Rubrik Security Cloud for Cisco XDR

By bringing Rubrik Security Cloud data context directly into Cisco XDR, enterprises can streamline data protection and security, reduce complexity, and enhance their overall IT security posture. This unified approach simplifies the management of data and security across the entire IT landscape, making it easier than ever to protect critical data assets, and delivering cyber resilience in the face of attacks.

CHALLENGE

In today's digital era, data stands as the most prized resource for any business. It's the key target for attackers who understand its immense value when compromised or stolen. Cybercriminals are more advanced and quicker than ever, exploiting vulnerabilities to access and either destroy, steal, or extort crucial data.

With the growing amount of data and rising costs of breaches, companies are finding it challenging to manage and secure their information. They often lack visibility into their sensitive data—uncertain of its location and who can access it—making protection efforts more difficult. The sheer volume of alerts and the complexity of disjointed security tools further complicate the ability to prioritize and respond effectively to critical data threats.

SOLUTION

Cisco XDR enhances security operations by integrating and correlating data from various security products, such as network, endpoint, and cloud. It provides a unified view of threats, enabling faster and more effective detection, investigation, and response. Cisco XDR uses AI-driven automation to prioritize threats based on risk, streamline workflows, and improve overall security posture by providing comprehensive visibility across the IT environment. This reduces complexity and helps security teams respond to incidents more efficiently.

The integration between Rubrik and Cisco XDR bridges a crucial gap in modern cybersecurity by combining data intelligence with advanced threat detection. By integrating Rubrik's detailed data protection insights with Cisco XDR's unified threat detection capabilities, InfoSec teams gain comprehensive visibility into potential threats, allowing for faster threat identification and response, effectively reducing risks and minimizing potential damage to critical data.

When an attack happens, every second counts. To respond quickly, security teams need immediate access to comprehensive context without navigating through multiple systems. By integrating Rubrik's data insights with Cisco XDR's threat detection capabilities, security teams gain all the necessary context in one place. This enables them to respond to threats with greater accuracy and speed, ensuring the protection of their most critical data assets more effectively.

RUBRIK AND CISCO XDR

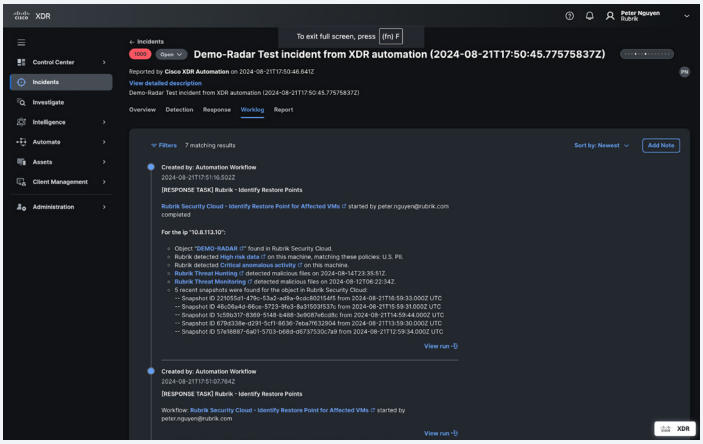
Rubrik Security Cloud integrates data risk insights into Cisco XDR, while also enabling security teams to take direct action to ensure an uncompromised backup is always available. This enables Security and IT Operations teams to enhance their incident response, accelerate threat investigations, and minimize business downtime.

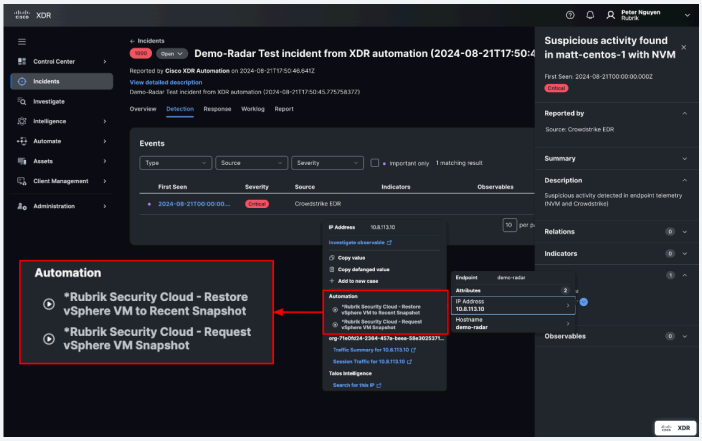
Prioritize threats with data context:
Rubrik enhances Cisco XDR by adding data context to security incidents, allowing security personnel to quickly assess risk levels based on the presence of sensitive data, malicious files, or anomalous activity. With data and threat context combined in a single view within Cisco XDR, security teams can correlate information more efficiently, eliminating the need to switch between different systems. Specific insights Rubrik provides within Cisco XDR include:

- **Sensitive data identification –** Identification of high risk data on a device associated with a security incident.
- **Anomaly Detection –** Rubrik uses a two-stage machine learning algorithm to detect file entropy and signs of encryption or malware. This provides visibility into the blast radius of an encryption attack.
- **Threat Hunting –** Rubrik uses malware-specific YARA rules to investigate a time-series history of data, pinpoint the initial infection, and identify both clean and infected snapshots to aid in recovery efforts.
- **Threat Monitoring –** Rubrik automatically identifies indicators of compromise within backups using its threat intelligence feed.

Rapidly identify safe restore points:
Within Cisco XDR, security analysts can easily review the latest Rubrik backup snapshots monitored for threats, to quickly identify the last safe backup. This allows the recovery process to start immediately, minimizing downtime and ensuring data integrity.

Backup and Restore:
Within Cisco XDR, security analysts can initiate a new backup, minimizing data loss in the event of a successful attack. The latest backup snapshot can also be restored directly from within Cisco XDR.





SUMMARY

By unifying data and threat contexts within Cisco XDR, Rubrik empowers security analysts to correlate information faster, prioritize alerts more effectively, and minimize the impact of attacks. This integrated approach ensures that organizations can quickly identify compromised data, maintain data integrity by verifying threat-free backups, and expedite recovery by identifying the last safe backup snapshot. Additionally, the ability to initiate restores directly from Cisco XDR simplifies the recovery process, allowing organizations to swiftly restore critical data and reduce downtime.

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

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

ds-rsc-for-cisco-xdr / 20240827