rubrik | Zero Trust Data Security™

WHITE PAPER

Definitive Guide to Zero Trust Data Security

Table of Contents

Introduction

Ransomware attacks are growing at an alarming rate. You can't turn on the news without hearing about yet another organization that has been affected. These attacks pose a severe threat to today's businesses.

To make matters worse, the rate of ransomware attacks continues to increase. According to Harvard Business Review, ransomware attacks were up 150% in 2020, and ransoms paid by victims increased by more than 300%.

A recent Gartner report, *Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware*, noted that "By 2025, at least 75% of IT organizations will face one or more attacks." In the battle against ransomware, traditional approaches to security and data protection are failing.

- **Perimeter security is not enough to keep ransomware out.** Despite massive investments in perimeter, endpoint, and application-layer defenses, attackers continue to gain access to valuable business data.
- **Traditional backups are vulnerable.** While backups are the last—and most important— line of defense against ransomware, sophisticated attackers know this too. Many ransomware attacks target backups to prevent recovery and force payment. Traditional backup methods are great for recovering from natural disasters and operational failures, but they were not built to withstand cyber threats and are therefore vulnerable.

In the face of these grim realities, IT teams are turning to Zero Trust methods to protect against ransomware and other cyber threats. Zero Trust is based on the assumption that all users, devices, and applications are untrustworthy.

This ebook explores the use of Zero Trust methods to protect backup data and minimize the impact of ransomware attacks. It explains key techniques to:

- Reduce the risk of intrusion
- Secure your backup data

- Detect anomalous behavior
- Discover and manage sensitive data to ensure compliance
- Contain incidents
- Recover quickly with minimal time and effort

Finally, this ebook explains the foundational technologies behind Rubrik Zero Trust Data Security, describing how Rubrik keeps data safe and makes it easy to recover.

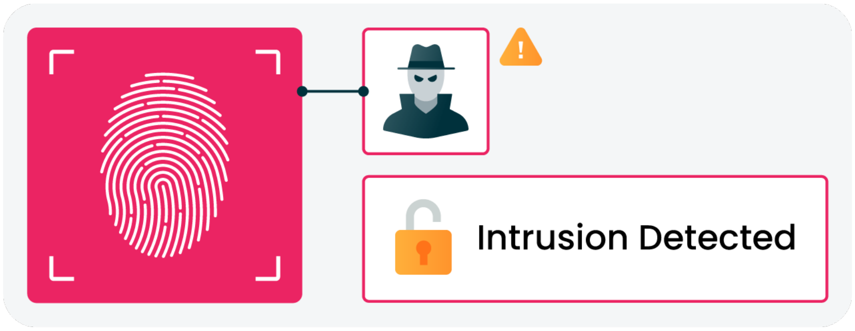
Why Zero Trust Matters to You

The limitations of perimeter security and traditional data backup are driving the need for Zero Trust. A Zero Trust architecture assumes all users, devices, and applications are untrustworthy and can be compromised. Only users that have been authenticated using multi-factor methods get access to data—and only to the data they need. Permissions and access are strictly limited, and users are unable to do anything malicious to stored data.

The Zero Trust model is defined by the National Institute of Standards (NIST), in the NIST SP 800-207 Zero Trust Architecture Specification. As NIST describes it, Zero Trust comprises *“an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources.”*

When it comes to protecting backup data, Zero Trust Data Security relies on six distinct capabilities.

Reduce Intrusion Risk



The first line of defense in Zero Trust is preventing attackers from gaining access to data in the first place. There are multiple methods to reduce unauthorized access:

- **Multi-factor authentication (MFA).** MFA validates a combination of factors requested from a user. The most common factor is a user's credentials. The second factor might be a Time-based One-Time Password (TOTP), biometric identifier, or key card. More factors can be used to further increase security. By combining something you know and something you have, MFA mitigates cyber-attacks and reduces the risk of unauthorized access. MFA should be considered a must have for access to backup systems and data.
- **Role-based access control (RBAC).** RBAC restricts access based on an individual's role within your organization or based on a service's function. (Service accounts are created to allow third-party tools to have the necessary privileges to perform their functions.) Various user accounts and service accounts have different access privileges. Limiting access based upon role can greatly reduce the amount of data affected if a ransomware attack or other intrusion does occur.
- **Least privileged access.** Employees and services only get access to the resources necessary to perform their specific job duties—and nothing more. Even if a user is successfully authenticated, if they are not assigned to perform a specific task as defined by policy (based on factors such as authority, responsibility, and job competency), they are not granted access rights.

Safeguard Backup Data From Compromise

The next line of defense is to protect your backup data to the greatest extent possible—even if ransomware gains access. Again, there are multiple methods that should be employed:

- **Encryption.** Encrypting backup data ensures that if malware or a hacker gains access to your backup data, it cannot be read, reducing the risk that sensitive customer and employee data or valuable intellectual property (IP) will be breached. Ideally backup data should be encrypted both in-flight and at rest.

- **Immutability.** Because ransomware is able to encrypt already encrypted data and make it inaccessible, immutability is necessary to protect backup data from being encrypted by hackers or ransomware. Once data has been written, an immutable backup cannot be modified or deleted—either for a set period of time or forever. The technologies that underpin immutable data storage are often referred to by the acronym WORM (write-once-read-many).

By combining encryption and immutability, you can ensure that even if ransomware gains access to your data, it can neither render your backups unreadable nor exfiltrate data that compromises your company, your employees, or your customers.

Detect Anomalous Activity For Faster Investigation

Another important line of defense against ransomware for any organization is early detection. Delayed detection gives hackers more time to find and exploit vulnerabilities within your operations and can extend the time needed to recover fully.

Modern technologies that leverage machine learning models can help detect security threats through deep analysis of filesystems and access behavior. Backups may include rich metadata that can be securely analyzed to detect and generate alerts on anomalous activity using ML-based technologies. When unusual behavior is detected, IT teams should be alerted immediately to investigate, accelerating recovery if needed.

Some solutions use *signature-based detection* that compares patterns and sequences to known malware variants. However, by itself this is not always an effective approach since ransomware often mutates. In addition, signature-based detection only works when you are not the first victim—most ransomware attacks use a morphing and code obfuscation approach with a zero-day signature. Solutions that employ behavioral-based detection are often a better approach since they can catch these zero-day ransomware attacks.

