WHITE PAPER

Best Practices Guide: Prepare and Recover from a Ransomware Attack

Rubrik Technical Marketing

November 2025

Table of Contents

3 THE NEED FOR CYBER RESILIENCE

- 3 Cyber Resilience
- 3 Cyber Recovery Time Objectives (Cyber RTO)
- 3 Zero Trust Data Security™
- 5 Secure By Design

5 SECURE DEPLOYMENT BEST PRACTICES

5 RECOVER FROM RANSOMWARE ATTACKS WITH RUBRIK

- 6 Rubrik Solution Overview
- 7 Rubrik Ransomware Response Team
- 8 Preparation
  - 8 Build a Plan
  - 9 Prioritize Critical Data and Systems
  - 10 Ensure Clean Recovery
  - 10 Know Your Application Recovery Strategy
  - 11 Test Your Plan
- 11 Detection and Analysis
  - 11 Determine Blast Radius
  - 12 Isolate Infected Systems
  - 12 Notify Stakeholders
  - 13 Assess and Neutralize
- 14 Containment, Eradication, and Recovery
  - 14 General Best Practices
  - 15 File-only Recovery
  - 15 Virtual Machine and Database Recovery
  - 16 Active Directory Recovery
  - 17 Hypervisor Manager Recovery
  - 18 Orchestrated Recovery

18 KEY RUBRIK SECURITY TECHNOLOGIES

- 18 Native Immutability
- 19 SLA Retention Lock
- 19 Quorum Authorization
- 19 Intelligent Data Lock
- 20 Legal Hold
- 20 Multi-Factor Authentication

20 RUBRIK SECURITY SOLUTIONS

- 20 Rubrik Security Cloud
- 21 Rubrik Secure Vault
- 21 Rubrik Cloud Vault
- 22 Rubrik Data Threat Analytics
  - 22 Anomaly Detection
  - 23 Threat Monitoring
  - 23 Threat Hunting
    - 23 Turbo Threat Hunting
    - 23 Advanced Threat Hunting
  - 23 Threat Containment
- 24 Rubrik Data Discovery and Classification
- 25 Rubrik Orchestrated Recovery

25 APPENDIX

- 25 Resources

Any unreleased services or features referenced in this presentation are not currently available and may not be made generally available on time or at all, as may be determined in our sole discretion. Any such referenced services or features do not represent promises to deliver, commitments, or obligations of Rubrik, Inc. and may not be incorporated into any contract. Customers should make their purchase decisions based upon services and features that are currently generally available.

THE NEED FOR CYBER RESILIENCE

As ransomware attacks continue to increase in volume and sophistication, Rubrik customers can quickly and effectively recover their data to minimize damage to their business. This guide will explain Rubrik Zero Trust Data Security™ and how its built-in capabilities make secured data immune to ransomware. You'll also learn about deployment best practices that make it even more challenging for cybercriminals to attack, recommended recovery processes, and a description of the unique solutions Rubrik provides to protect customer data.

CYBER RESILIENCE

Cyber resilient organizations are prepared to anticipate, withstand, and recover from cyberattacks. They focus equally on prevention, detection, and quick recovery, understanding that defense in depth is key, but that incidents are still likely to occur. Key elements of cyber resilience include reducing risk by understanding threats and vulnerabilities, minimizing impact through techniques like segmentation and encryption, and optimizing recovery with robust data protection, proactive threat detection and orchestrated workflows.

CYBER RECOVERY TIME OBJECTIVES (CYBER RTO)

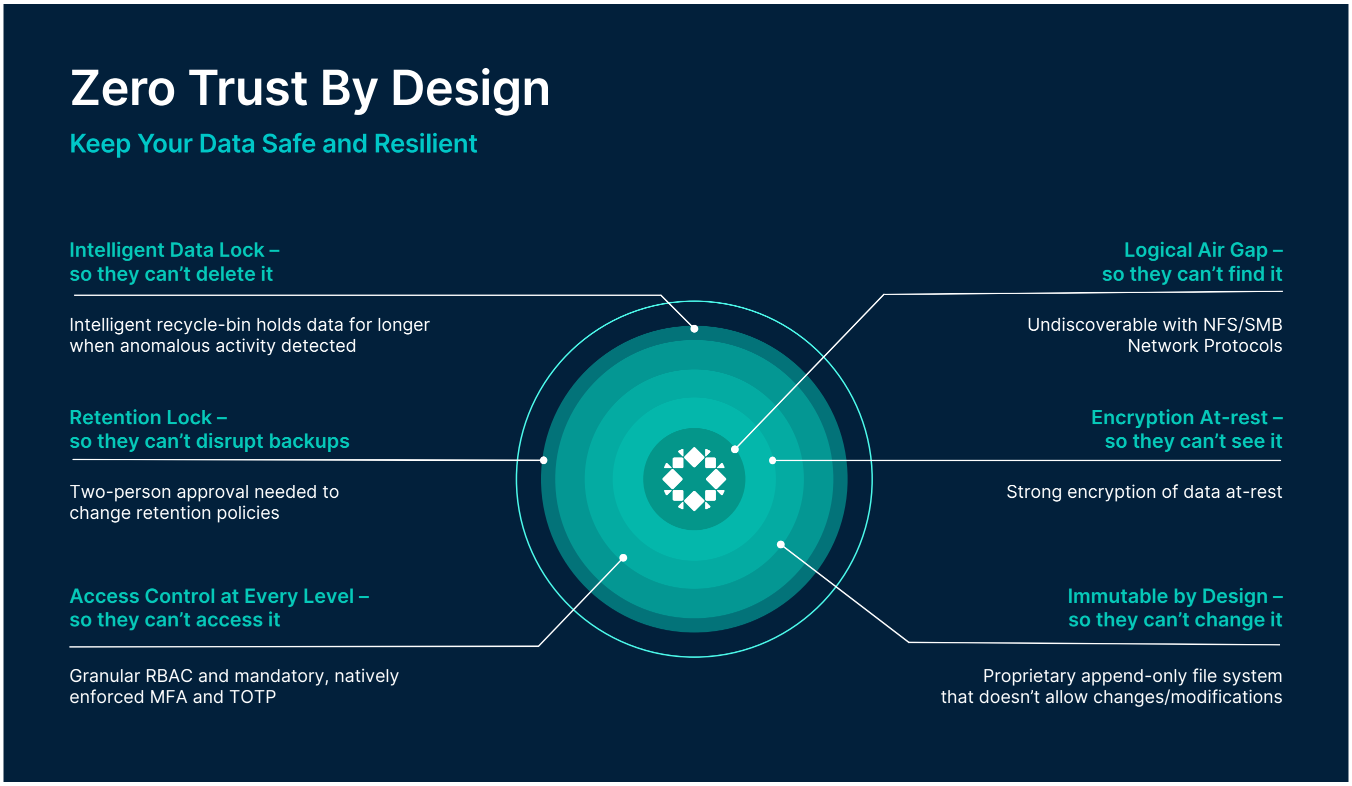
As the final backstop for any cyber incident, rapid recovery is crucial for quickly restoring business operations. But having unaffected backups and finding the clean point in time to recover from is often a major contributor to the long recovery times experienced after a cyber attack.

Cyber Recovery requires strong data protection that does not allow backup snapshots or recovery infrastructure to be vulnerable to disruption during an attack. As part of the recovery process, the ability to discover and surgically prevent recovery of threat artifacts is a key stage in determining how quickly a clean recovery can occur, ideally as part of a highly automated and streamlined recovery process.

Unless all of these elements are in place before the attack, the time to a clean recovery could be slow enough to cause permanent damage to the business. This has been the focus of Rubrik's ransomware protection strategy: to have rock solid protection of backups, to be proactive in the analysis of data to more quickly identify and contain threats, and to orchestrate the recovery to be as fast and consistent as possible.

ZERO TRUST DATA SECURITY™

Zero Trust Data Security™ is the Rubrik proprietary architecture modeled after the Zero Trust architecture from NIST (National Institute of Standards and Technology), discussed in SP800-207. The core architecture of the Rubrik platform is based on this Zero Trust model. It supports a purpose-built file system that never exposes backup data via open protocols. This approach creates a logical air gap that blocks data from being discoverable or accessible over the network.



Zero Trust By Design

Keep Your Data Safe and Resilient

Intelligent Data Lock – so they can't delete it

Intelligent recycle-bin holds data for longer when anomalous activity detected

Retention Lock – so they can't disrupt backups

Two-person approval needed to change retention policies

Access Control at Every Level – so they can't access it

Granular RBAC and mandatory, natively enforced MFA and TOTP

Logical Air Gap – so they can't find it

Undiscoverable with NFS/SMB Network Protocols

Encryption At-rest – so they can't see it

Strong encryption of data at-rest

Immutable by Design – so they can't change it

Proprietary append-only file system that doesn't allow changes/modifications

Rubrik's founders established security as a foundational design principle from the outset of product development. This began with a custom file system engineered to provide out-of-the-box immutability, ensuring that once data is written, it cannot be altered or encrypted by an attack. They also implemented a logical air gap, which protects data by blocking it from being discoverable or accessible over the network, safeguarding it from attackers and rogue administrators.

