rubrik | Zero Trust Data Security™

Definitive Guide to Zero Trust Data Security

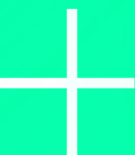# Table of Contents

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 security defenses, attackers continue to gain access to valuable business data.

- **Traditional backups are now vulnerable.** While backups are the last—and most important—line of defense against ransomware, sophisticated attackers know this too. Many ransomware attacks now 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 the 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 in detail, describing how Rubrik delivers maximum protection from hackers and fast recovery from ransomware attacks.

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.

So, what does Zero Trust look like? Rubrik adheres to the model defined by the National Institute of Standards (NIST), which is defined by the NIST SP 800-207 Zero Trust Architecture Specification. As NIST puts 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
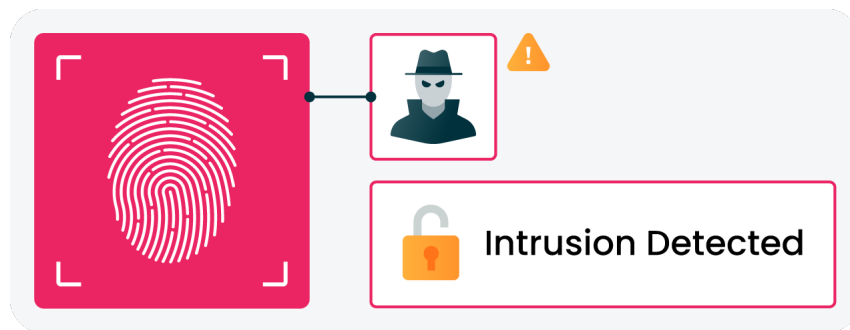
The first line of defense in Zero Trust is preventing intruders from gaining access in the first place. NIST defines intrusion as a security event where *"an intruder gains, or attempts to gain, access to a system or system resource without having authorization to do so."* Note that an intruder may be an outsider or someone from within your own company.

There are multiple methods to reduce intrusion risk:

- **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.

Secure Backup Data

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 can 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 or Abnormal Activity

Another important line of defense for any organization facing a ransomware attack 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 assets ahead of time. 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.

Full ransomware protection should also include the ability to contain any incidents that occur and return to normal operations quickly.

Contain Incidents & Recover 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 always 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 sections that follow describe the technologies that underlie Rubrik Zero Trust Data Security, beginning with a comprehensive look at Rubrik's Zero Trust Data Protection.

Zero Trust Data Protection		Ransomware Investigation		Sensitive Data Discovery		Incident Containment		Orchestrated Application Recovery
	+		**+**		**+**		**+**	

Zero Trust Data Protection

Safeguard Your Data against Any Threat

Rubrik Zero Trust Data Protection builds on the principles of Zero Trust to secure your data with:

- Intrusion Control
- A secure data layer

API Gateway
Policy Engine
Threat Engine
Immutable Data Platform
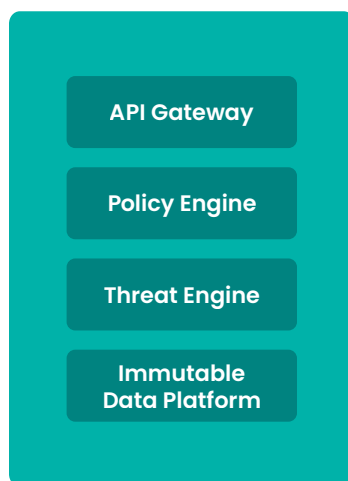
The foundation of the Rubrik Zero Trust Architecture is a core set of technologies that set Rubrik apart from legacy backup solutions. It is purpose-built to fortify your data from the inside out to support fundamental use cases and to answer your most pressing security-related questions:

Are our backups secure and resilient?
The Rubrik immutable data platform makes backups tamper-proof.
Once ingested, no external or internal operation can modify the data. Even during a Restore or Live Mount operation for recovery, data managed by Rubrik is never available in a Read/Write state to the client.

And since Rubrik does not allow data to be overwritten, if infected data is ingested it cannot infect other files or folders. This level of protection is only achievable because the Rubrik purpose-built filesystem and logical air gap prevent malicious manipulation of your data and block data from being discoverable or accessible over the network.

