From Reactive to Proactive: Harnessing the Power of Threat Monitoring

Rubrik Security Cloud provides automated scanning of your backups by utilizing an up-to-date Rubrik Threat Intelligence feed to detect lurking threats early.

CHALLENGE

Cyber threats are a growing concern for organizations of all sizes. Data breaches, malware infections, and ransomware attacks can significantly disrupt operations, leading to financial losses, damage to reputation, and legal consequences. 99% of IT and security leaders surveyed were made aware of at least one attack in 2022. On average, leaders dealt with attacks 52 times in 2022. According to the Incident Response team at Palo Alto Networks' Unit 42, the highest ransom demand in 2022 amounted to $50 million USD. Therefore, it is crucial to actively monitor your environment to identify malicious activity and detect threats before they inflict substantial harm on your organization.

Conducting thorough and frequent threat hunting is vital to enhancing your security strategy. This process entails identifying ongoing attacks, assessing potential vulnerabilities, and evaluating the likelihood and consequences of a breach. By comprehending your organization's risk profile, you can effectively prioritize security investments and allocate resources where they are most needed.

SOLUTION

Rubrik offers data security solutions for a diverse set of data sources, presenting an advantageous opportunity for identifying malicious activity and files. Consequently, security teams can conduct a thorough threat analysis without needing agents or deploying potentially disruptive measures on production infrastructure assets. By analyzing backups separately from the production infrastructure, the impact on ongoing operations is negligible. Simultaneously, security teams gain valuable insights into the organization's vital infrastructure components without the complexity and agent-based dependencies of traditional infrastructure monitoring.

Rubrik Threat Monitoring delivers a proactive cybersecurity approach that empowers you to swiftly identify and respond to potential threats—helping mitigate the time threats go undetected. This approach helps reduce the threat dwell time and, in turn, decreases the likelihood of severe damage. Rubrik Threat Monitoring uses a curated threat intelligence feed that includes YARA rules and file hashes to search for IOCs—all of which Rubrik maintains as part of the service. From here, Threat Monitoring performs automated scans on the stored backup data and notifies you when a match is identified.

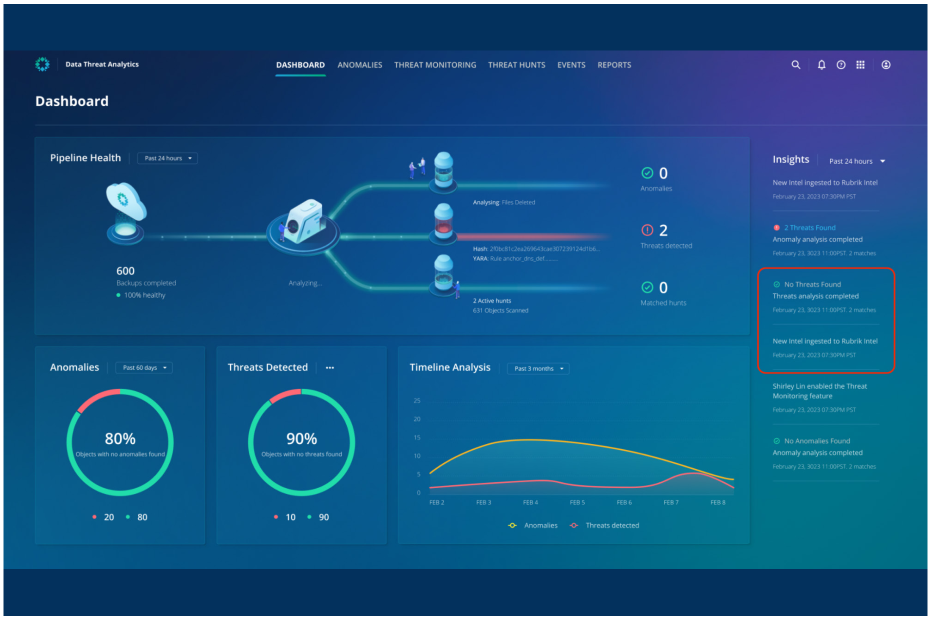
CUSTOMER BENEFITS

Earlier detection of new threats

Threat Monitoring utilizes an up-to-date threat intelligence feed which is vetted by Rubrik's team of experts. The intelligence from this feed includes the latest threat information from the Rubrik Information Security team, Rubrik Zero Labs, and various 3rd party sources. To decrease the chances of potential false positive findings, Rubrik utilizes high-quality intelligence feeds, enabling more effective and efficient threat detection and response.

Automated monitoring for threats

Threat Monitoring is specifically designed to automate malware detection, enabling a proactive and accelerated incident response. By identifying issues promptly, you can swiftly initiate root cause analysis and begin the remediation process, effectively reducing the mean time to resolution (MTTR). This solution provides security teams with vital visibility into the most crucial components of their infrastructure, even in situations where monitoring capabilities may be limited or challenging. Additionally, automated alerts can be sent to the relevant IT teams, SIEM/SOAR solutions, or existing log management systems, enabling them to address any pressing security concerns and take immediate action promptly.