Once data is written to the Rubrik platform, it cannot be modified or encrypted by an attack, ensuring that a clean copy is readily available for recovery. Additionally, it is possible to enable SLA Retention Lock and Quorum Authorization, which prevent a bad actor from expiring any backup data prematurely and making changes to the environment even if they compromise administrative credentials. Multiple recovery options, including Live Mount and In-Place Recovery, are built-in and available as part of Orchestrated Recovery so IT teams can quickly recover the files and workloads impacted by an attack regardless of whether the recovery is happening surgically back into production or entirely to an Isolated Recovery Environment.

Additional robust protections include role-based access controls (RBAC), stringent API authentication requirements, and the disabling of unused ports to minimize attack surfaces. Rubrik Secure Vault further enhances security through certificate signing, continuously validating the identity of Rubrik services to prevent tampering or compromise. As the threat landscape evolves, Rubrik has integrated more protections, such as native multi-factor authentication (MFA), which is enabled by default and does not rely on third-party solutions. For enterprise environments requiring integration with third-party Identity Providers (IDPs), SAML 2.0 based IDPs are supported, including for MFA. The advantage of native MFA is that it provides a robust defense against compromised accounts in directory services, like Microsoft's Active Directory, without external dependencies, allowing for quicker setup, reduced attack vectors, and the ability to remain secured even when the rest of the environment is down or compromised.

SECURE BY DESIGN

In today's malware landscape, threat actors are increasingly targeting backup infrastructure to exfiltrate sensitive data before launching broader attacks. Google Cloud noted in its H2 2025 Cloud Threat Horizons Report that financially motivated threat actors are increasingly sabotaging cloud backups to maximize leverage in extortion schemes. Notable adversary groups like Scattered Spider are now utilizing attacks against backup jobs and infrastructure as part of their core techniques to increase the likelihood of a ransom payout. This makes a secure-by-design approach, which prioritizes the integrity and isolation of backup data, more critical than ever.

Backup data truly represents the last line of defense and is crucial for recovering from a ransomware attack. Rubrik's secure-by-design methodology simplifies the implementation of a superior security posture for backups and data management by reducing manual efforts post-deployment. This approach, as part of Zero Trust Data Security™, instills confidence in customers that their data is not only safe but also quickly recoverable in the event of an attack.

SECURE DEPLOYMENT BEST PRACTICES

Security is an essential part of any data management system. When security is compromised, attackers can disrupt, steal, and destroy an organization's valuable data. Data management systems are not immune to this type of behavior from attackers. Rubrik protects customers' valuable data by providing features and best practices that ensure security.

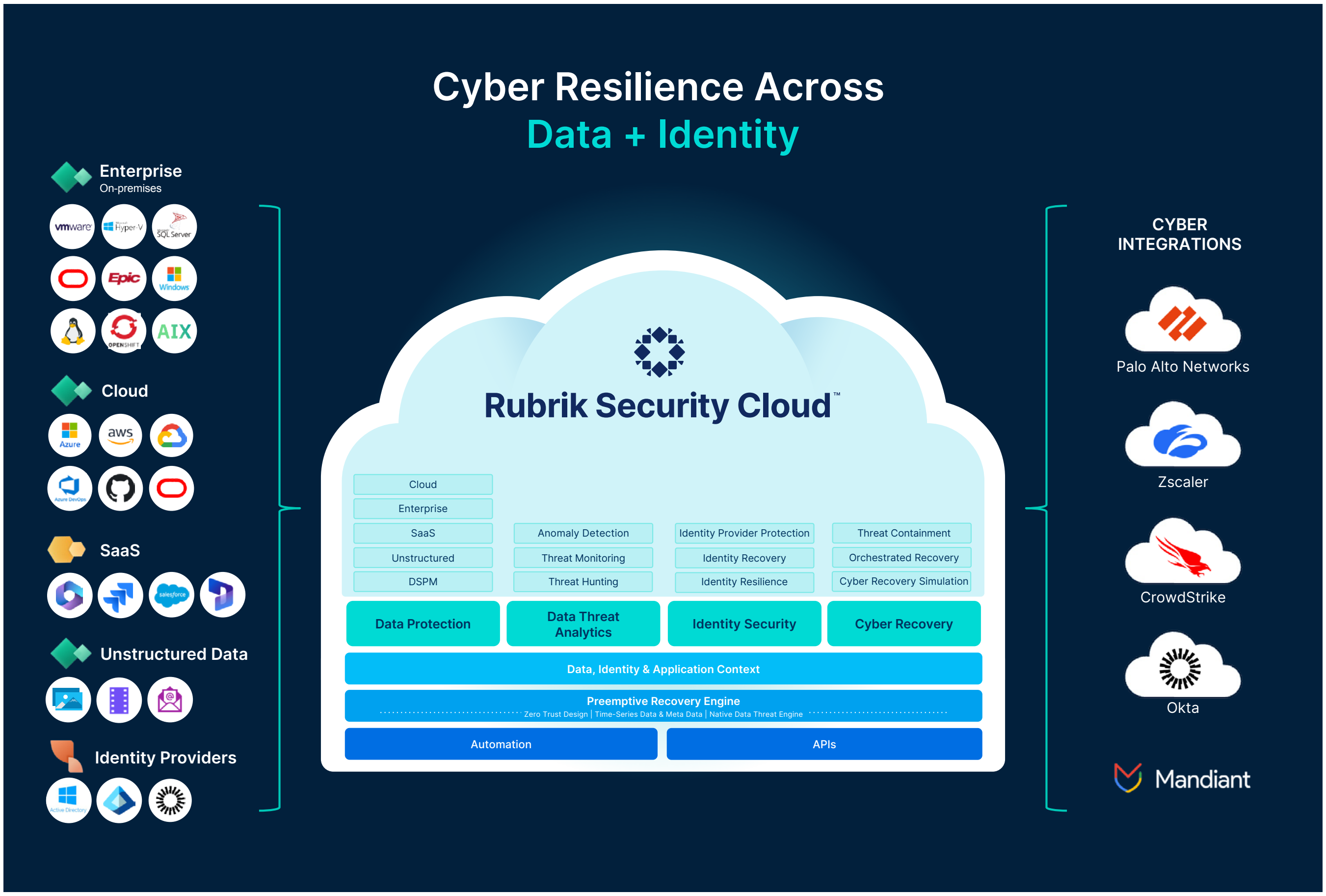
Rubrik maintains extensive Security Hardening Guides that must be followed to secure the Rubrik environment. This approach is necessary to keep bad actors from compromising the Rubrik infrastructure, which must be available and unaffected in order to respond to a ransomware attack. Hardening the Rubrik environment is a must after installation and configuration and before onboarding workloads to be protected. Customers can find additional security hardening guides for self-hosted archive (external) storage (e.g., AWS S3, Azure Blob) on the Rubrik Support portal.

RECOVER FROM RANSOMWARE ATTACKS WITH RUBRIK

As guardians of our customers' data, Rubrik understands that a ransomware attack is one of the worst-case recovery scenarios an organization can face. An impacted customer will likely be dealing with widespread business and logistics issues caused by the attack.

RUBRIK SOLUTION OVERVIEW

Rubrik Solution	Description
Anomaly Detection	**Determine the scope of ransomware attacks faster and easier using machine learning to detect deletions, modifications, and encryptions.** Utilizes machine learning to monitor data and generate alerts for anomalous activity (e.g., file changes, encryption, entropy), quickly identifying snapshots that can be filtered out during recovery to avoid reintroduction of malware. Alerts can be passed along to security tools to help security teams respond to incidents. Includes ransomware strain identification for some of the most common tools.
Data Discovery and Classification	**Reduce sensitive data exposure and manage exfiltration risk by discovering sensitive data captured within backups.** All new backup data is investigated and discovers, classifies, and reports on what types of sensitive data (e.g., PHI, credit card numbers, passport numbers) reside where and who has access.
Threat Monitoring & Hunting	**Prevent malware reinfection by analyzing the history of data for indicators of compromise to identify the initial point, scope, and time of infection.** All new backup data is investigated to automatically identify Indicators of Compromise (IOCs) in new backups. Utilizing this knowledge, precise searches across time can give users the ability to very quickly pinpoint which backups contain an IOC and which ones do not.
Threat Containment	**Ensure safe and quick data recovery by quarantining backup data infected with malware.** Files discovered to be malware, and their associated snapshots, can be easily quarantined. Utilizing role-based access controls, these items can be retained for forensics while preventing accidental recovery and reinfection.
Data Threat Analytics	**A collection of tools for quickly discovering the scope of a cyber attack.** Includes Anomaly Detection, Threat Monitoring, Threat Hunting, and Threat Containment. Together, these tools work proactively to help customer IT and Security teams to detect threats in their data and prevent accidental recovery of these threats.
Orchestrated Recovery	**Recover applications quickly with pre-built workflows and disaster recovery blueprints.** Utilize pre-built workflows and disaster recovery blueprints to automate the recovery of applications and data, integrating with Anomaly Detection and Threat Containment to identify impacted objects and pinpoint safe recovery points. It supports both on-demand and scheduled tests, allowing organizations to validate their recovery plans regularly and build confidence. During a cyberattack the utilization of isolated recovery environments can be used for forensic analysis and secure restoration to prevent reinfection.