Is our data in compliance with data lifecycle policies?
The Rubrik declarative policy engine automates the data lifecycle. (Watch this video for an introduction to Rubrik's policy engine.) Rubrik allows administrators to avoid the complexity that's usually required to build and maintain data protection, so they can focus on adding strategic value. Because imperative details are abstracted away and handled by an intelligent scale-out system, the Rubrik policy engine is elegantly simple. Required inputs are reduced to just RPO, retention period, archive target, and replication target. The Rubrik policy engine also grants least-privilege access based on a user's specific role using granular RBAC.

What is in our data? What are users doing with our data?

The Rubrik threat engine lets you actively monitor sensitive data. As each backup snapshot's metadata is collected, machine learning is used to build out a full picture of what is happening with the workload. The network is trained to identify trends across all samples and classify new data based on similarities with existing data using supervised learning without human input. In addition, all traffic is logged and inspected as a countermeasure against malicious data access and manipulation. The result is that Rubrik detects anomalies, analyzes threats, and helps accelerate recovery with multiple expert-guided recovery options, enabling your team to quickly recover any files or workloads affected by an attack.

Can operations be automated securely?

A secure, API-first architecture integrates with your technology stack and accelerates service delivery. With the Rubrik API-Driven Architecture, every action in the Rubrik UI has a corresponding API documented and available for use. If you can perform a task through the Rubrik UI, you can do the same thing programmatically through a secure API that is protected by role-based access and API tokens.

Attackers are getting smarter and going straight for your backup data. By securing the data itself, Rubrik provides a last line of defense.

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 user, employee, and service accounts.
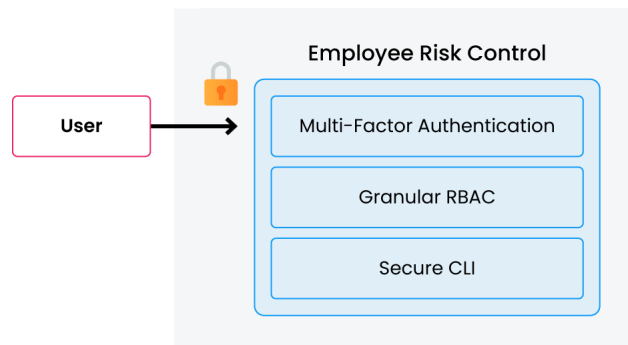
Multi-Factor Authentication

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.
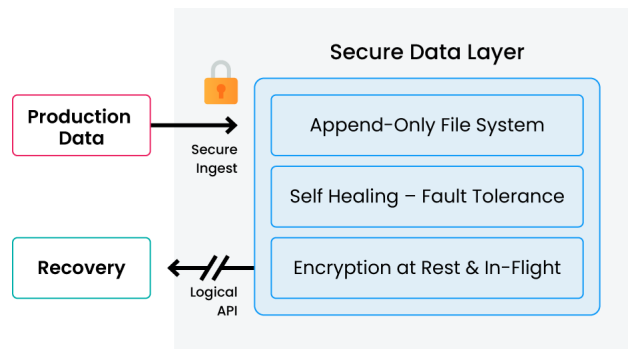
Factory Reset is Disabled

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.

