WHITE PAPER

Increase Your Data Resiliency with Zero Trust Data Security for AWS

Available in AWS Marketplace

TABLE OF CONTENTS

DIGITAL TRANSFORMATION AND THE MOVE TO CLOUD

To survive as a business with digital-first customers, enterprises need to move faster and with greater agility. Applying new technologies to existing business activities (e.g., leveraging cloud and SaaS applications that generate more data than ever before) continues to fuel the cloud paradigm. For many enterprises, running applications on public clouds such as Amazon Web Services (AWS), represent the ability to rapidly access resources for faster innovation, flexibility, and economies of scale while operating in a data-rich environment.

Though cloud adoption can enable ambitious business outcomes, it creates security blindspots and significant vulnerabilities as the network perimeter expands and the attack surface widens. With more and more data being created, consumed, and stored on AWS, having reliable, secure remote access to critical data and applications is paramount to limiting data sprawl, reducing protection gaps between siloed systems, and minimizing the chance of a cyberattack.

THE RISE OF RANSOMWARE

Although ransomware is not a new threat, it has dominated headlines over the past five years, beginning with WannaCry, Bad Rabbit, and NonPetya in 2017 and DarkSide, REvil, and Hello Kitty/FiveHands in 2021. Ransomware is malware that encrypts an organization's (or individual's) valuable data to deny access until a ransom is paid, typically targeting critical infrastructure, supply chain, and healthcare/first responder networks. These attacks pose a severe threat to businesses today.

Some Ransomware Trends Currently Impacting Organizations Include:

- **Enterprise Threats:** The number of organizations impacted by ransomware increased 102% between 2020 and 2021,[1] and global ransomware costs were expected to reach $20 billion in 2021[2].
- **Financial Exposure:** The average ransomware recovery cost was $1.85 million in 2021, more than double the cost in 2020[3].
- **Low Risk for Attackers:** Anonymous cryptocurrency transactions enable extortion of huge ransoms, as there is little chance of getting caught.

Double Extortion

Another alarming ransomware trend is the rise of "double extortion" ransomware attacks.

In addition to encrypting a victim's data and demanding a ransom, the attacker exfiltrates a copy of the victim's data before it is encrypted. The attacker can then sell the victim's sensitive data—such as personally identifiable information (PII) or credit card numbers—on the dark web even after a ransom has been paid.

[1] Check Point Research, The New Ransomware Threat: Triple Extortion, May 202

[2] Cybersecurity Ventures, Global Ransomware Damage Costs Predicted To Reach $20 Billion (USD) By 2021, October 2019

[3] Dark Reading, Ransomware Recovery Costs Near $2M, April 2021

[4] NPR, How Bitcoin Has Fueled Ransomware Attacks, June 2021

RANSOMWARE AS A SERVICE (RaaS)

In addition to traditional attacks by sophisticated cybercriminals and APT groups, RaaS leverages a franchise deployment model, increasing the accessibility of using ransomware. Instead of writing their own code, aspiring cybercriminals can purchase or rent a RaaS kit with different price points, billing models, encryption methods, technical skill level requirements, and more.

When the data is encrypted, a message displays on the victim's system demanding a ransom—typically to be paid in cryptocurrency (such as Bitcoin)—to retrieve the decryption key that will enable the victim to decrypt their data and restore access. Ransom amounts typically vary from several thousand to millions of dollars, depending on the victim's organization. The attackers usually demand a ransom amount they expect the victim to be able to pay. Ransom amounts also tend to increase as more time (hours or days) passes to limit the victim's options—such as restoring from backup and contacting law enforcement—and to entice the victim to pay sooner rather than later.

Law enforcement agencies, such as the U.S. Federal Bureau of Investigation (FBI) and U.S. Cybersecurity and Infrastructure Agency (CISA), generally recommend that ransomware victims not pay a ransom, because doing so funds and encourages further threat activity by cybercriminals, Advanced Persistent Threat (APT) groups, cyberterrorists, and rogue nation-states. However, this guidance must be evaluated on a case-by-case basis. Ultimately, the decision whether or not to pay a ransom belongs to the victim and is often predicated on factors such as the scale and scope of the attack, the value of the encrypted data, and the victim's ability (or lack thereof) to rapidly restore their data from backups.

For victims, it is important to remember that paying a ransom is no guarantee that data will be successfully restored. Just as the attackers have a reasonable expectation of the victim's ability to pay a ransom, the ransomware "business" model relies on a victim's reasonable expectation that if they pay the ransom, they will receive the decryption key. Although this is generally the case, there are no "money-back guarantees" and there is no honor among thieves—or cybercriminals, APT groups, cyberterrorists, and rogue nation-states. Even if the decryption key is provided, the victim may still be unable to restore their data, or it may be faster to restore the data from a backup as the decryption process often takes a very long time.