Discover and Manage Sensitive Data

Another important line of defense is to identify and manage sensitive data ahead of time – before a breach occurs. At a minimum, this should include ensuring compliance with the laws and regulations of the region(s) in which you operate (such as GDPR and CCPA), industry-specific regulations (like HIPAA and PCI-DSS), and your own internal policies. If you suffer a ransomware attack, being out of compliance only adds to your troubles.

In practice, you need to make sure that you:

- Properly protect all new workloads
- Enforce data retention periods
- Have the ability to quickly identify any sensitive data that may have been exfiltrated

In a busy IT environment, automation is essential to ensure that these requirements are met and your policies are enforced—with compliance audits and regular reporting so that any problems can be quickly remediated.

Contain Incidents and Recover Quickly

Full ransomware protection must also include the ability to contain any incidents that occur and return to normal operations quickly. Incident containment ensures that after an attack occurs you can fully contain it and avoid reinfection. Once ransomware enters your systems, it is necessary to quickly identify the scope of the infection, isolate all infected systems, and track signs of the infection backwards in time to the point of infiltration. Machine learning techniques can help you work your way back in time until you are certain that recovery can proceed with clean data.

Rapid recovery is essential to get your business back on its feet as quickly as possible with minimal disruption to business function. No organization is immune to cyber attacks but a long recovery time after an incident may create significant impacts to your business and its reputation. The ability to rapidly recover from an incident while minimizing data loss is critical to your bottom line. A comprehensive backup plan that is regularly tested is essential for minimizing losses.

Your backup and recovery solution should be designed for fast, reliable disaster recovery. Even in the event of a ransomware attack, it should be relatively straightforward to identify and restore to the most recent clean version of your data. Technologies that help automate the assessment of an attack's impact and provide a clear view into what applications and files are infected or encrypted and where they reside, can enable your teams to quickly restore at a more granular level.

Rubrik Zero Trust Data Security

Modeled after the Zero Trust Implementation Model from NIST, Rubrik Zero Trust Data Security implements all of the capabilities described above, providing maximum protection against hackers and rapid recovery from ransomware attacks.

Data written to the Rubrik system cannot be modified, deleted, or encrypted by an attack, ensuring that backup data is readily available for recovery. Multiple expert-guided recovery options—including Live Mount, Mass Recovery, and Orchestrated Application Recovery—enable you to quickly recover files and workloads impacted by an attack.

Rubrik Zero Trust Data Security Benefits

IT Teams

- Protect critical data from ransomware attacks
- Recover data and applications quickly
- Avoid ransom payments

Security Teams

- Leverage secure backup data for attack forensics
- Initiate recovery from security operations center

Application Owners

- Rest easy knowing business data is protected
- Applications can be restored quickly to maintain business continuity

CIOs and CFOs

- Ransomware recovery supported by Zero Trust
- Minimize cyber insurance costs
- Prevent reputational damage

Rubrik Zero Trust Data Security goes to the heart of data protection—keeping hackers out of your backup system, identifying ransomware activity, and making sure all data has a clean backup that can be recovered quickly.

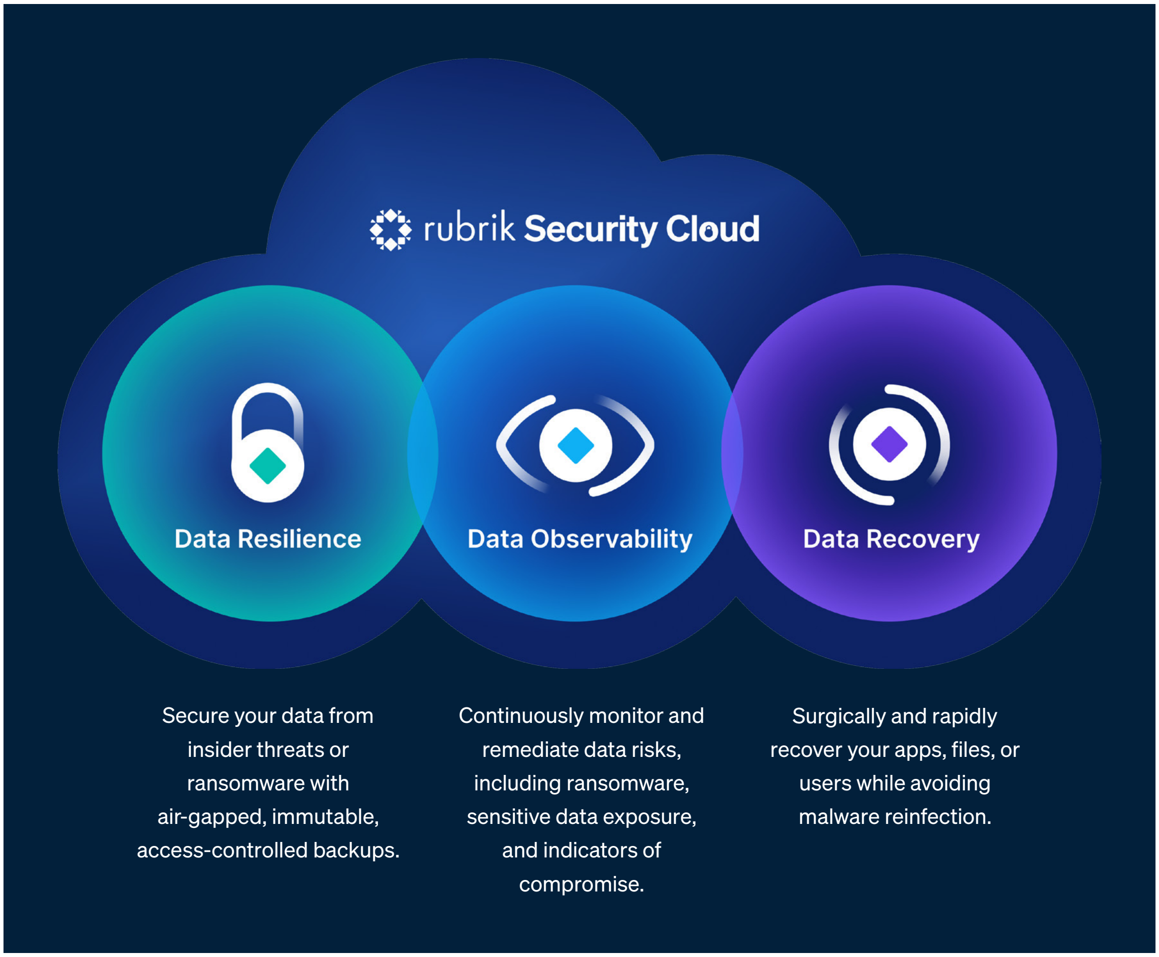
At the core of Rubrik Zero Trust is a purpose-built filesystem that never exposes backup data via open network protocols. Because Rubrik backup storage is not online nor is it accessible over the network, there's a logical air gap that blocks data from being discoverable or accessible. This approach offers similar protection without the impact to recovery time of a physical air gap.