Secure Data Layer

Production Data → Secure Ingest → Append-Only File System

Self Healing – Fault Tolerance

Recovery ← Logical API ← Encryption at Rest & In-Flight

Air Gap　　　**Immutability**　　　**Retention Lock**　　　**Data Encryption**

Encryption

Data managed by Rubrik is always encrypted. Whether at rest, or in-flight between sites or clouds, 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
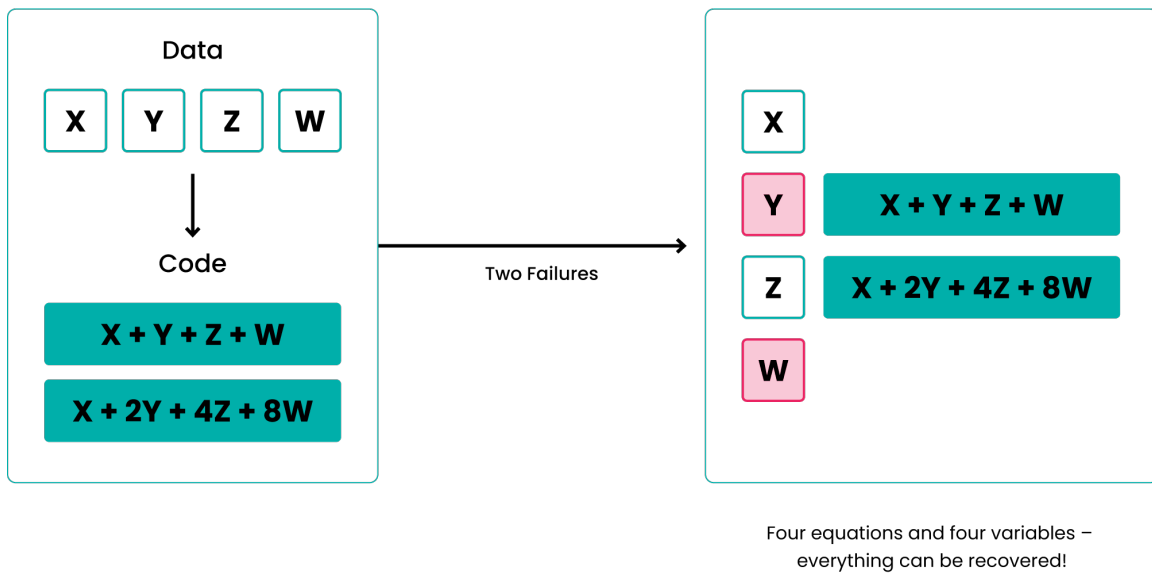
desired data sets and then plan for and manage the additional data usage. Rubrik does that all natively and transparently.
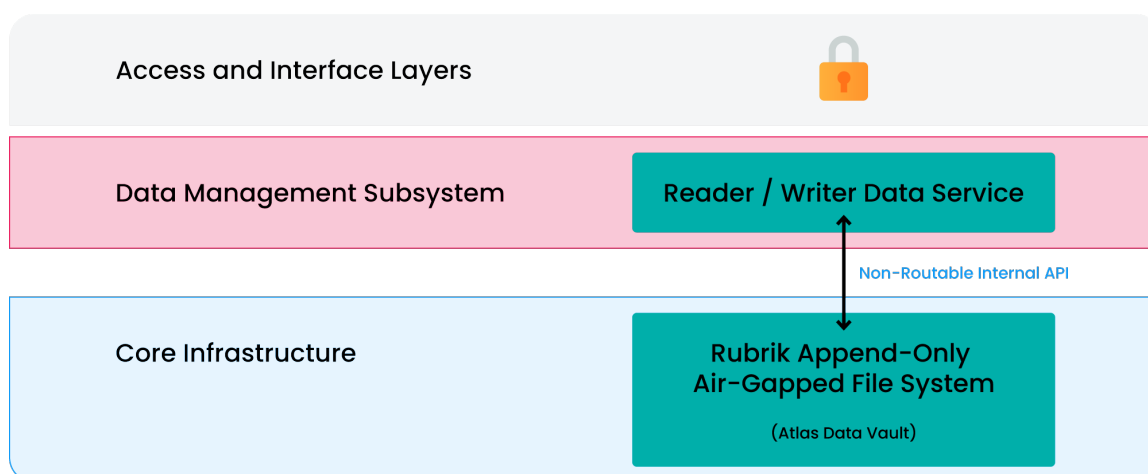
Zero Trust cluster design. With the Rubrik Zero Trust cluster design, operations within a cluster can *only* be performed through authenticated APIs. Other cluster designs rely on a *full-trust* model in which all members of a cluster are able to communicate freely with one another. In some cases, this 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.

Data

| X | Y | Z | W |

↓

Code

X + Y + Z + W

X + 2Y + 4Z + 8W

Two Failures →

X

Y   X + Y + Z + W

Z   X + 2Y + 4Z + 8W

W

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.

Ransomware Investigation

Discover Data Anomalies with Machine Learning

Rubrik understands that a ransomware attack is one of the worst-case scenarios. An impacted customer will likely be dealing with widespread business and logistics issues caused by the attack. Rubrik has developed a set of best practices to help you plan for, identify, and remediate ransomware attacks.

Built-in ransomware investigation capabilities, can help you discover attacks quickly so they can be contained. Rubrik utilizes machine learning-based anomaly detection to discover potential threats automatically. The solution can also scope the blast radius of an attack and make recommendations about the best possible recovery points. API-integration with popular security operations tools enables strong collaboration between IT and security groups for faster incident response.

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 ransomware recovery decision-making process.

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. A deep neural network (DNN) is used to build out a full perspective of what is going on with 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 goes deeper to look for signs of encryption and compute an encryption probability.

