rubrik | Zero Trust Data Security™

M-22-09
Memorandum for the Heads of Executive Departments and Agencies

January 26, 2022

The Executive Office of The President issued this memorandum setting forth a Federal zero trust architecture (ZTA) strategy. Agencies are now required to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024. This is to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns.

Many of the key requirements in this memo are the same Rubrik had at its creation and have been implemented in its solutions: Protect the data no matter where it is, Use the best authentication available today, Integrate into the existing ecosystem, Know what data is where. Rubrik is a Data Security platform based upon the principles of NIST Zero Trust Architecture. It secures protected application and user data against unauthorized access and cyber threats to support efficient recovery operations.

This Rubrik technical brief details how Rubrik Data Security can assist Federal agencies in complying with M-22-09.

1. **M-22-09**: "This strategy places significant emphasis on stronger enterprise identity and access controls, including multi-factor authentication (MFA). Without secure, enterprise-managed identity systems, adversaries can take over user accounts and gain a foothold in an agency to steal data or launch attacks."

   Rubrik Zero Trust Data Security solutions can enforce multi-factor authentication (MFA) on all system interfaces, for all users requesting access. Rubrik solutions can be integrated with SAML 2.0 Identity Providers for centralized management. Rubrik also has native MFA using token based one-time password (TOTP) protection for local accounts.

2. **M-22-09**: "All traffic must be encrypted and authenticated as soon as practicable. This includes internal traffic, as made clear in EO 14028, which directs that all data must be encrypted while in transit. This strategy focuses agencies on two critical and widely used protocols in the near-term, DNS and HTTP traffic;"

   Rubrik Zero Trust Data Security applies strong encryption and authentication to the full data lifecycle. First, all data ingested by Rubrik is encrypted before it is stored. Rubrik uses AES-256 encryption to protect data at-rest. Additionally, all data communications between nodes in the system are fully encrypted, and management communications between Rubrik appliances and Rubrik Software as a Service are encrypted using HTTPS protocols.

3. **M-22-09**: "When agencies encrypt data at rest in the cloud, agencies must use key management tools to create a trustworthy audit log that documents attempts to access that data. This can be achieved by using key management tools operated by the cloud provider, or key management tools that are on-premise or otherwise external to the agency-controlled cloud environment."

   Rubrik Zero Trust Data Security integrates with industry standard Key Management Systems(KMS) available on premise and in the cloud.

4. **M-22-09**: "As agencies grapple with security events throughout their systems and cloud infrastructure, automation of security monitoring and enforcement will be a practical necessity. This capability is often referred to as Security Orchestration, Automation, and Response (SOAR)."

   Rubrik Zero Trust Data Security has an API-first architecture allowing for easy integration with many tools such as Security Orchestration, Automation, and Response (SOAR) and Security Information and Event Management (SIEM). One example of this is that Rubrik and Palo Alto Networks have developed integrations between the Rubrik Platform and Palo Alto Networks Cortex XSOAR. Through integrations like this, SOAR tools can extend their playbooks to leverage Rubrik APIs to orchestrate threat hunts and automate recovery of affected data.

5. **M-22-09**: "While agencies have been required to inventory their datasets for some time, a comprehensive zero trust approach to data management requires going beyond what agencies may be accustomed to thinking of as "datasets."

   Rubrik Zero Trust Data Security has an integrated data locating solution that allows users to discover where data resides, who has access to it, and if that location was affected by a cyber attack.

6. **M-22-09**: "Agencies should strive to employ heuristics rooted in machine learning to categorize the data they gather, and to deploy processes that offer early warning or detection of anomalous behavior in as close to real time as possible throughout their enterprise."

   Rubrik Zero Trust Data Security indexes metadata from protected sources and applies advanced machine learning models to identify anomalies around data change rate and potential malicious encryption. Then, Rubrik shows the data classification of the affected data so agencies know the type and sensitivity of data as well as who has access to the affected data. This enables quick and seamless risk analysis as soon as anomalous data is detected.

It is clear that cyber criminals and their attacks are evolving to circumvent layers of protection. Attacks are becoming more targeted and are increasing at an alarming rate. Agencies are looking for vendors to aid them in ensuring a fast and effective recovery. Rubrik is the powerful, easy to deploy, foundation to a robust Zero Trust strategy.

rubrik

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

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

brf-memorandum-for-the-heads-of-executive-departments-and-agencies / 20220503