RUBRIK RANSOMWARE RESPONSE TEAM

As an industry leader in data security and ransomware recovery, Rubrik handles ransomware attacks as a top priority to facilitate recovery efforts and mitigate further impact. When a customer has been attacked by ransomware, Rubrik engages our Ransomware Response Team (RRT). The RRT provides urgent recovery assistance, continuity, communications, and confidentiality for customer ransomware and cyber incidents.

The RRT is a virtual team of highly experienced individuals built on our award-winning, world-class global support organization, powered and delivered by Rubrik support. RRT is ready and available 24×7×365 and composed of critical incident managers and senior support staff. In addition, Rubrik's executive leadership is part of the virtual team and has clear visibility of every customer engagement RRT is involved with.

RRT's primary mission objective is to partner with and complement our customer's teams, cybersecurity vendors, and any other technology vendors to help with recovery of the environment as quickly and efficiently as possible. RRT provides our customers with the highest levels of urgency, ownership, continuity, communications, and confidentiality regarding incident response and data recovery operations during the event lifecycle. There is no additional cost for RRT engagement—only a valid support contract is required.

Rubrik has already helped many customers successfully recover from ransomware attacks. As a result, Rubrik has developed a set of best practices to help other customers plan for, identify, and remediate ransomware attacks.

PREPARATION

Organizations put themselves in the best position for success when they prepare for a ransomware attack ahead of time. The steps below outline some of the tasks and processes that Rubrik has found to be successful.

Build a Plan

Develop a ransomware response and recovery plan and supporting playbook. A comprehensive plan developed before an attack occurs is critical to a successful outcome. This plan should be updated and reviewed periodically. Additionally, you should store this plan in a secure location that ransomware cannot compromise. A printed copy is suitable for this. Following an established procedure during an attack will limit confusion as everyone will know what to do. Also, a plan that has been tested ahead of an actual incident will help expedite the identification, forensics, and cleanup of the ransomware by enabling the entire response team to react efficiently and effectively.

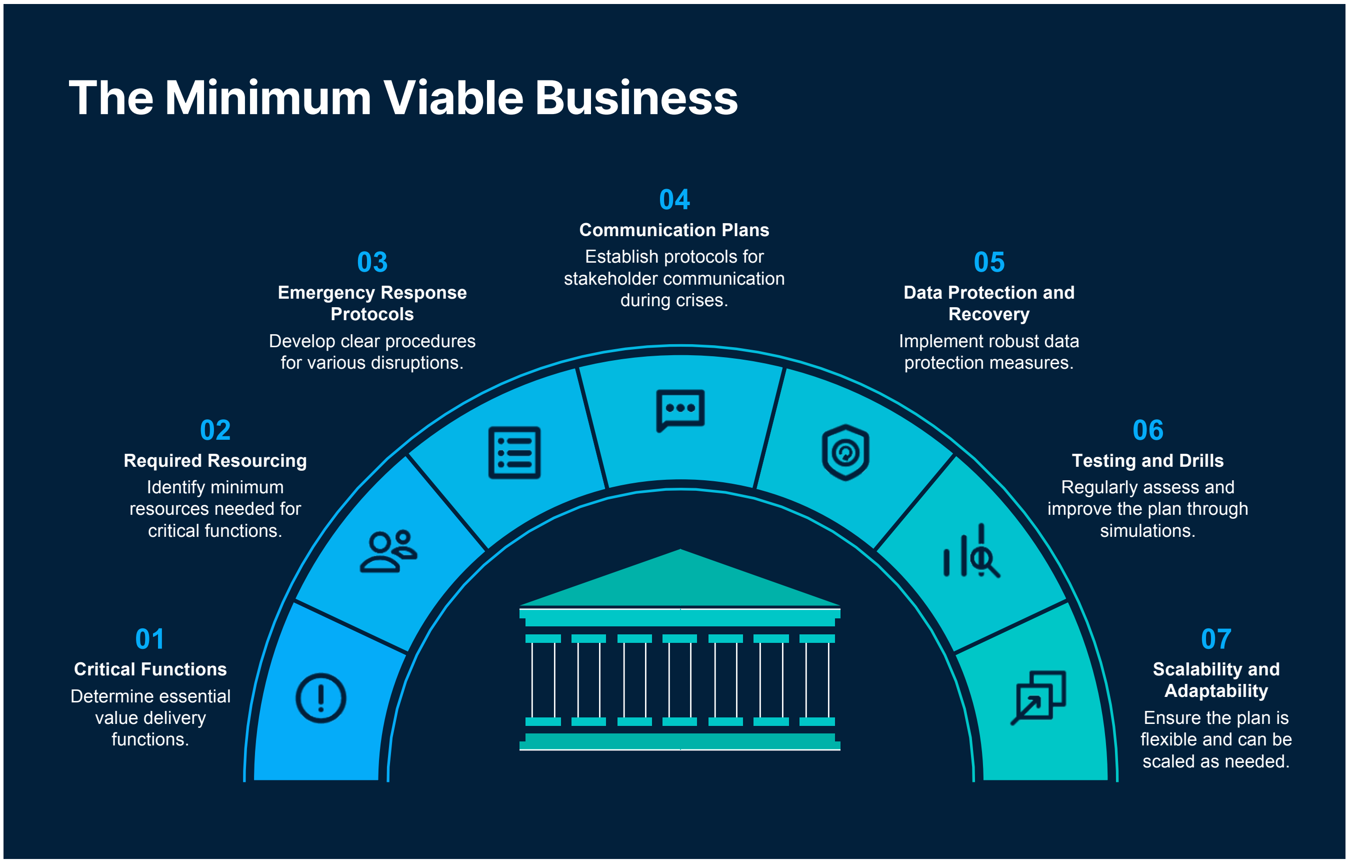
The plan should identify key stakeholders across management, public relations, IT, system/application teams, etc., who will be responsible for executing and managing the incident response. Make sure those people know their responsibilities and how to complete their portion of the recovery plan. A key success factor is timely and thorough internal communication within the affected organization.

The aftermath of a cyber attack is a stressful situation, and it is vital that all concerned parties know their role in recovery. The recovery plan should be tested on a regular basis, to identify any potential gaps or improvement opportunities. A well rehearsed team is in the best position to recover with confidence when the real attack occurs.

Rubrik strongly recommends engaging a reputable, experienced digital forensics and incident response service provider if an attack or suspected attack occurs. These vendors can provide critical assistance with determining the blast radius and neutralizing the attack. Subsequently, they can help with data validation to help orchestrate a safe point in time from which to recover. Your cyber insurance provider may provide this service or recommend a third party for the role.

Finally, the plan should include methods of communication that will be available during a ransomware event. An attack may cause an impact on corporate email and phone systems, so plan for alternate means of communicating both internally and with outside vendors such as Rubrik.

Prioritize Critical Data and Systems
Identify the criticality of each system to the business and any dependencies. Knowing which systems need attention first and how they interact with other business systems will allow a smooth and orderly recovery. This will help you create your business' framework for the Minimum Viable Business.



The Minimum Viable Business

01
Critical Functions
Determine essential value delivery functions.

02
Required Resourcing
Identify minimum resources needed for critical functions.

03
Emergency Response Protocols
Develop clear procedures for various disruptions.

04
Communication Plans
Establish protocols for stakeholder communication during crises.

05
Data Protection and Recovery
Implement robust data protection measures.

06
Testing and Drills
Regularly assess and improve the plan through simulations.

07
Scalability and Adaptability
Ensure the plan is flexible and can be scaled as needed.

A Minimum Viable Business (MVB) is the simplest version of a business that can generate sustainable revenue and validate your business model with real customers. This approach is important because it allows the business to start generating income quickly while testing their core value proposition with minimal investment, reducing financial risk and providing crucial market feedback before scaling.

For example, foundational infrastructure services must be operational before applications and lines of business can be restored. Services in this category typically include Active Directory, DNS, DHCP, NTP, and certificate servers. Based on each system's criticality level, document a recovery plan of which systems would be recovered and in which order.

As crucial as those fundamental services is knowing what sensitive data you have, and where this resides. Rubrik Data Discovery and Classification can provide visibility into this and forms a vital part of the ongoing risk management process and incident response in a ransomware attack.