The Gartner report mentioned in the introduction recommends implementing features for: early detection, protecting the backup system, and fast recovery. To ward off direct attacks on backup systems, Gartner strongly encourages a number of measures including immutable file storage, eliminating the use of network file protocols for backup, multi-factor authentication (MFA), separation of roles, and use of multi-person authorization for changes to the backup system. All of these capabilities are incorporated as part of the Rubrik solution.

The remainder of this ebook describes the various technologies that underlie Rubrik Zero Trust Data Security. These technologies fall into three categories:

- **Data Resilience.** Prevent and protect against ransomware infection
- **Data Observability.** Detect and identify ransomware attacks quickly
- **Data Recovery.** Contain ransomware after infection and recover efficiently

All capabilities are accessible from the Rubrik Security Cloud—and via Rubrik APIs for easy integration.



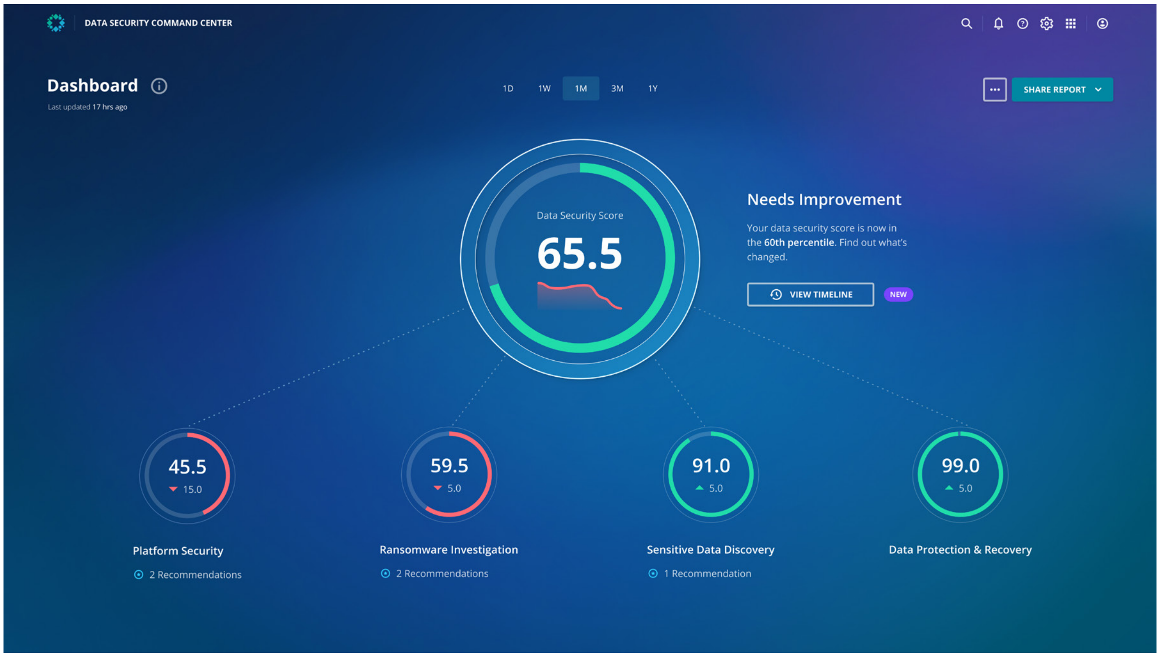
Secure your data from insider threats or ransomware with air-gapped, immutable, access-controlled backups.

Continuously monitor and remediate data risks, including ransomware, sensitive data exposure, and indicators of compromise.

Surgically and rapidly recover your apps, files, or users while avoiding malware reinfection.

Data Security Command Center

The Rubrik Data Security Command Center (DSCC) allows your team to access all of the capabilities of the Rubrik Security Cloud, helping your organization determine whether your data is safe and protected. A data security score is calculated across four major risk categories, providing a breakdown of scores by category, with details that enable you to assess data risk properly.



Your data security score is now in the **60th percentile**. Find out what's changed.

A convenient and easy-to-use SaaS service, DSCC provides visibility into your organization's data risks and security gaps, with recommendations to improve overall security posture. It radically simplifies data risk management by providing a single point of global visibility and collaboration. As a result, you can reduce the complexity of data risk management, avoid unnecessary costs and make smarter, data-driven business decisions around data security.

Data Resilience

Data Resilience

Your data is defended against cyber threats

When it comes to ransomware protection, backups can be a significant point of vulnerability.

- **Manual backup management** for hundreds of applications creates too many opportunities for error (and wastes valuable staff time).
- **Backup access** may not be restrictive enough, and credentials to gain access may be easily compromised
- **Under- or un-protected applications** increase risk from a successful attack.
- **Inadequate security tools** leave backup data vulnerable to compromise.

Rubrik automates and simplifies data management to address these challenges.

- A scalable platform manages data throughout its entire lifecycle, delivering better economics and simpler operations.
- Rubrik eliminates the overhead of managing legacy backup jobs, replacing them with just a handful of easy-to-define and manage policies.
- The Rubrik platform integrates easily into your environment.

