NEWS RELEASE

Rubrik Threat Hunting Now Available on Rubrik Security Cloud - Government

4/10/2024

- Rubrik Threat Hunting is designed to accelerate safe recovery by determining the initial point, scope, and time of infection
- Rubrik Security Cloud - Government enhancements now include protection of new workloads, advanced access control measures, and additions to Data Threat Analytics

PALO ALTO, Calif.--(BUSINESS WIRE)-- As government agencies increasingly fall victim to catastrophic cyberattacks, **Rubrik**, the Zero Trust Data Security™ Company, announces **Rubrik Threat Hunting** is now available to **Rubrik Security Cloud - Government** customers. Rubrik Threat Hunting empowers federal, state, and educational institutions to prevent malware reinfection with insights into the initial point, scope, and time of infection.

In the event of a malicious cyber event such as ransomware, speed is paramount to recovery and remediation. But as data continues to rapidly surge and sprawl across SaaS, cloud, and on-premises, organizations struggle to identify what systems were first affected before they can surgically and rapidly restore business continuity, without the risk of reinfection.

According to the most recent **Rubrik Zero Labs State of Data Security report**, 66% of IT and security leaders surveyed believe their organization's current data growth is outpacing their ability to secure this data and manage risk. This can lead to delays in identifying the chronology of a cyberattack, and further delay overall incident response.

"Imagine recovering from a cyberattack, only to find out that your organization has accidentally reintroduced the

malware back into the system. After the costly downtime, psychological impact, and reputational damage — you're back at square one," said Anneka Gupta, Chief Product Officer at Rubrik. "Pinpointing the point, scope, and time of the infection can be nearly impossible without the ability to analyze the history of data for indicators of compromise. Rubrik Threat Hunting provides this deep level of intelligence, designed to enable federal and state governments to be confident in their cyber recovery."

Find Malware and Avoid Reinfection with Rubrik Threat Hunting

Now with Rubrik Threat Hunting, government entities can directly scan their backups for indicators of compromise, including ransomware. With this added intelligence, organizations can more accurately identify the last known clean copy of data in order to prevent reinfection during and after recovery. This allows organizations to verify the integrity of backups and other assets before restoration, and thereby adhere to The National Institute of Standards and Technology (NIST)'s **recently updated** Cybersecurity Framework guidance as part of its Incident Recovery Plan Execution (RC.RP).

New Workloads and Enhancements to Data Threat Analytics and Data Protection

Rubrik also announces additional enhancements to Rubrik Security Cloud - Government, including:

Data Threat Analytics:

- VM encryption detection: Receive anomaly alerts for VM-level encryption activity, quickly assess the blast radius, and recover from such attacks.
- Anomaly Detection for Nutanix AHV and Microsoft Hyper-V: Assess the cyberattack blast radius and identify malicious activity, now available for two new workloads.

Data Protection:

- Quorum authorization: Enforce the requirement of getting quorum approvals for performing data-modifying actions in Rubrik Security Cloud - Government.
- Granular control over password complexity rules for local users: Set policies in Rubrik Security Cloud - Government that ensure users set strong, complex passwords and prevent password reuse.

Protection of New Workloads:

- IBM Db2 protection: Automatically discover and protect Db2 databases while unifying data protection with Rubrik Security Cloud - Government. Perform restore operations with your existing Db2 tools and processes.
- Microsoft Active Directory: Ensure the data users and applications need to authenticate and enforce access

controls are readily available and quickly recoverable. Automatically discover and protect Active Directory data and support recovery of complete domain/domain controllers and individual objects.

Integration:

- Zscaler DLP integration: Discover and classify sensitive data out-of-band from production systems to more effectively prevent the loss of critical business data and double extortion ransomware.

To date, Rubrik Security Cloud - Government has achieved:

- **StateRAMP™ certification**
- **"In Process" FedRAMP® status** and attained security attestations for Criminal Justice Information Services (CJIS) Security Policy and Family Education Rights and Privacy Act (FERPA) security conformance

Rubrik has a long history of securing data for federal, state, local governments and educational institutions. Hundreds of state and local governments nationwide rely on Rubrik, including the **Lewis County Public Utility District**, **San Joaquin County**, and **South Louisiana Community College**.

Learn more about Rubrik Security Cloud - Government by **visiting Rubrik's website**.

About Rubrik

Rubrik is on a mission to secure the world's data. With Zero Trust Data Security™, we help organizations achieve business resilience against cyberattacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine learning, secures data across enterprise, cloud, and SaaS applications. We help organizations uphold data integrity, deliver data availability that withstands adverse conditions, continuously monitor data risks and threats, and restore businesses with their data when infrastructure is attacked.

For more information please visit **www.rubrik.com** and follow **@rubrikInc** on X (formerly Twitter) and **Rubrik** on LinkedIn.

press@rubrik.com

Source: Rubrik