Ensure Clean Recovery

Implement tools like Rubrik Data Threat Analytics to identify what data has been impacted by ransomware at a file or object level. Having this information during an attack will be invaluable to speeding up recovery and preserving uninfected data. If engaged, determine a safe recovery point with a digital forensics and incident response service provider. Ransomware's impact is felt when the payload is triggered and the data is encrypted. However, the hackers may have been in the system for quite some time beforehand, gathering intelligence, compromising identities, installing malware, establishing command and control, and planning the attack. Furthermore, classifying this data with a tool like Rubrik Data Discovery and Classification will help determine if any of the compromised data is sensitive in nature, along with who has access to it.

Ensure that all critical systems and data are protected in accordance with the required levels of data retention. Here it is better to include all data and exclude as needed rather than only including targeted systems and data. In this manner, all data required for recovery will be in the data protection system. Assigning Rubrik SLA Domains at the top-level of a hierarchy (e.g., vCenter Server, SQL Server) is an excellent way to ensure that existing objects and any objects created in the future are protected.

Know Your Recovery Strategy

Determine the best recovery methods for each application and the various threats to them. For individually deleted, corrupted, or modified files or databases, a file- or database-level restore would be the fastest and least disruptive recovery option. For full VM recovery, Instant Recovery or Live Mount can be used to replace the original VM or create a new VM, respectively, at a previous point in time very quickly by utilizing Rubrik as the storage location. While these methods allow for near instantaneous recovery of storage, these methods create overheads on the Rubrik system and require later migration of the storage layer. Therefore they should only be used on a limited number of recoveries at once.

For larger scale recoveries, Export recovery can be used to create a new VM at a previous point in time by copying the entire VM from Rubrik to the VM storage location. This ensures best performance of the recovered VM, but will cause a delay in powering on the VM while the VM is copied across the network. In-Place recovery can be used to shorten recovery time while also utilizing production storage by copying only the differences between the snapshot on Rubrik and the live VM.

Recovering from a cyber attack could require the full recovery of VMs from many days in the past, which is likely an unacceptable amount of data loss for most businesses. In this case, file level restores from a more recent snapshot could be completed as a follow-up to have more precise recovery of unaffected files with minimal loss of data.

In addition to recovering production, there could be a need to recover systems into an isolated environment. This allows for deeper inspection of systems for threat forensics or to conduct a complete recovery of production in a known-clean environment to prevent reinfection. For this use case Rubrik Cyber Recovery allows recovery into an isolated recovery environment.

A key factor during the Recovery phase is automation, as it minimizes the risk of human error. It also speeds up recovery and aids in progress tracking. With Rubrik Orchestrated Recovery, you can predefine application-level and full data center blueprints that include all the associated resources for unified automated recovery. Rubrik also provides a complete set of APIs and SDKs to help automate recovery. These can be integrated with automation tools such as Ansible, Terraform, Puppet, Chef, PowerShell, and Python. Once a recovery plan and prioritization have been established, automation is the next step in building a more robust recovery capability.

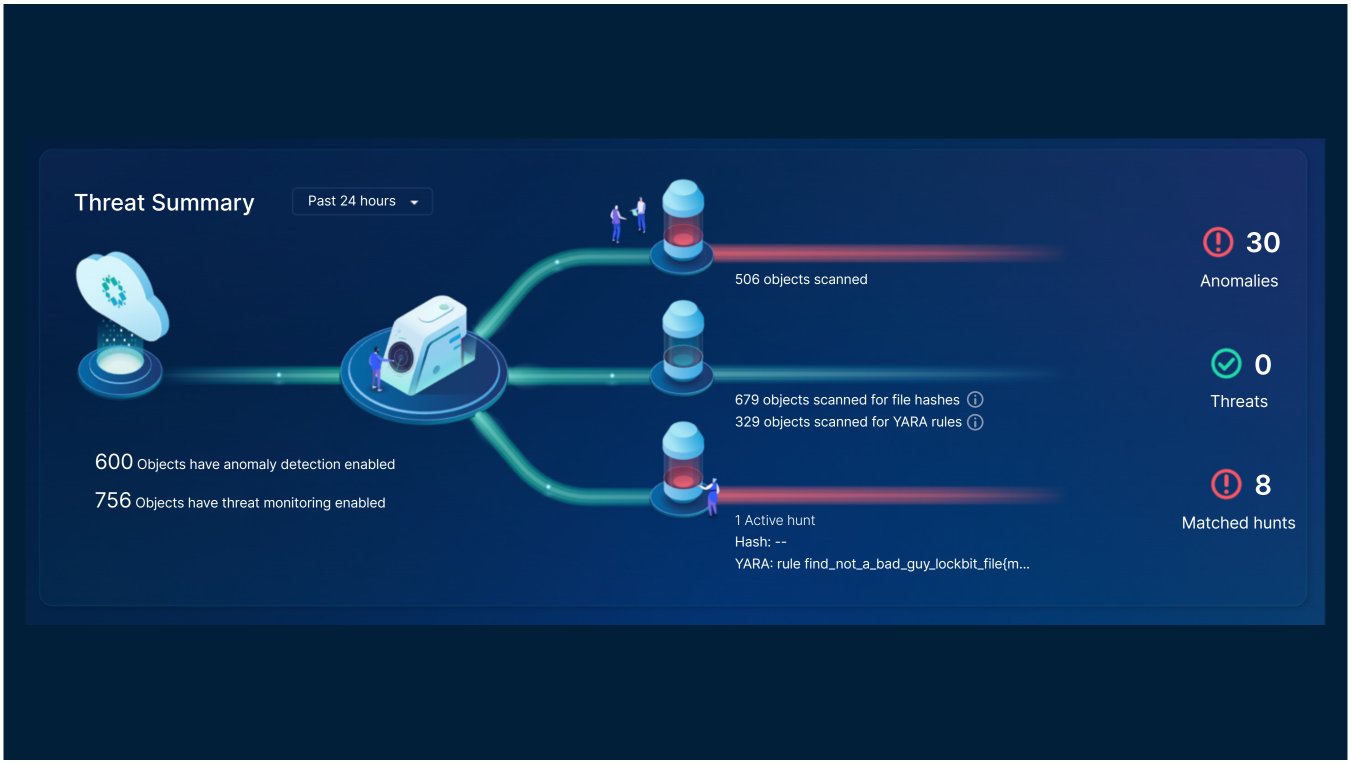
Test Your Plan

Another advantage of automation is to ease the all important task of testing your plan and making periodic test data recovery easier. Without testing the recovery plan, there can be no assurance that it will work when an attack happens. Testing also provides the experience and confidence to staff members that an attack can be successfully and quickly remediated. Tests should be made as realistic as possible without disrupting business operations and performed at planned and unplanned intervals. A more complete automation recovery plan can lead to not only easier and more reliable recoveries, but also more frequent and even regularly scheduled recovery tests.

Equally important to test are the communication and business process reviews. These are generally tested as tabletop exercises. Rubrik offers generic exercises called Save the Data and Zero Hour that can help IT organizations prepare for the unexpected, which can be an invaluable experience to have before the chaotic events caused by an attack.

DETECTION AND ANALYSIS

Determine Blast Radius



Threat Summary

Past 24 hours

506 objects scanned

679 objects scanned for file hashes

329 objects scanned for YARA rules

1 Active hunt

Hash: --

YARA: rule find_not_a_bad_guy_lockbit_file{m...

600 Objects have anomaly detection enabled

756 Objects have threat monitoring enabled

30 Anomalies

0 Threats

8 Matched hunts

Ransomware continues to evolve at breakneck speeds. It is reasonable to suggest that no organization is entirely immune. In fact, assuming you have already been breached is an advisable position. An “assumed breach” mindset requires a “Zero Trust” or “never assume trust, always verify” approach. Even with the best prevention tools, humans are undoubtedly the weakest link, making detecting an attack crucial. Once an attack is detected, determining its blast radius is vital so that you can mitigate damage and recovery can begin.

Rubrik Anomaly Detection helps detect ransomware by analyzing backup data for signals of unusual file system behavior. Rubrik's file system analysis performs behavioral analysis on the metadata, looking at items like the number of files added, deleted, and file system entropy, then reviewing the results for false positives. Once outlier behavior is detected, Anomaly Detection performs file content analysis on the backup to identify if encryption has occurred.

Threat Monitoring and Threat Hunting can also be used to identify the malware itself and other tools utilized by the attackers for things like backdoors, password cracking, and other tools used in the attack chain. Looking back through previous snapshots can help incident response teams identify the general time and location of the first compromise of the environment. This can help teams more quickly identify clean recovery points and narrow down the range of investigation.

A list of the impacted files, their associated probability of being encrypted, and, if identifiable, the likely ransomware tools used is then presented to the user within RSC. Integration with security platforms such as Palo Alto Networks, CrowdStrike, and Microsoft can provide the data insights discovered by Rubrik directly to the Security Operations (SecOps) team to assist their investigations.

Isolate Infected Systems

Systems that are suspected or confirmed to be infected with ransomware should be isolated. This approach will prevent the ransomware from spreading to other systems on the network.