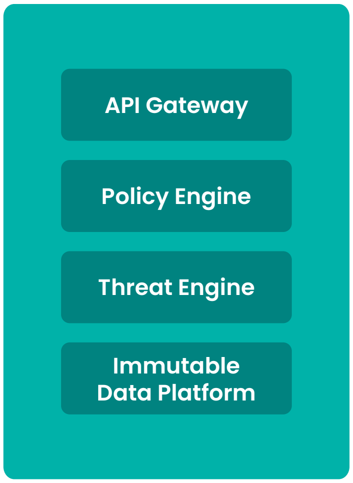
Rubrik ensures the resilience and security of your critical data with:

- **Rubrik Zero Trust Data Protection.** Safeguard your data against internal and external threats.
- **Rubrik Cloud Vault.** Ensure a clean copy of your data is stored off site and easily accessible and available for recovery.

Rubrik Zero Trust Data Protection

Rubrik Zero Trust Data Protection ensures the security of your critical apps and data. Rubrik:

- Prevents attackers from discovering your backups.
- Ensures backup data can't be encrypted.
- Controls access to backups of VMs, databases, and more.

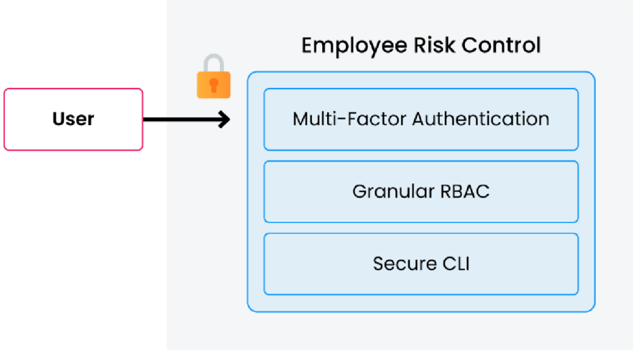


Rubrik Zero Trust Data Protection builds on the principles of Zero Trust, unifying protection across on-prem, multi-cloud, and SaaS environments, while protecting your data via *intrusion risk control* and a *secure data layer*.

Rubrik Intrusion Risk Control

Intrusion risk control is a critical component of Rubrik Zero Trust Data Protection. Rubrik incorporates:

- Multi-factor Authentication.
- 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.

Multi-Factor Authentication

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.

Rubrik includes native Multi-Factor Authentication that doesn't require the use of a third-party SAML provider such as Okta. Using a Time-based One-Time Password (TOTP) method to implement MFA, our algorithm automatically generates an authentication code which changes after a certain period of time. Because the passcode is one-time and time-based, even if an attacker were to obtain a user's login password, they would not be able to access the backup system and compromise backup data. 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. The two are not mutually exclusive. With TOTP, attackers cannot gain access to your backup data, even if your active directory is compromised and attackers obtain stolen username and password credentials or try to bypass SSO via local accounts. Utilizing both SSO and MFA increases security.

Granular Role-Based Access

Rubrik makes it easy to assign granular RBAC permissions and integrate with Active 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

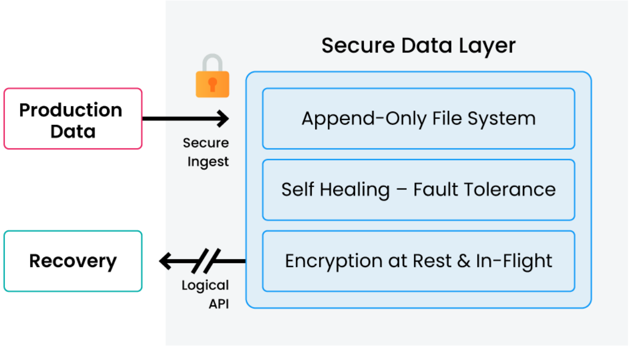
Factory reset commands are proactively disabled, providing important additional security. Even if a hacker is somehow able to access a Rubrik system using stolen user credentials, they are unable to reset the system to compromise data access or recovery. Should an individual Rubrik node or a cluster 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 Command Line Interface (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.



Air Gap

Immutability

Retention Lock

Data Encryption

Encryption

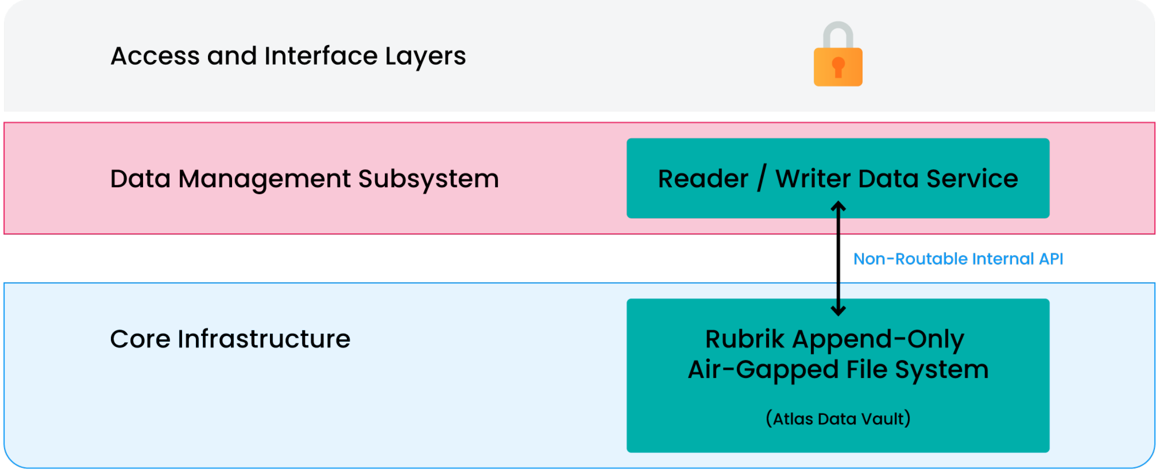
Rubrik offers data encryption at rest and in-flight so that data is never exposed to untrusted users.If your organization is compromised, data encryption is the best way to ensure that data cannot be read and misused by malicious actors. Data encryption protects the confidentiality of your data by making it unreadable to prying eyes that lack the necessary keys for decryption.

Immutability

With Rubrik, immutability goes beyond simple file permissions, folder ACLs, or storage protocols. Our architecture combines an immutable filesystem with Zero Trust cluster design.

Immutable filesystem. The Rubrik filesystem is immutable and prevents unauthorized access to or deletion of backups, ensuring your team can quickly restore to the most recent clean backup with minimal business disruption.