Data backups have always been, and remain, your best and last defense against ransomware attacks. However, attackers are also aware of this axiom and frequently target a victim's data backups in addition to production data.

Without a reliable and immutable data backup, a ransomware victim has no option but to pay the ransom and hope for the best—and "hope" is a poor cybersecurity strategy.

CYBER RESILIENCE ENABLED BY ZERO TRUST

To contend with the new normal, IT teams are turning to Zero Trust Security models to protect against ransomware and other cyber threats. Delivering protection for your data on AWS requires a modern approach that protects your entire journey to AWS, from migration and protection to replication and long-term retention. For an added layer of security, this approach needs to integrate immutability as a standard across processes.

One way to accomplish this is with a Zero Trust architecture, designed with a "never trust, always verify" approach to security. This methodology assumes that every user, device, or application connected to a network can be compromised and is therefore afforded no inherent trust.

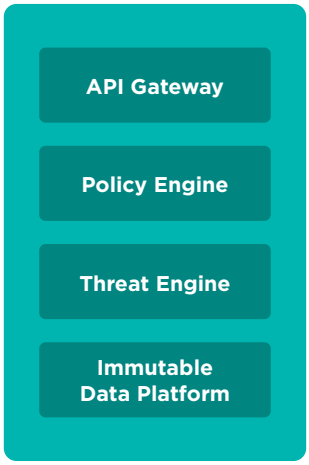
Zero Trust requires every user's identity to be verified to a level beyond a simple username and password. Should a user fall prey to a phishing attack, for example, their compromised credentials could allow an attacker to access privileged systems—including your backup systems—threatening your organization's ability to recover from a ransomware attack.

Only users that have been authenticated using strong methods, such as multi-factor authentication (MFA), can connect and get access to data—and only to the data they need to perform their authorized job functions. Permissions and access are strictly enforced, based on the principle of least privilege, and users are unable to do anything malicious to stored data.

RUBRIK ZERO TRUST DATA SECURITY

Rubrik Zero Trust Data Security is built on the principles of Zero Trust security, and unifies protection across on-premises and AWS environments, while protecting your data via intrusion risk control and a secure data layer. Rubrik Zero Trust Data Security ensures the security of your critical applications and data by:

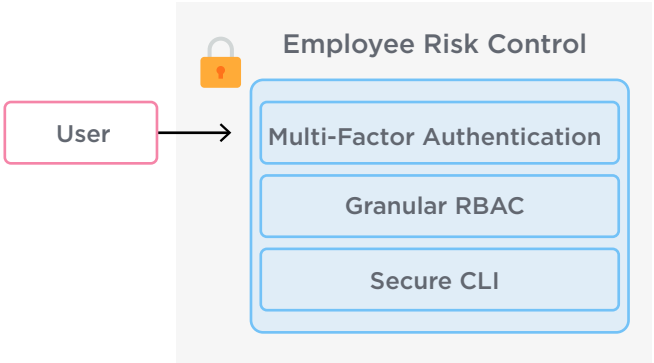
- Preventing attackers from discovering your backups
- Ensuring backup data can't be encrypted
- Controlling access to backups of virtual machines (VM), databases, and more



Rubrik Intrusion Risk Control

Intrusion risk control is a critical component of Rubrik Zero Trust Data Security and incorporates:

- MFA
- Granular Role-based Access Controls
- Disablement of Factory Reset
- Secure Command-Line Interface (CLI)



These security techniques reduce the inevitable risks inherent in having multiple user, employee, and service accounts. Next, we'll jump into the value of each one of these features.

Multi-Factor Authentication

Rubrik includes native MFA that doesn't require use of a third-party security assertion markup language (SAML) provider. With a Time-based One-Time Password (TOTP) method to implement MFA, Rubrik generates an authentication code that changes after a set period of time, meaning even if attackers are able to obtain a user's login password, they will not be able to use that information to access the backup system.

MFA is available for local Lightweight Directory Access Protocol (LDAP) and Single Sign-On (SSO) accounts. Companies using an SSO provider should implement both SSO and MFA to increase security.

Granular Role-Based Access

Rubrik makes it easy to assign granular role-based access control (RBAC) permissions and can integrate with your directory. MFA first verifies identity, then the policy engine grants least-privilege access based on a user's or service's role. If an attacker somehow manages to steal credentials with approved access to your data, RBAC can drastically reduce the potential impact, especially when it comes to ransomware.