This same approach should be taken with backups to ensure any malware captured in a backup snapshot isn't reintroduced during a restore. It is also recommended to carefully review snapshot expiration to ensure no valid snapshots expire, affecting clean data recovery. You should extend SLAs with near-term retention policies to at least one year for the duration of the ransomware event. Make a note of the original retention periods to reset after the ransomware event is over. Customers can also call Rubrik Support to assist. Rubrik Support and RRT will assess the Rubrik environment upon being engaged to assist with a ransomware attack. They will help to carefully review and secure the Rubrik snapshots and pause any data expiration and garbage collection jobs. Data which may expire under normal circumstances may be vital to the investigation and recovery efforts.

Plan for a scenario where you may need to heavily restrict internet access to prevent an adversary from maintaining command and control of an attack. It is advisable to identify an allowlist of trusted URLs for tooling that would be required in such a scenario. Such a list should include Rubrik Security Cloud, any EDR/XDR provider in use, connectivity to any third party incident response teams, etc.

Notify Stakeholders

As noted earlier, a plan should be pre-established so that all stakeholders can be notified of the ransomware attack and can start to execute their portions of the recovery plan, even if standard corporate communication channels are affected and unavailable. Early notification to stakeholders, Rubrik, and other third-party vendors will allow them to respond even while the attack is still being investigated. Rubrik Support and RRT are pleased to partner with any cybersecurity or other technology vendors in the assessment and data recovery process.

Engage Rubrik Support as soon as possible, and open a priority 1 support case. Even if the event is still in the Investigation or Neutralization phase, Rubrik may be able to assist. The Rubrik RRT will immediately engage and remain so until recovery efforts are completed. The RRT will provide incident management and oversight and the highest urgency, focus, and continuity during the event. Ensure that management, technical stakeholders, and all technology vendors, including Rubrik, are collaborating, communicating, and aligned on priorities, the order of operations, and action items. Please help to ensure all internal and vendor technical stakeholders are copied on all case updates to maintain overall situational awareness. It is best to over-communicate in these situations. Rubrik Support always has the latest attack information and can help should your plan have gaps or encounter an unforeseen situation.

Assess and Neutralize

Ascertain the current status, impact, and scope of the situation. Failing to understand the current position can lead to restoring before the attack is fully neutralized. Doing so can reintroduce the ransomware and reinfect systems, causing more damage and downtime.

In preparation for the recovery process, strongly consider establishing an isolated recovery environment. Rubrik Cyber Recovery can help recover systems into this isolated environment, providing automation and repeatability to the process. This approach allows for restorations to be thoroughly scanned for malware even while the neutralization and/or forensics of the attack is on-going in production. This isolated environment can then be fully validated as clean before releasing into the production environment.

Scoping the attack involves understanding which business functions, systems, identities, and data were compromised. Rubrik Anomaly Detection and Threat Hunting can help determine the blast radius of the attack to be contained, so that only the affected systems need recovering. Otherwise, the safest approach would be to recover all systems and data, leading to more data loss than is necessary due to the rollback of systems unaffected by the attack. Rubrik's insight allows for more surgical recovery, avoiding unnecessary data loss and restoring service more quickly. Rubrik Threat Containment makes it easy to identify clean recovery points and prevent malware reinfection.

Taking assessment one step further, Rubrik Data Discovery and Classification can help determine which sensitive data has been exposed or compromised. Having this information at hand can help prioritize recovery efforts and determine if additional procedures need to be followed and if customers or regulatory authorities need to be notified.

As the scope of the ransomware attack is understood, you must take the appropriate action to stop the spread or reintroduction of the ransomware. If it is necessary to pause protection of affected systems, pause protection on only the compromised infrastructure vs. a blanket pause. Taking this approach will limit the impact to only the parts of the business which the ransomware affected. Consider also pausing expiration of backups until the investigation is completed, and the attack fully remediated. Snapshots of infected machines have value in an isolated recovery environment throughout the investigation of an attack, and it is important that no potential recovery point is aged off until you can be certain that it is no longer required. Reach out to Rubrik Support for help with this.

As mentioned earlier, proper prioritization helps ensure a faster recovery. Once it is clear which systems and data have been affected, prioritize recovery based on the established recovery plan. Doing this will allow those systems and data to be recovered quickly and per the business' needs.

CONTAINMENT, ERADICATION, AND RECOVERY

Before starting the recovery process, it's essential to know what type of recovery is required. If the ransomware only affected files on servers or user shares on a NAS, you can use a file-based recovery method. If, however, the ransomware attacked the virtual disk images for a hypervisor or the master boot records (MBRs) of a physical system, you may need a complete system recovery. The best practices for recovering from each attack are covered here, along with general best practices for all recoveries.

General Best Practices

These best practices apply to all recovery scenarios.

- **Recover safely:** Only begin recovery operations after you have neutralized the ransomware, unless recovering in isolation or to new systems. Restoring systems or data before fully neutralizing the ransomware may result in repeat infection. If the ransomware cannot be isolated and neutralized promptly, the alternative is to recover to an isolated environment, where reinfection cannot occur.

- **Decrypt data:** Recovery may not be necessary if there is a decryptor for the identified ransomware strain available through public or law enforcement channels. When possible, decrypt existing data to prevent data loss. Decryption should occur in a safe environment. If you cannot fully neutralize the ransomware, you may require decryption in isolation.

- **Recover to an isolated environment:** Often, ransomware attacks are so pervasive or preservation of the attack environment is necessary for forensics that recovering back to original locations will only result in secondary attacks. Recovering in an isolated environment where the ransomware did not have access is the best prevention for a secondary attack. During the Preparation phase, you should have identified and tested an isolated environment. During the Recovery phase, use the isolated location to recover data if needed securely.

- **Prioritize recovery:** As planned for in the Prevention phase, recovery will occur based on the prioritization of applications and lines of business. The prioritized list of what to recover and when should come from the Detection & Analysis phase. Ensure that foundational services required for basic functionality, such as Active Directory, DNS, DHCP, NTP, and Authentication, are recovered first. Without these, the other recovered systems may not function properly.

- **Use automation:** Use the tested automation that you developed during the Preparation phase. Automated recovery via automation tools and Rubrik's APIs and SDKs will speed up recovery times. Proven and tested automation will also add to the accuracy of the recoveries. Automation might not be necessary for all types of recoveries. Some examples of where automation can be beneficial are:

  - Recovering NAS systems with tens or hundreds of shares.

  - Recovering complete virtual environments with hundreds or thousands of VMs.

  - Recovering database servers with many databases.

  - Recovering filesets across multiple servers to or near the same point in time.

File-only Recovery

These best practices apply to scenarios where only files and directories need recovering. Consider that malware may lay dormant for some time before executing its payload, and unless you can be 100% confident that this is not the case, a clean OS followed by a file-level recovery is the only safe option.

- **Verify the operating system:** Verify that the underlying operating system was not compromised by the ransomware attack and is trusted. As more organizations begin to leverage build automation, redeployment of the OS from a known clean template may become the easiest route to take.
- **Recover to clean systems:** If you cannot trust the original system, recover files to a known good system. You may newly build this system in isolation or freshly deploy an OS pushed from a known clean template.
- **Identify files for recovery:** Use a tool like Rubrik Data Threat Analytics to identify which files were attacked by the ransomware and recover clean versions of them.
- **Identify sensitive information:** Tools like Rubrik Data Discovery and Classification can help identify which files contain sensitive information. Ensure these files are adequately secured no matter where they are restored. A further forensic examination may be required to validate if this data has also been exfiltrated. If so, you should notify the relevant authorities.

Virtual Machine and Database Recovery

These best practices apply when you cannot use the VM itself. This may happen if the NAS that the VM is running on is compromised. It may also occur if the ransomware renders the VM unbootable. Consider the steps you would take for file-level recovery: can you trust that the guest Operating System does not have a dormant infection? Malware typically lies dormant for some time before the payload is deployed (in the case of ransomware, encryption, or theft of data). If you cannot be confident, deploy a clean operating system and recover at a file or application level. All of this can apply to the hypervisor itself, which is increasingly the vector of attack.

- **When to use Instant Recovery or Live Mount:** (Smaller data sets) Recovery efforts can be sped up by utilizing Rubrik's Instant Recovery or Live Mount recovery options. Both allow VMs and databases to be mounted directly from the Rubrik storage, saving time to copy backups back to primary storage before making resources available. Once mounted, VMs can be moved back to primary storage in the background while providing their regular services. Databases can run in this way until the business can take a planned outage to move the database back to primary storage.

  Instant Recovery and Live Mount are good options for a smaller number of VMs, which may include mission-critical systems. Care should be taken so that the Rubrik Secure Vault resources are not overloaded. Rubrik Secure Vault is not a substitute for primary storage. Also, for VMs, the time and resources required to Storage vMotion VMs back to primary storage are higher. The reason for this is the Storage vMotion protocol and the ability for multiple users to access the VMs simultaneously.