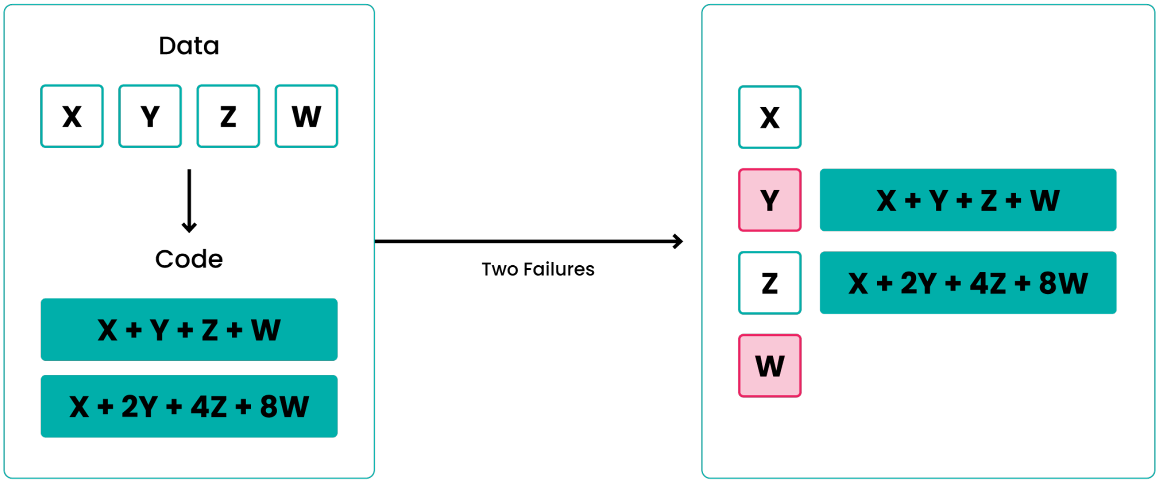
With Rubrik, immutability is not a feature that is turned on or off for specific workloads, applications, or data sets. It is baked into the filesystem so it is on by default for all data managed by Rubrik and can't be disabled. Other solutions rely on the administrator to enable or disable immutability or WORM for the desired data sets and then plan for and manage the additional data usage. Rubrik does that all natively and transparently.


Access and Interface Layers
Data Management Subsystem
Reader / Writer Data Service
Non-Routable Internal API
Core Infrastructure
Rubrik Append-Only
Air-Gapped File System
(Atlas Data Vault)

Zero Trust cluster design. 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. In some cases, this may include root-level authority, no mutual authentication checks, and the ability to read or modify data held within the filesystem. Once a single node has been penetrated in a full-trust cluster, backup data can be compromised to make restores impossible.

Erasure Coding

An important aspect of the Rubrik filesystem is the way it uses erasure coding—a method of storing redundant data to ensure full recoverability from storage failures—to write data to disk. Erasure coding allows Rubrik to strike a balance between the overhead due to storage redundancy and availability. It makes more of a system's total storage available for protecting data, reducing the total cost of ownership (TCO) while ensuring the system is tolerant to failures.



Four equations and four variables – everything can be recovered!

When disks or cluster nodes fail, erasure coding ensures continued data availability with self-healing. Rubrik can typically self-heal in less than an hour, reducing the probability of simultaneous node failures in large, distributed systems.

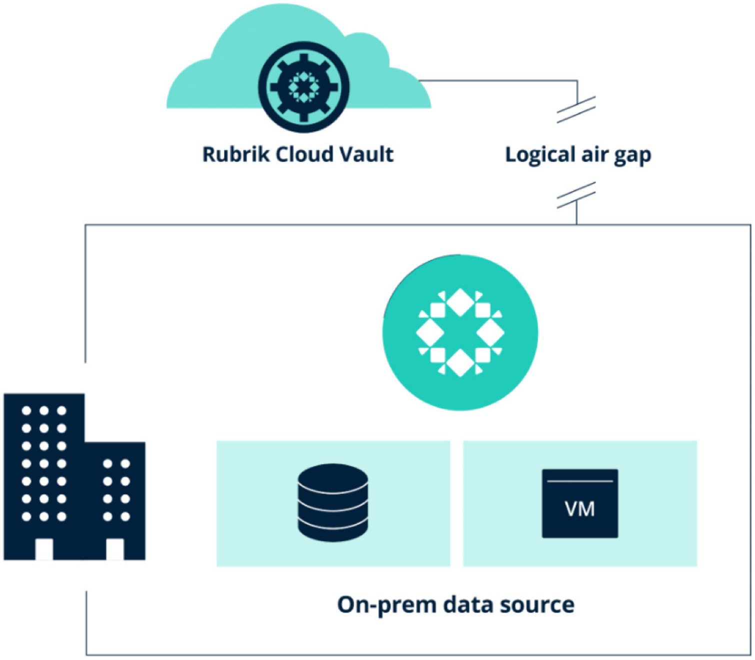
SLA Domains

Some people believe that tape 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.

Rubrik Cloud Vault

Rubrik Cloud Vault extends the capabilities of Rubrik Zero Trust Data Protection and Rubrik's Secure Data Layer to isolated, off-site cloud archival. The fully managed service removes operational complexity while providing a logically air-gapped archive solution with predictable costs. Built on Azure storage, Cloud Vault provides completely isolated, immutable copies of your protected data in the cloud to support recovery from cyber-attacks and natural disasters.

Once Cloud Vault is configured, you simply create one or more SLAs that utilize it. All data protected with those SLAs are automatically stored on-premises and in the cloud, providing managed redundant backup and archived data. All storage and egress charges are included in the service.



Data Observability

Data Observability

Cyber threats are monitored continuously and analyzed quickly

Once you've created a backup environment that's secure and resilient, the next step is to ensure that you can detect any attempted attacks quickly, but this can be a challenge with traditional approaches:

- **Failure to identify sensitive data** ahead of time increases risk and cost.
- **Locating where and when threats entered** your environment can be time consuming.
- **Reinfection of production systems** can occur during recovery.
- **Data risks** spread unchecked.