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

Sensitive Data Discovery

Classify Data and Assess Exfiltration Risk

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.

Discovery, classification, and reporting have zero impact on your production environment. Existing Rubrik deployments can 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 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 can be run 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.

Incident Containment
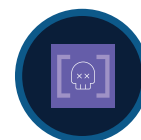
Quarantine Data to Prevent Reinfection

Sometimes organizations 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 will 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 Ransomware Investigation can continuously scan the 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. Ransomware Investigation 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 can help you 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.
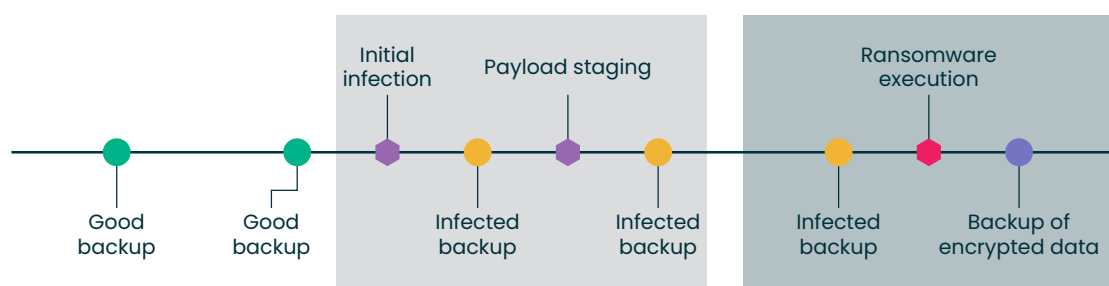
Orchestrated Application Recovery

Recover Apps & Data with Guided Workflows

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 DR service that provides orchestration of DR failover/failback and testing. It includes application-focused ransomware remediation that radically simplifies recovery.

Orchestration utilizes application blueprints which group together objects (in this case VMs) providing a timeline view for each server used in an application. Blueprints contain information on an application's VM recovery sequence and resource mapping configurations (compute, storage, and network) to provide management simplicity and application-level orchestration.

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. For example, 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. Granular recovery capabilities ensure you recover with the least amount of data loss. Since blueprints are unbounded, they can encompass hundreds of VMs, enabling granular recoveries at scale.

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's ransomware investigation and incident containment using Ransomware Investigation, 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. From that point, Orchestrated Application Recovery automates the rest of the restore process, enabling your team to track the progress through the UI.

Rubrik Ransomware Investigation

Encrypted Servers and Files

Rubrik Orchestrated Application Recovery

Servers and Files Recovered
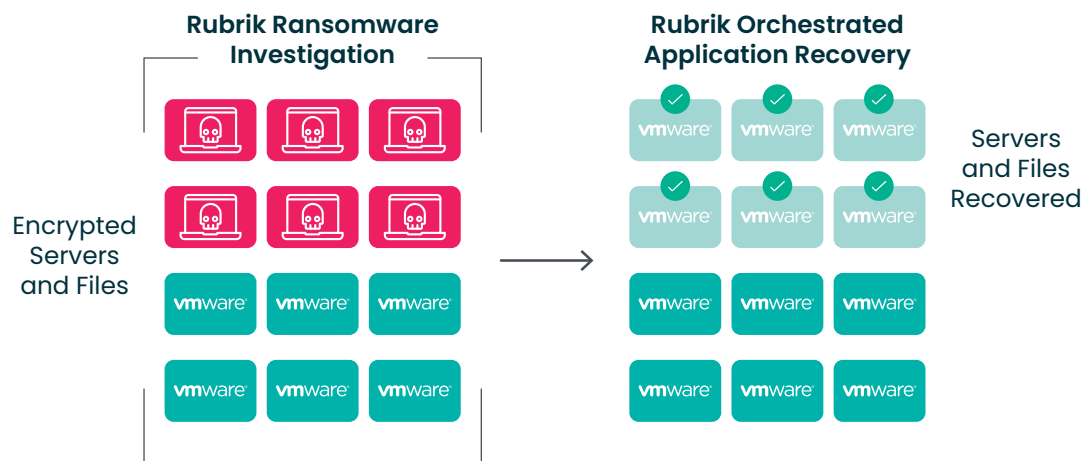
It's Time for Zero Trust

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, to create new backup and recovery requirements based on Zero Trust principles, and to 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 critical capabilities that are essential 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/industry-first>> 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, visit 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

Trust Nothing. Always Verify.