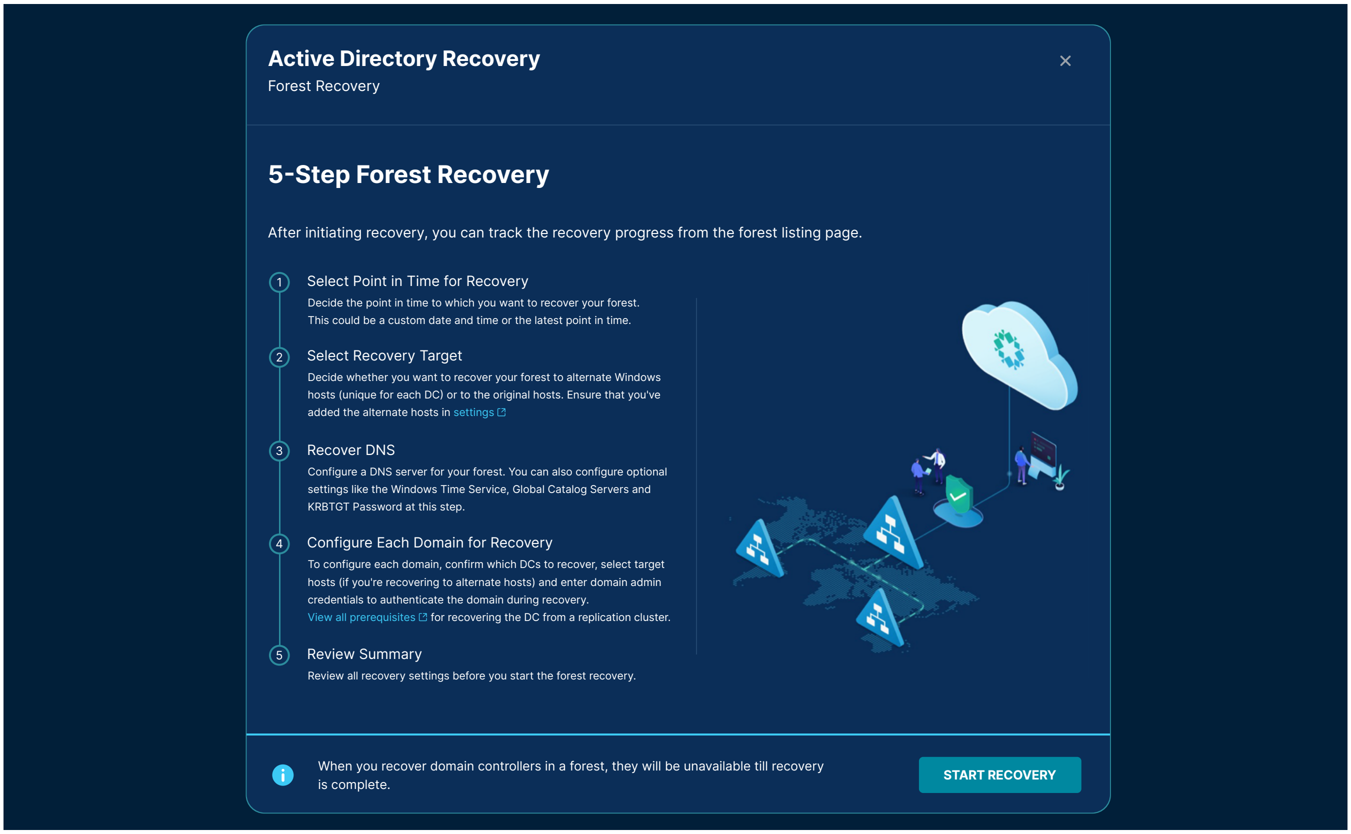
  Instant Recovery and Live Mount are good options for a smaller number of databases because the Rubrik storage is not designed with the same performance characteristics as primary storage. Additionally, databases cannot be Storage vMotioned to primary storage. Instead, they must be shut down during a maintenance window and moved offline. The trade-off of gaining immediate access to the database needs to be balanced against the requirement to move it later.

- **When to use Export:** Rubrik's Export function recovers copies of the database or VM directly to primary storage. Once copied, you can bring the database or VM back online. This method provides the fastest data transfer performance back to primary storage and is best for recovering many VMs. You can use the entire Rubrik cluster's performance to move the data back to primary storage. There is no contention with workloads that are also writing data.

- **When to Mix Instant Recovery or Live Mount with Exports:** Instant Recovery, Live Mount, and Export workloads can be mixed on the Rubrik cluster. You should do this with extreme care. Exports will utilize the full resources of the Rubrik cluster to move data back to primary storage before powering on the workload. VMs running from an Instant Recovery or Live Mount will contend with the files that are being Exported. This congestion may cause degraded performance in the databases and VMs that have been Instantly Recovered or Live Mounted. Mixing workload recovery methods should be evaluated on a case-by-case basis.

Active Directory Recovery

Microsoft's Active Directory is a widely used, distributed directory service that forms the fundamental platform underlying many enterprise environments. It provides authentication services, usually provides DNS and NTP, and may also provide the underlying Public Key Infrastructure (PKI) and DHCP in many environments. It is also one of the infrastructure components most commonly utilized by cyber attackers as part of the attack chain. Due to these factors, it is typically one of the first pieces of infrastructure that needs to be recovered, while also being one of the most suspect.



Active Directory Recovery

Forest Recovery

5-Step Forest Recovery

After initiating recovery, you can track the recovery progress from the forest listing page.

1. Select Point in Time for Recovery
   Decide the point in time to which you want to recover your forest. This could be a custom date and time or the latest point in time.
2. Select Recovery Target
   Decide whether you want to recover your forest to alternate Windows hosts (unique for each DC) or to the original hosts. Ensure that you've added the alternate hosts in settings
3. Recover DNS
   Configure a DNS server for your forest. You can also configure optional settings like the Windows Time Service, Global Catalog Servers and KRBTGT Password at this step.
4. Configure Each Domain for Recovery
   To configure each domain, confirm which DCs to recover, select target hosts (if you're recovering to alternate hosts) and enter domain admin credentials to authenticate the domain during recovery.
   View all prerequisites for recovering the DC from a replication cluster.
5. Review Summary
   Review all recovery settings before you start the forest recovery.

When you recover domain controllers in a forest, they will be unavailable till recovery is complete.

Active Directory relies on multi-master data replication (not only for the Active Directory Domain Services database but also Distributed File Services). Because of this, you must ensure that you do not just add a recovered Domain Controller back to an environment where the infection is still active. If malware is still present, you may find yourself in a vicious cycle of recovering only to have your recovered server re-infected. Recovering into a clean-room environment and scanning each workload for infection before connecting to the network is an excellent way to avoid this. Once confirmed to be clean, you can rebuild your corporate network in a known good state. In addition to recovering your existing Domain Controllers using VM restore capabilities, Rubrik also offers an Active Directory Object Recovery Tool in the event of a need to retrieve individual objects or metadata.

When the infiltration or damage from a cyberattack is so complete that a complete recovery of the domain or forest is necessary, Rubrik's Active Directory Forest Recovery can automate all the documented best practice steps to improve recovery time through automation and eliminating rework due to failed steps. This can have a significant impact on getting the very first part of a complete recovery done quickly.

When connected to Entra ID, this recovery can become even more complex due to the connections between AD and Entra ID. By protecting both with Rubrik, the recovery process can be eased by having Rubrik guide the recovery of both environments for a true hybrid recovery process.

For more information about recovering Active Directory with Rubrik, please see How It Works: Protecting Microsoft Active Directory with Rubrik Security Cloud.

Hypervisor Manager Recovery

Coordinate the recovery of vCenter(s) with the appropriate support team to ensure a smooth recovery.

- **vCenter Server Recovery:** Exercise care if vCenter Server has to be recovered or when recovering VMs into a new vCenter Server. Rubrik Secure Vault uses the Managed Object Identifier (MOID) of a VM for tracking. Duplication or reuse of the MOID can lead to issues during the recovery of VMs. If vCenter Server has been compromised, it is better to restore it from backup than create a new empty vCenter Server and then recover the VMs. Recovering all VMs into a newly deployed vCenter Server instance will assign all VMs a new MOID, meaning that new backup chains will begin for each workload, with the old chains seen as relics. If the vCenter Server is self-managed (that is, it does not reside on infrastructure managed by another vCenter Server), you can recover Rubrik snapshots of the vCenter Server directly to an ESXi host. Minimize the risk of re-infection by recovering this to a standalone host in a clean environment rather than pre-existing infrastructure.

  For more details on recovering vCenter Server from an image-based backup, please consult the official Rubrik and VMware documentation. Alternatively, backup the vCenter Server Appliance using the File Based Backup & Restore native to the appliance and save these files to a network filesystem. From there, back up the files using Rubrik filesets.

- **Recovery or reinstallation of non-vSphere Hypervisor Managers(s):** If hypervisor managers such as Microsoft's System Center Virtual Machine Manager (SCVMM) or Nutanix Prism are protected using Rubrik snapshots, please engage Rubrik Support for recovery options. When the hypervisor manager is protected using built-in backup methods, please engage the hypervisor vendor in addition to Rubrik Support. These hypervisor managers are usually prioritized higher in the recovery workflow to ensure that Rubrik can focus on the individual VMs afterward.