Rubrik Zero Trust Data Security addresses these challenges with comprehensive capabilities that reduce risk and save time:

- **Sensitive Data Monitoring.** Classify data and assess exfiltration risk.
- **Ransomware Monitoring & Investigation.** Detect anomalies using machine learning.
- **Threat Monitoring & Hunting.** Find malware and avoid reinfection.

Sensitive Data Monitoring

Lack of visibility into sensitive data can lead to vulnerabilities and unnecessary incident response costs. Rubrik Sensitive Data Monitoring scans backups and locates sensitive data in files and applications to help you stay compliant.

Rubrik provides visibility into the content of your data, where it lives, and who has permission to access it. If data is breached, the ability to know what data may have been exfiltrated can guide IT teams in their negotiations with cyber criminals.

The ability to guard against threats, answer pressing business questions, and determine whether high-value or sensitive data has been affected during a ransomware attack is an important part of the recovery process. These capabilities are a fundamental component of the Rubrik Zero Trust Architecture.

Rubrik's discovery, classification, and reporting have zero impact on your production environment. Rubrik deployments process backup data and metadata with zero additional infrastructure and without installing any agents. Rubrik enables you to identify at-risk data and better withstand a data breach or ransomware attack to avoid reputational, financial, or legal consequences.

Asset Discovery and Protection

Rubrik Sensitive Data Monitoring helps you minimize vulnerability by discovering all data across your environments—from the datacenter to public cloud— and can automatically apply SLA policies to protect newly created assets. The Rubrik Unmanaged Objects Report runs periodically to discover virtual machines, databases, or cloud workloads without an assigned SLA so that the right level of protection can be applied.

Retention Lock

Rubrik helps prevent malicious actions by rogue users by ensuring that no single person can clear or shorten retention policies or delete archival or replication locations. The security of retention-locked SLAs is controlled through a validation process. If a modification to a retention-locked SLA is requested, two appointed individuals from your organization are required to authenticate and acknowledge the modifications with the Rubrik Support Team. This is especially important in heavily regulated industries requiring WORM compliance as mandated by regulations such as SEC Rule 17a-4(f) or FINRA Rule 4511(c).

Compliance Reporting

Rubrik helps mitigate sensitive data exposure by proactively scanning backups to identify sensitive data and facilitate compliance with applicable privacy laws, such as GDPR, HIPAA, and PCI-DSS. Rubrik helps gain valuable insight into what data lives where and can quickly produce reports on regulated data or policy violations.

Ransomware Monitoring & Investigation

Rubrik understands that a ransomware attack is a worst-case scenario for most enterprises. After an attack, your company will likely be faced with widespread IT, business, and logistics issues all at the same time. Rubrik has developed a set of best practices to help you plan for, identify, and remediate ransomware attacks.

Rubrik Ransomware Monitoring & Investigation capabilities help you discover attacks quickly so they can be contained, by monitoring for encryption, analyzing unusual access patterns, and alerting you of signs of potentially malicious activity in your backup data. Rubrik:

- **Uses machine-learning-based anomaly detection** to discover potential threats automatically.
- **Scopes the blast radius of an attack** and makes recommendations about the best recovery points.
- **Provides API integration** with popular security operations tools, enabling strong collaboration between IT and security groups for faster incident response.

Rubrik enables your teams to quickly identify and locate which applications and files were impacted by ransomware, so you only restore the files and applications that have been affected.

Anomaly Detection Using Machine Learning

Backup data is rich with information, including the content itself along with metadata such as path, size, ACL details, UIDs, GIDs, and other attributes. Rubrik Zero Trust Data Security feeds this information into a machine learning pipeline that provides intelligent insights that streamline the decision-making process during ransomware recovery.

At Rubrik, once a backup (snapshot) is completed, a filesystem metadata diff (FMD) file is created, containing a list of entries corresponding to files that have been created, deleted, or modified since the last backup. A deep neural network (DNN) is used to build out a full perspective of each workload.

The DNN is trained using supervised learning and can identify trends across all samples and classify new data based on similarities to existing data without human input.

The DNN analysis consists of an anomaly detection model and an encryption detection model:

- **Filesystem Behavior Analysis.** Performs behavioral analysis on filesystem metadata by looking at things like number of files added, number of files deleted, and so on.
- **File Content Analysis.** If there is an anomaly in filesystem behavior, a second analysis is performed to determine if there is a characteristic sharp increase in file entropy that signals a ransomware attack. This model also looks for signs of encryption and computes an encryption probability.

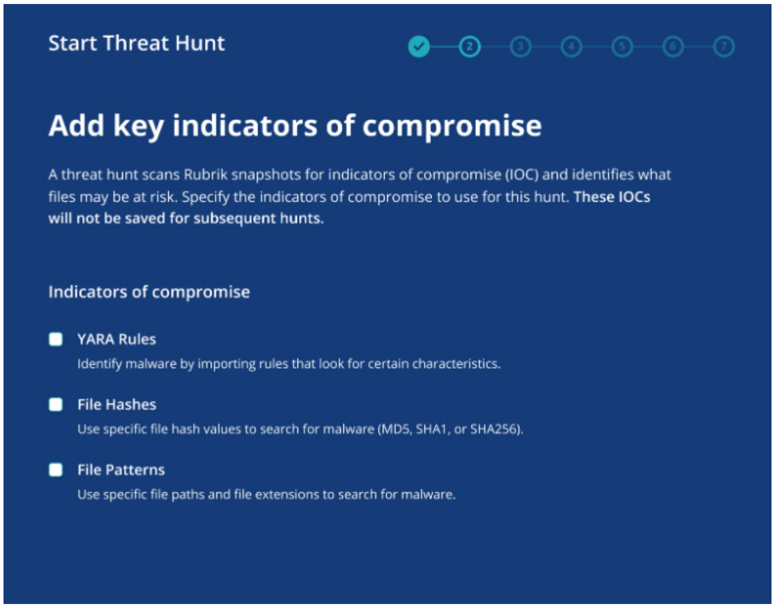
Every time you perform a backup, Rubrik applies its machine learning approach to look for signs of ransomware and other anomalies, enabling you to detect attacks and initiate recovery more quickly.