New Intel ingested to Rubrik Intel
February 23, 2023 07:30PM PST

2 Threats Found
Anomaly analysis completed
February 23, 3023 11:00PST. 2 matches

No Threats Found
Threats analysis completed
February 23, 3023 11:00PST. 2 matches

New Intel ingested to Rubrik Intel
February 23, 2023 07:30PM PST

Shirley Lin enabled the Threat Monitoring feature
February 23, 2023 07:30PM PST

No Anomalies Found
Anomaly analysis completed
February 23, 3023 11:00PST. 2 matches

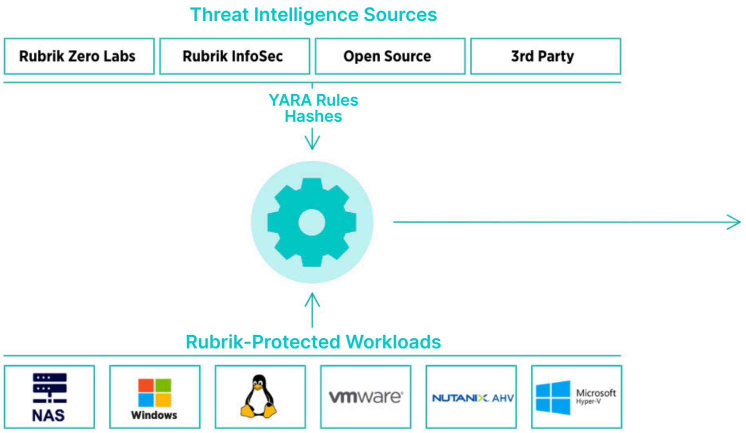
Data Threat Analytics Dashboard

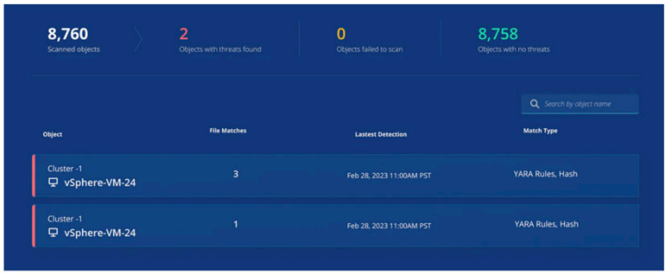
Minimize effect on production system performance

With Rubrik, security teams can perform comprehensive threat analyses on the backup infrastructure, which is out-of-band from production infrastructure, without requiring additional agents or compute resources. This out-of-band approach ensures that even if attackers are present within your production environment, they remain unaware of any ongoing threat investigations being conducted. By doing this, the attackers can avoid raising any alarms and escalating the attack or choosing to initiate data deletion immediately.

HOW IT WORKS

Threat Monitoring is a comprehensive turnkey solution available in Rubrik Security Cloud. You can easily enable Threat Monitoring for your organization by leveraging the Data Threat Analytics room.





8,760	2	0	8,758
Scanned objects	Objects with threats found	Objects failed to scan	Objects with no threats

Object	File Matches	Lastest Detection	Match Type
Cluster -1 vSphere-VM-24	3	Feb 28, 2023 11:00AM PST	YARA Rules, Hash
Cluster -1 vSphere-VM-24	1	Feb 28, 2023 11:00AM PST	YARA Rules, Hash

Rubrik Threat Monitoring Dashboard

1. Once enabled, Threat Monitoring is connected to the Rubrik Threat Intelligence Feed, which incorporates intelligence from various trusted sources. This includes Rubrik's own Zero Labs threat research team, Rubrik's Infosec team, and selected third-party providers. This feed delivers up-to-date threat intelligence in the form of prevalent YARA rules and Hashes for automated hunting of your backups to detect Indicators of Compromise (IOCs).

2. After thorough vetting, Rubrik evaluates newly discovered zero-day Indicators of Compromise (IOCs) and incorporates them into its Threat Intelligence feed. By automatically updating the feed with these validated IOCs, Rubrik ensures your environment remains safeguarded against the most recent threats.

3. Threat Monitoring periodically scans for IOCs, and where matches are identified, the specific file and location are promptly displayed on the dashboard. From there, you can drill down to view the matched Hash/YARA rule and access associated attributes for more background information. This assists in potential follow-up actions, such as initiating additional threat hunts through Rubrik's Threat Hunting product or using third-party tools like SIEMs or EDR solutions.

4. By leveraging Rubrik Threat Containment, you can immediately quarantine infected files or the entire snapshot, effectively mitigating the associated risk. By isolating the infected snapshots, Rubrik Threat Containment minimizes the likelihood of reintroducing the malware into the environment during recovery operations. These quarantined files or snapshots can be retained for post-incident reviews. To understand the root cause, point of origin, and other pertinent details, you can utilize Rubrik Cyber Recovery in an isolated environment to recover the quarantined snapshot, to gain insights into the root cause, point of origin, and other relevant details, Rubrik Cyber Recovery allows you to recover the quarantined snapshot within a secure, isolated environment. This enables you to thoroughly investigate and analyze the snapshot while maintaining the integrity of your production environment.

Once the initial setup is complete, Threat Monitoring will perform day-to-day operations without needing manual intervention. This ensures ongoing protection and detection of potential threats without needing constant manual oversight. With Threat Monitoring, you can confidently secure your environment while focusing on other critical aspects of your organization's security strategy.

SUMMARY

Maintaining a proactive cybersecurity approach is paramount in today's threat landscape. Rubrik Threat Monitoring provides an innovative solution enabling you to detect and respond to threats swiftly. By leveraging automated and proactive threat hunts, you can stay ahead of the evolving threat landscape, reduce your risk exposure, and mitigate the potential impact of security incidents. By leveraging Rubrik's up-to-date and validated threat intelligence feeds, you can leverage proactive threat hunts without investing time in personal vetting. This approach allows you to tap into Rubrik's expertise rather than getting entangled in the vetting process. Rubrik Threat Monitoring provides the proactive approach you need to ensure you can avoid costly disruptions and reputational damages to your organization.

For more information, please visit https://www.rubrik.com/threat-monitoring

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com