Orchestrated Recovery

In the event of a multi-system or application-based recovery, these best practices apply to scenarios where the impact is to an entire application.

- **Coordinate and evaluate:** Before any orchestrated recovery of an application or group of systems, ensure that all infected systems are isolated from the recovery environment. Validate your target recovery location for compute and storage resources required for the recovery. Take note and understand both the scope of the recovery and the system dependencies needed for the application. If applicable, leverage existing DR plans and runbooks to facilitate these efforts and coordinate with application owners to prepare for recovery. The target resources and application dependencies are already configured within the recovery plan and provide details for orchestrated recovery.

  Rubrik Data Threat Analytics can be helpful during this process. Threat Containment can guide you to the safest point in time to recover from while minimizing data loss from the event.

- **Execute recovery:** Once application recovery is complete, notify application owners and stakeholders to test and validate the application. Validation is a critical piece of the recovery plan and procedures and must occur before sign-off. These policies often include user authentication, data validation, and system dependency checks noted earlier.

KEY RUBRIK SECURITY TECHNOLOGIES

At Rubrik, we've built a highly secured, robust, and intelligent data management solution by engineering purpose-built components. We created our resilient file system, which stores all backup data and backup metadata in an immutable format. Data, once written, cannot be changed. It is also a distributed file system that provides for horizontal scalability, integrity checks, and data redundancy. Immutability is a critical feature when ransomware is at hand.

This commitment to purpose-built components and not sacrificing security for usability allows Rubrik to take a Zero Trust approach. Rubrik gives customers an out-of-box solution that minimizes the effort needed to take their security posture to the next level. The Rubrik Zero Trust architecture provides several advantages to ensure rapid recovery during an incident regarding ransomware. The following are core elements of the Rubrik Zero Trust Architecture.

NATIVE IMMUTABILITY

Rubrik engineered a purpose-built, natively immutable file system to protect its customers' on-premises data. While there are many advantages to how this file system operates, having data immutability built-in reduces complexity, operational overhead, and security risks. Once written, you cannot change data in any way. Since Rubrik stores data in a non-native format, data cannot be easily read or exfiltrated. This approach is in stark contrast to other solutions where data is readily accessible in its native format, making it easy for attackers to modify or steal the backup data.

The approach of default immutability also holds true when data is stored by Rubrik in the cloud by utilizing cloud-native immutability features. This is true for cloud-native backups, SaaS backups, or data archived to Rubrik Cloud Vault.

SLA RETENTION LOCK

SLA Retention Lock, a critical component of Rubrik's Zero Trust Data Security architecture, enhances data resilience by strictly enforcing immutability periods driven by SLA retention policies. Once enabled, Retention Lock prohibits any modification to an SLA Domain policy that would result in the deletion or premature expiration of backup data, including data stored in Archive targets (such as Rubrik Cloud Vault) and Replication targets. This ensures that data remains unalterable for the defined retention period.

In the event of a ransomware attack, where privileged accounts are frequently compromised, traditional backup solutions are vulnerable to tampering. Rubrik mitigates this risk by managing retention-locked SLAs through the Rubrik Quorum Authorization process. This multi-factor authorization and separation of duties provide a formidable defense against unauthorized data manipulation, including early expiration of retention periods, even in scenarios involving compromised credentials.

QUORUM AUTHORIZATION

Rubrik offers a capability that requires approval from at least one other user in order to make certain changes. Quorum Authorization enables an added level of security against rogue administrators or compromised credentials by adding an additional layer of approvals for some critical changes. When enabled, many items, including the following, can be configured to require two or more users to be involved in the change:

- Managing retention lock
- Reassigning SLA Domains
- Pausing protection
- Changing legal hold status
- Deleting or expiring snapshots
- Changing NTP configuration
- Editing SLA Domains

Additionally there are two ways this is implemented, Governance mode and Compliance mode.

In Governance mode, a requester requests the change, and then the designated approver must approve of the change before it goes into effect. The designated approver role is a special role that cannot be assigned to a user that also has administrator capabilities and cannot request any changes. This allows for separation of duties between requesters and approvers.

In Compliance mode, changes to a policy protected by Quorum Authorization can only be accomplished when the customer contacts Rubrik support to have the changes made. Rubrik support will require signed documentation from designated approvers at the customer before the changes are made.

INTELLIGENT DATA LOCK

Intelligent Data Lock gives users an additional window of time to retrieve data by keeping Rubrik Secure Vault snapshots after expiration or deletion. This allows for recovery of these snapshots even after they have been expired or deleted. This capability is available and on by default with CDM versions 8.0.3 and newer.

LEGAL HOLD

Legal Hold provides a method to prevent a snapshot from expiring and aging off the backup solution. While typically used to maintain evidence for legal requirements, it may also be helpful to apply Legal Hold to snapshots taken before or when you detected the infection for legal reasons and forensic investigation.

MULTI-FACTOR AUTHENTICATION

Compromised directory service platforms and individual accounts are hallmarks of a modern ransomware attack. Privileged accounts and directory services are high-value targets, and attackers will focus on compromising either one to gain further control of an environment and simply log in to their targets. To defend against these vulnerabilities, Rubrik enables MFA, by default, that can be used natively with Rubrik's Time-based One Time Passwords (TOTP). When configured, access through all system interfaces (GUI, CLI, and API) requires the end-user to perform a secondary authentication process before granting access. This additional layer of security provides robust defense against any compromised accounts in directory services (such as Microsoft's Active Directory). Since this is native to Rubrik, there is no dependency on third-party identity providers, allowing customers to be up and running with just a few clicks. Rubrik also supports additional third-party MFA providers via 3rd party Identity Provider(IdP) services that support SAML 2.0 should you already have one in place.

To defend against compromised accounts in the Rubrik system, all local accounts can inherit these exact authentication requirements and must provide secondary authentication to gain system access.

All MFA solutions adhere to the account lockout and lockout duration policies defined within the Rubrik system. Authentication events such as configuration, re-syncs, and resets are logged accordingly for incident and event management purposes. Properly handled correlation of these events can quickly identify a potential bad actor attempting to brute-force a password while masquerading as a known user..

RUBRIK SECURITY SOLUTIONS

While the Rubrik Zero Trust Architecture provides a robust, out-of-the-box security posture, it's the products and solutions that plug into that framework that bring true data resilience and threat protection. In this section, we'll cover the four main areas of the Rubrik portfolio and show how they protect your data while also ensuring a quick recovery from an attack.

RUBRIK SECURITY CLOUD

Rubrik Security Cloud (RSC) is a web-based management plane for all Rubrik products. It provides an interface designed to simplify the management of data protection across a global hybrid infrastructure. Instead of conventional backup jobs, RSC uses a declarative policy engine to maintain a set of user-defined SLA policies. Rather than dozens, hundreds, or even thousands of per-application backup jobs, a small number of SLA policies are defined based on the RPO, retention, replication, and archival requirements. You can then apply a single SLA policy to any number of different applications, hypervisors, databases, cloud workloads, or other supported datasets.

RSC is a powerful metadata catalog, with each data control plane bringing in actionable intelligence around your data. This metadata is instrumental in understanding changes between various point-in-time copies and drives how the system stores, replicates, archives, and restores data. This system design applies to all data within Rubrik's purview, including on-premises and the cloud. This metadata pool also contributes to Rubrik's global search capabilities, aiding in granular, file-level recovery and audit or discovery for security purposes. For example, a Security Administrator can globally search all protected objects for a particular filename to identify its inception into the environment.

RSC also acts as a control plane for cloud native and SaaS application protection, requiring no on-premises components.