Threat Monitoring & Hunting

Rubrik Threat Monitoring & Hunting is designed to help you spot malware and avoid reinfection. It searches your backups without the need to recover data, enabling you to look back in time at your VMs and file sets to help pinpoint when an infection started and to avoid reinfection during recovery.

Rubrik Threat Monitoring & Hunting enables you to:

- **Discover threats.** Rubrik analyzes backup data and provides insights that help avoid malware reinfection.
- **Find the malware.** Scan backups using file patterns, file hashes, and YARA rules to look for key indicators of compromise across all objects in the backup.
- **Establish a safe recovery point.** Analyze a time series history of backup snapshots to pinpoint the best snapshot(s) to restore.
- **Document evidence for investigations.** Leverage insights from IOC scans to provide evidence during internal and external cyber investigations.



Start Threat Hunt

Add key indicators of compromise

A threat hunt scans Rubrik snapshots for indicators of compromise (IOC) and identifies what files may be at risk. Specify the indicators of compromise to use for this hunt. **These IOCs will not be saved for subsequent hunts.**

Indicators of compromise

□ **YARA Rules**
Identify malware by importing rules that look for certain characteristics.

□ **File Hashes**
Use specific file hash values to search for malware (MD5, SHA1, or SHA256).

□ **File Patterns**
Use specific file paths and file extensions to search for malware.

Rubrik Threat Monitoring & Hunting differs from competing solutions because it has no impact on your production environment. It can process multiple rules across multiple points in time, and an intuitive UI eliminates the learning curve that comes with other products, making it possible to execute complex searches and achieve greater insight in less time.

Data Recovery

Data Recovery

Your business operations are recovered within hours

If your organization suffers a ransomware or other cyber attack, you need recovery to proceed as quickly and easily as possible. Recovery is where a ransomware solution really proves itself. Unfortunately, many backup solutions come up short when it comes to ransomware recovery:

- **Different recovery approaches** may be needed for data center vs. cloud vs. SaaS recovery.
- **Threats aren't quarantined** from the active backup set.
- **It is difficult to recover data** at file, user, object, or system level.
- **Success is uncertain** and restore times are long.

Rubrik Zero Trust Data Security enables you to quarantine malware and automate recovery to restore business operations in less time and with far less uncertainty. Rubrik provides:

- **Threat Containment.** Quarantine data to prevent reinfection.
- **Mass Recovery.** Identify affected data and initiate recovery in minutes.
- **Orchestrated Application Recovery.** Recover apps and data quickly and easily with guided workflows.

Threat Containment

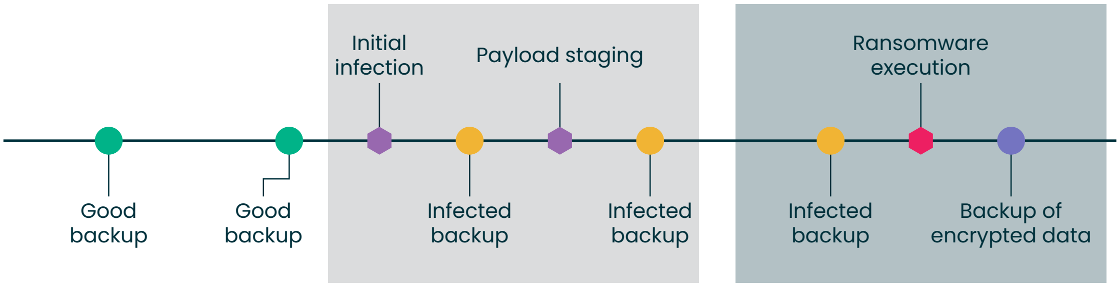
Sometimes your organization may find clues pointing to ransomware attacks in progress, such as suspicious emails, communication with external IP addresses associated with threat actors or botnets, or known malware. The earlier you detect and contain an attack, the less impact it will have on your operations and the faster you can recover.

Containing ransomware attacks is important for two reasons. First, attackers often continue to extend their reach and encrypt new systems even after encrypting an initial set of systems and declaring their presence. Second, some of the steps involved in containment can prevent attackers from coming back and launching a new attack.

Analyze Threat Impact

Rubrik continuously scans your entire environment to provide insights on how your data is changing over time. In the event of an attack, you can quickly identify which applications and files were impacted and where they are located through simple, intuitive visualizations. Using the UI, you can browse through the entire folder hierarchy and drill down to investigate what was added, deleted, or modified at the file level. Rubrik helps you minimize time spent discovering what happened and provides granular visibility into the files affected.

Rubrik operators can pause all access and activities in the event of compromise or threat. This gives you the ability to contain affected data, so it does not reinfect the environment. Rubrik enables you to scan for Indicators of Compromise (IOCs) on multiple systems and across time to provide insights from system and data backups, helping you identify clean backups for recovery.