Factory Reset is Disabled

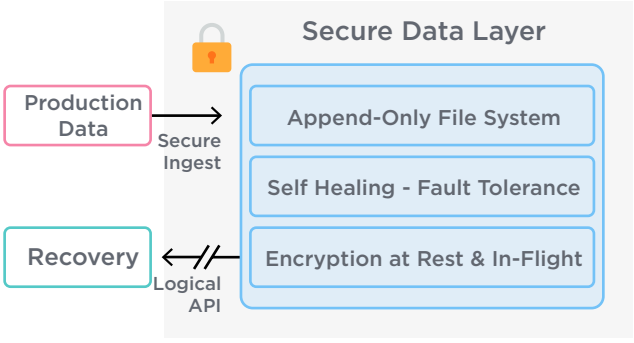
Factory reset commands are proactively disabled, providing important additional security. Even if a hacker is able to access a Rubrik system using stolen credentials, they are unable to reset the system to compromise data access or recovery. Should an individual Rubrik node or a cluster require a reset, Rubrik Support must be contacted with additional provable credentials.

Secure Command-Line Interface

Rubrik is built to secure and protect all system interfaces. This includes protection for the CLI via one-time passcode functionality. With TOTP for CLI, an additional layer of security protects against vulnerabilities such as OS command injection attacks that might somehow remotely execute arbitrary code on Rubrik-managed systems.

THE RUBRIK SECURE DATA LAYER

The Rubrik Secure Data Layer applies security best practices to ingest, manage, and store data immutably, providing a last line of defense against ransomware. Rubrik uses the latest techniques to ensure your backup data is protected against threats, including encryption, immutability, erasure coding, and Service Level Agreement (SLA) domains.



Air Gap

Immutability

Retention Lock

Data Encryption

Encryption

Rubrik offers data encryption at rest and in-flight so that data is never exposed to untrusted users. If your organization is compromised, data encryption is the best way to ensure that data cannot be read and misused by malicious actors.

Immutability

Rubrik architecture combines an immutable filesystem with Zero Trust cluster design, preventing unauthorized access to or deletion of backups, ensuring your team can quickly restore to the most recent clean backup with minimal business disruption. Immutability is baked into our filesystem so it is on by default for all data managed by Rubrik and can't be disabled.

With the **Rubrik Zero Trust cluster design,** operations within a cluster can only be performed through authenticated APIs. Other cluster designs rely on a full-trust model in which all members of a cluster are able to communicate freely with one another, a structure that can make restores impossible.

Erasure Coding

An important aspect of the Rubrik filesystem is how erasure coding is used to write data to disk. Erasure coding is a method of storing redundant data to ensure full recoverability from storage failures. When disks or cluster nodes fail, erasure coding ensures continued data availability with self-healing.

Service Level Agreement Domains

Some people believe that tape storage is more immune to ransomware than other forms of backup. While that may be true in some cases, how long does it take to recover from tape stored offsite? Extended recovery after a ransomware attack creates a significant financial and business impact. It is crucial to have built-in, intelligent orchestration to achieve an efficient return to operations.

Rubrik's robust SLA Domains ensure that data is where it needs to be, when it needs to be there, enabling Rubrik to deliver rapid recovery combined with the security provided by encryption and an immutable filesystem.

SECURE YOUR AWS CLOUD JOURNEY

With the amount of data growing faster than ever, customers are on a journey to keep their infrastructure on par to meet the changing business demands. This journey inevitably leads them to the cloud. Rubrik can accelerate and secure your AWS Cloud adoption with cloud-native protection in the following areas:

- **Cloud Protection:** Always have reliable, clean copies of your data with native, immutable snapshots of Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Block Store (Amazon EBS), Amazon Relational Database Service (Amazon RDS), Amazon Elastic File System (Amazon EFS), and Amazon FSx.
- **Cloud Migration:** Instantiate on-premises apps and workloads with automated VM to Amazon EC2 conversion for development/testing and cloud recovery.
- **Long-term Retention:** Reduce storage costs by archiving backup data to Amazon Simple Storage Service (Amazon S3) with storage tiering while retaining instant access with predictive search.
- **Heterogeneous Replication:** Copy data across public clouds, AWS accounts and regions, edge locations, and data centers using global SLA policies.

Amazon S3 is an object storage service offering industry-leading scalability, data availability, security, and performance. The Amazon S3 Object Lock feature can help prevent objects from being deleted or overwritten either for a fixed amount of time or indefinitely. You can use Amazon S3 Object Lock to meet regulatory requirements that call for write-once-read-many (WORM) storage or add an extra layer of protection against object changes and deletion.

Rubrik-supported Amazon S3 storage class options include:

- **Amazon S3 Standard:** Active, frequently accessed data, milli-second access
- **Amazon S3 Standard-IA (Infrequent Access):** Infrequently accessed data, millisecond access, retrieval fee per giga-byte, minimum storage duration, minimum object size

Rubrik supports backup immutability with Amazon S3 Object Lock in compliance mode, so backup and archive data are protected whether it is on Rubrik or archived out to Amazon S3. When an object is locked in compliance mode, it cannot be overwritten or deleted by any user—including the root user. In addition, its retention mode cannot be changed, and its retention period cannot be shortened, helping ensure that an object version cannot be overwritten or deleted for the duration of the retention period. Rubrik's support of Amazon S3 Object Lock adds additional protection against both accidental and malicious deletion.

