Design

End-to-End Encryption

Zero Trust Cluster Design

Immutable File System

SOC 2 TYPE 2

Information Security Management System 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.

Rubrik Security Hardening

Best Practices Guide

Updated regularly

rubrik

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

Don’t Backup. Go Forward.

rubrik