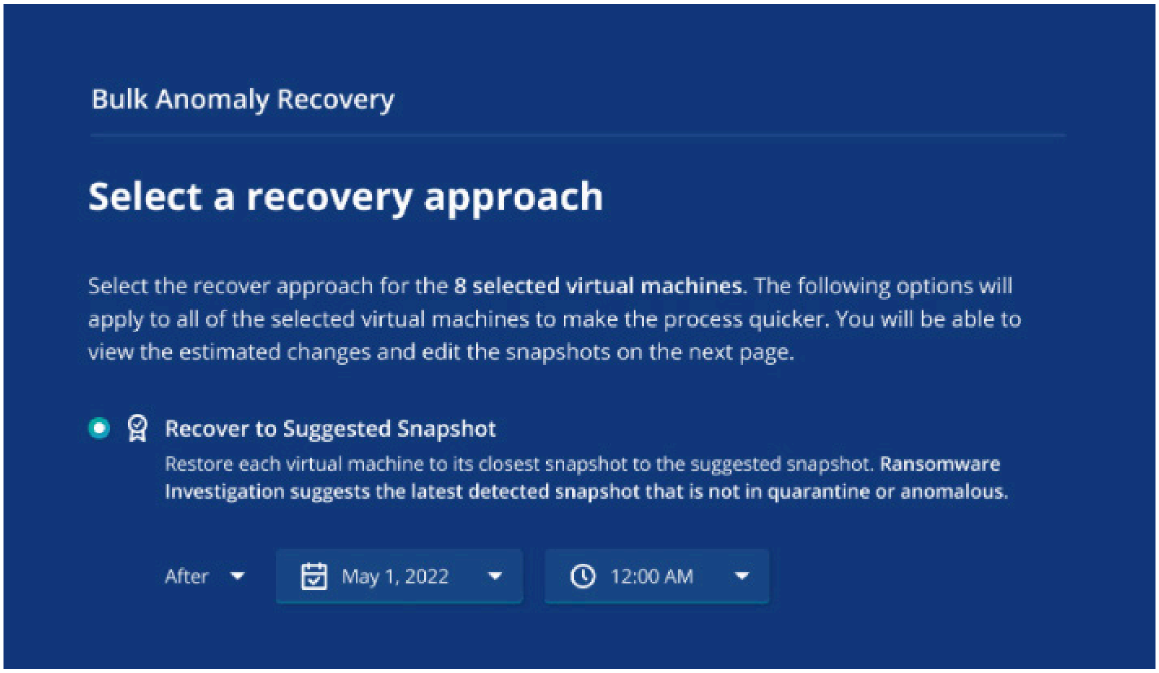


Mass Recovery

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 to meet your stringent recovery time objectives.

With Rubrik Mass Recovery you can:

- **Minimize downtime.** Recover hundreds of VMs or restore tens of thousands of files to a clean state in minutes.
- **Avoid reinfection.** By identifying files and applications infected by ransomware, Rubrik enables you to quickly identify a clean snapshot and recover your data with no reinfection.
- **Recover only what you need.** Recover only the data that has been compromised with guided workflows for file-level, object-level, application-level, and system-wide restore.



Bulk Anomaly Recovery

Select a recovery approach

Select the recover approach for the **8 selected virtual machines**. The following options will apply to all of the selected virtual machines to make the process quicker. You will be able to view the estimated changes and edit the snapshots on the next page.

● Recover to Suggested Snapshot

Restore each virtual machine to its closest snapshot to the suggested snapshot. **Ransomware Investigation suggests the latest detected snapshot that is not in quarantine or anomalous.**

After ▾ | May 1, 2022 ▾ | 12:00 AM ▾

Many ransomware recoveries proceed slowly because they depend on the expertise of one or a few “experts” within your organization to determine how to decide on a plan and carry out restores. Rubrik’s mass recovery wizard uses machine learning technology to quickly identify the latest clean snapshot(s), and enables your team to execute smooth mass recovery operations without relying solely on internal experts or requiring a lot of specialized knowledge and skills.

Orchestrated Application Recovery

Ensuring security and resiliency for data and business services in the face of cyber attacks and other disaster events is a critical responsibility. Executing manual recovery plans for applications with multiple tiers and interdependencies slows down the recovery process and introduces opportunities for error.

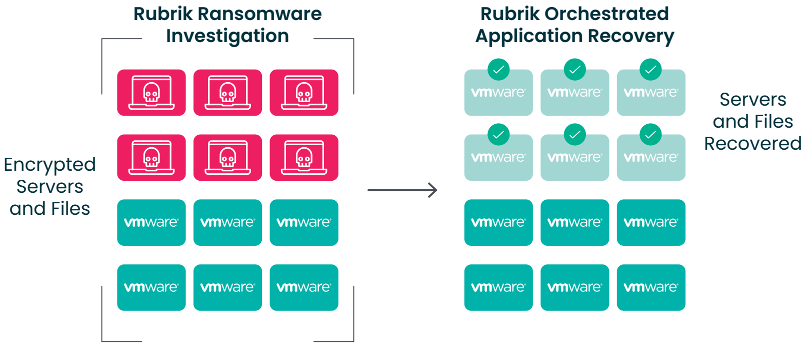
Rubrik Orchestrated Application Recovery is a tightly integrated and automated recovery service that provides orchestration of DR failover/failback and testing. It leverages application-focused Ransomware Monitoring & Investigation that radically simplifies recovery.

Rubrik utilizes application Blueprints that contain information on an application's VM recovery sequence and resource mapping configurations (compute, storage, and network) to provide application-level orchestration.

For example, suppose you have a three-tier application with a web server front end, a middleware server, and a backend database. A Blueprint recovery allows you to individually roll back the necessary servers to a clean state. Depending on the date of infection, you could roll back your middleware server to 2 days ago, and roll back your front and back ends to 3 days ago. Blueprints can encompass hundreds of VMs for recovery at scale, with groups of Blueprints making up a Recovery Plan to enable failover for an entire datacenter.

Using Blueprints, you can failover to your on-premises DR site or a public cloud with just a few clicks. When you are ready, failback to your on-premises data center while continuing your existing snapshot chains and CDP recovery points to maintain SLA compliance throughout the event.

When combined with Rubrik Ransomware Monitoring & 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.


Rubrik Ransomware Investigation
Encrypted Servers and Files
vmware
Rubrik Orchestrated Application Recovery
Servers and Files Recovered

For more on Orchestrated Application Recovery, see the white paper, *An Introduction to Rubrik Orchestrated Application Recovery*.

It’s Time for Zero Trust

The message from security experts and the highest levels of government is clear—the bad guys are getting through traditional security defenses, and they are targeting your backup data as a growth strategy. If you haven’t done so already, it is time to rethink your data protection strategy, create new backup and recovery requirements based on Zero Trust principles, and make the necessary IT investments to secure your data and help ensure your organization never has to pay a ransom.

Rubrik Zero Trust Data Security provides the essential capabilities to protect your backup environment against ransomware attacks while ensuring that you can accelerate recovery. Rubrik helps you reduce the risk of intrusion and secure your backup data in an immutable form while also making it much simpler to detect anomalous behavior and enforce compliance with important laws, regulations, and policies.

Rubrik also offers a unique Ransomware Recovery Warranty to provide further peace of mind. To find out how Rubrik can help you enhance the security of your data protection environment, with maximum protection from hackers and fast recovery from ransomware attacks, rubrik.com/ransomware

Additional Ransomware Resources

And be sure to check out our complete set of ransomware-related resources (registration required):

- Framework for a Comprehensive Ransomware Recovery Plan
- Best Practices Guide: Prepare and Recover from a Ransomware Attack with Rubrik

rubrik

Zero Trust Data Security™