Amazon S3 bucket versioning is automatically enabled by Rubrik when you enable Amazon S3 Object Lock. Amazon S3 versioning allows customers to preserve, retrieve, and restore every version of every object stored in their buckets. With versioning, you can recover more easily from both unintended user actions and application failures.

MANAGING RECOVERY AND RESTORE

When a disaster or ransomware attack strikes, a simple, scalable path to full recovery is essential to avoid costly interruptions. Rubrik Mass Recovery enables you to ensure business continuity with secure recovery of your data and applications on AWS to meet stringent recovery time objectives. Ensuring security and resiliency for data and business services is a critical responsibility. Executing manual recovery plans for applications with multiple tiers and interdependencies can slow down the recovery process and introduces opportunities for error.

Rubrik Mass Recovery helps you to minimize downtime by recovering hundreds of VMs or restoring tens of thousands of files to a clean state in minutes. It's easy to avoid reinfection as well with simple identification of files and applications infected by ransomware. Rubrik then enables you to quickly identify a clean snapshot and recover your data with no reinfection, while recovering only what you need, accelerating the recovery and restoration process. Recover only the data that has been compromised with guided workflows for file-level, object-level, application-level, and system-wide restore.

AWS supports your recovery on-demand from outages, regardless of where you run Rubrik or store data. Rubrik can automate the conversion of VMs, or cloud-based object storage like Amazon S3, into compute instances running on Amazon EC2. Whether your applications are on-premises or in AWS, you can move on from your largely idle disaster recovery site.

When combined with Rubrik Ransomware Monitoring and Investigation and Threat Containment, you can accelerate recovery from ransomware by analyzing and then selecting all impacted applications and files and restoring to the most recent clean version with a few clicks. Orchestrated Application Recovery automates the restore process.

ZERO TRUST DATA SECURITY BEST PRACTICES

SETTING UP AN USING AMAZON S3 OBJECT LOCK CORRECTLY

After you set up Amazon S3 Object Lock, the data cannot be deleted as compliance mode is used for all Amazon S3 buckets. Setting Amazon S3 Object Lock up correctly the first time is critical.

MAKING DECISIONS AROUND ATE RETENTION

Remember that your data is going to be retained for the period you specify for it to be locked, and you will need to pay for the storage during this time. This means you will need to put some thought into the creation of your SLA domain that will be uploading objects to the archive. For example, you have the following SLA constructs:

- Backup every day, retain for 31 days
- Backup every month, retain for 6 months
- Archive data older than 1 month

In this case, 5 months of data will be archived out. Therefore, the most logical retention period for immutability is 5 months. When a backup attains the age of 5 months plus 1 day, it will then be free for deletion.

SECURITY ROLES AND ACCESS MANAGEMENT

Rubrik has many prebuilt AWS CloudFormation templates which create everything for you in terms of archives, following best practices including least-privilege security. Role-based access control (RBAC) is also available in Rubrik, and administrators should always be restricted to only those objects they need access to.

DEPLOYING RUBRIK FROM AWS MARKETPLACE

AWS Marketplace enables buyers to search, select, purchase, and deploy software, data products, solutions, and services on AWS with simplicity. It complements traditional procurement workflows and allows buyers to experience a variety of financial benefits that help lower bottom-line costs and eliminate time-intensive efforts.

Many organizations struggle with outdated and cumbersome procurement processes and also fulfill AWS spending commitments. If this rings true for your organization, instead of losing a portion of investments or attempting to increase AWS use in organizational areas that might not be ready, driving purchases through AWS Marketplace can help solve this situation. Forrester research shows that organizations that shifted their software procurement to AWS Marketplace saw a 550% return on investment.

Purchasing through AWS Marketplace can drive efficiency throughout your entire procurement process and the deployment process as well. Once purchased, deployment of Rubrik is accelerated by leveraging one of Rubrik's prebuilt AWS CloudFormation templates. These templates help you define needed resources, allowing for simple updates and wrap-up.

LEARN MORE

It's time to start thinking about your security strategy and how it relates to data backup, recovery, and long-term archival storage. Get started today: view Rubrik in AWS Marketplace.

rubrik

Rubrik, Inc.
3495 Deer Creek Rd
Palo Alto, CA
94304

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

Rubrik is a cybersecurity company, and our mission is to secure the world's data. We pioneered Zero Trust Data Security™ to 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 Twitter and Rubrik, Inc. on LinkedIn.