Threat Monitoring

Find Lurking Threats Early

Cyber threats often lurk undetected in environments, especially within critical infrastructure. An insufficient understanding of potential threats, reliance on reactive hunting, and over-taxed production systems are common challenges for IT and Security teams. These issues can contribute to longer dwell times, slower investigations, greater cyber incident impact, and increased risk of reinfection.

Rubrik's comprehensive data backup capabilities provide unique visibility into your organization's data landscape, enabling proactive detection of potential threats within those backups. Teams can perform in-depth threat analyses offline – without requiring agents to be deployed on critical infrastructure – to better protect their organizations against these lurking threats.

Rubrik Threat Monitoring combines intelligence from third party threat feeds with proprietary intelligence from Rubrik Zero Labs (Rubrik's data threat intelligence unit) and Rubrik's InfoSec team to automatically identify indicators of compromise (IOCs) within backup snapshots. Threat Monitoring proactively scans for threats out-of-band from production infrastructure based on vetted threat intelligence, accelerating investigation and reducing the risk of reinfection.

DETECT THREATS EARLY

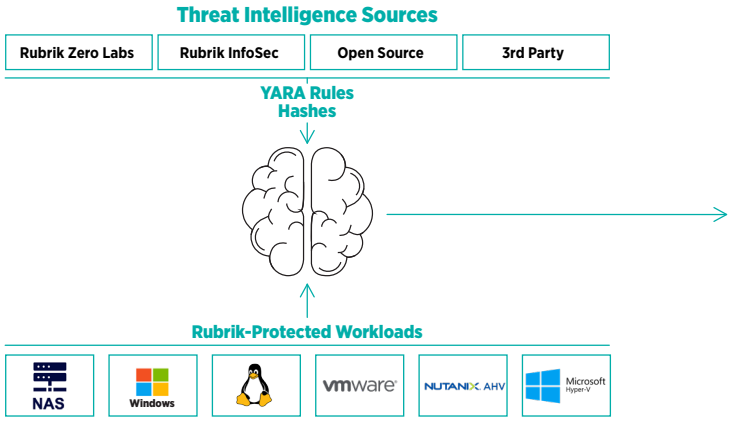
Minimize cyber incident impact by detecting previously unknown threats in your environment using Rubrik's proprietary threat intelligence feed

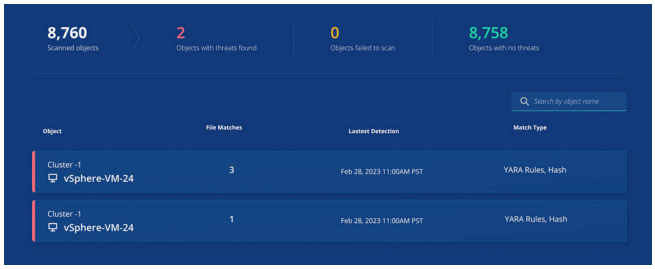
MONITOR FOR THREATS AUTOMATICALLY

Eliminate manual, reactive workflows by scanning for threats proactively

MINIMIZE IMPACT TO PRODUCTION

Preserve production system performance by monitoring existing backup data out-of-band





Rubrik Threat Monitoring Dashboard

HOW THREAT MONITORING WORKS

1. Automatically ingest vetted threat intelligence from Rubrik Zero Labs, Rubrik's InfoSec team, and third party sources.
2. Automatically hunt for indicators of compromise within backups – using file hashes and YARA rules – when new intelligence is available.
3. Generate accurate, real-time alerts for IOC matches from scans.
4. Provide infection insights from IOC scans (e.g., threat type, first matched snapshot, hashes) for deeper cyber investigations.

From here, you can conduct further threat hunts with Threat Hunting or quarantine infected data with Threat Containment.

HOW WE ARE DIFFERENT

1. Comprehensive threat intelligence from both proprietary and third party sources
2. Proactive and automated threat monitoring ("set it and forget it")
3. No learning curve: intuitive UI and fast, easy onboarding

20230615_v1