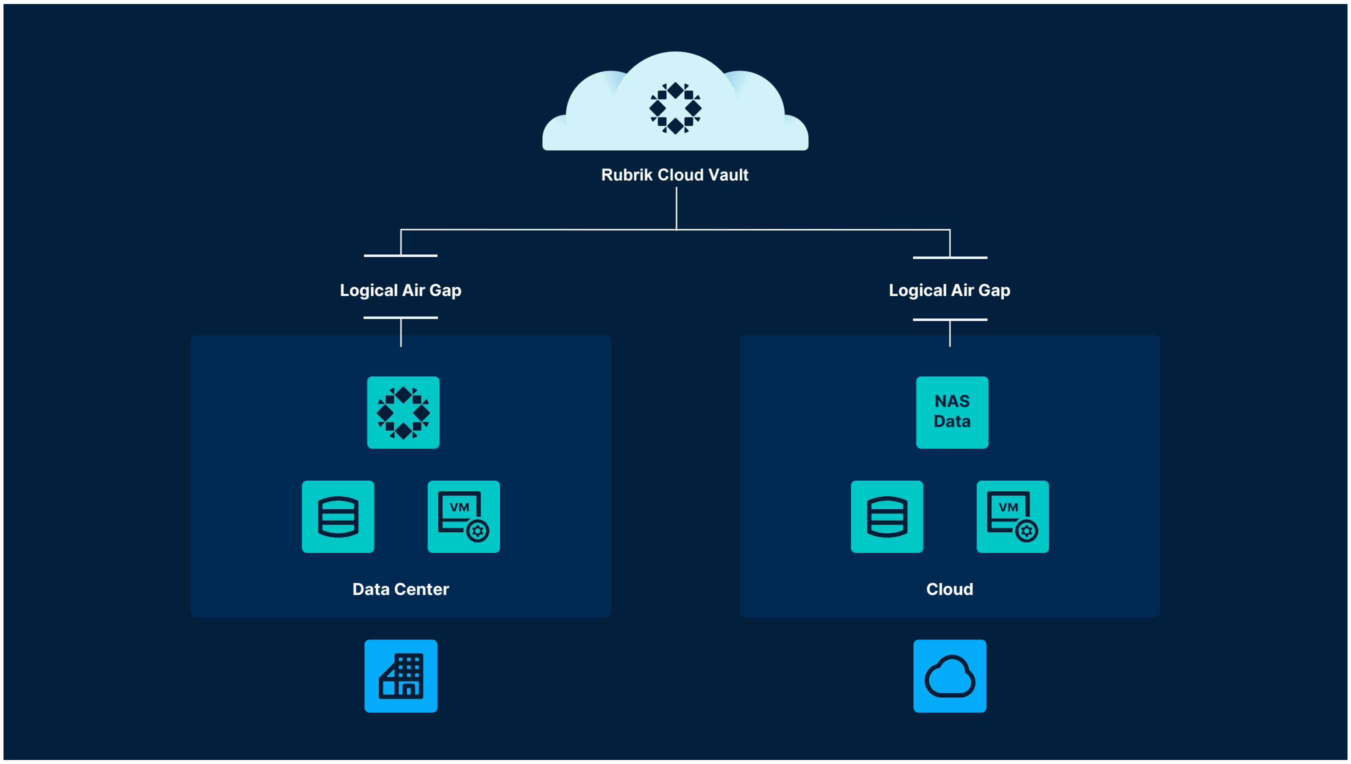
For on-premises data protection, Rubrik Secure Vault acts as both the control plane and primary storage location.

RUBRIK SECURE VAULT

Rubrik Secure Vault (RSV) is a hyperconverged solution built around the previously mentioned natively immutable file system and utilizes a Zero Trust architecture to mitigate attack vectors that cybercriminals are known to exploit. This architecture includes immutability, SLA Retention Lock, NTP poisoning protection, and native TOTP for MFA. The result is a secure on-premises data protection platform with minimal manual work post-deployment.

RUBRIK CLOUD VAULT

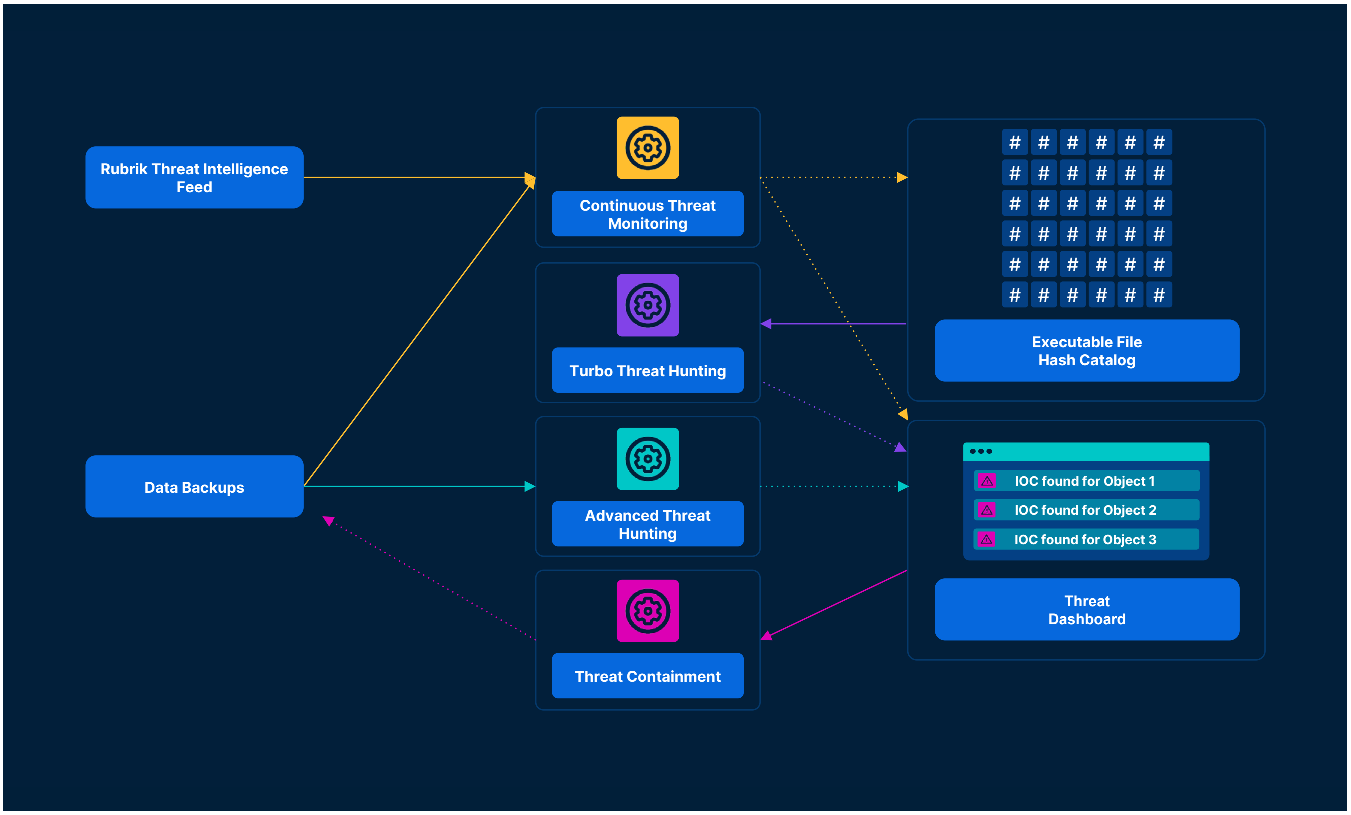
Rubrik Cloud Vault (RCV) is a fully-managed cloud service that enables customers to maintain secure, isolated copies of data for cyber resilience and regulatory compliance. It ensures data immutability, a credential gap to prevent lateral movement, reduced operational overhead, and less security risks.



In the event of a ransomware attack, RCV benefits customers by providing an additional layer of data resilience. Its immutability by default, coupled with SLA Retention Lock and Quorum Authorization, significantly reduces an attacker's ability to gain access and modify backups. Furthermore, credential-gapping prevents lateral movement into the RCV environment, ensuring that a clean, unalterable copy of data is available for recovery, mitigating the impact of an attack and preventing data loss.

RUBRIK DATA THREAT ANALYTICS

Data Threat Analytics (DTA) is a collection of engines used to identify suspicious activities within backup data that could indicate the presence of a cyber attacker or execution of a data disruption attack, like ransomware.



Anomaly Detection

Anomaly Detection's primary purpose is to determine anomalous activity by analyzing metadata from backups. This process uses both machine learning algorithms and Generative AI to analyze data change rates and randomness indicators (data entropy) to remove the usual false positives of data seasonality, giving Rubrik customers more confidence in notifications and alerts.

Through its metadata analysis, Anomaly Detection allows administrators to quickly determine an attack's blast radius, resulting in a more straightforward and efficient recovery. Knowing what is and is not affected by an attack, administrators can determine what files, folders, or systems to recover. This more surgical approach minimizes the loss of data not affected by the attack. For example, recovering a single file instead of a multi-terabyte virtual machine will save time and resources.

Threat Monitoring

Threat Monitoring analyzes backup metadata in parallel with Anomaly Detection to look for Indicators of Compromise (IoCs). This analysis utilizes a feed that comes from Rubrik Threat Intelligence that combines high-confidence IoCs from the Google Mandiant Threat Intelligence feed with customer-defined IoCs added via RSC. The resulting feed is a combination of YARA rules, file path rules, and file hashes that is updated on a daily basis.

When new IoCs are added to this combined feed, those IoCs will be evaluated against all retained backups. This allows Rubrik to quickly identify newly added malware IOCs that utilize zero-day exploits that may have been dwelling in customer environments for a long time.

As part of this evaluation, all files in the incremental backup are hashed. For every executable file in the backup, Threat Monitoring will store the file name, location, snapshot, and file hash into a database within RSC that will be used by Turbo Threat Hunting (see next section).

Threat Hunting

Threat Hunting is used to search some or all existing backups for very specific IoCs, provided by the user at the time of the hunt. There are two types of threat hunts Rubrik provides: Turbo and Advanced.

- **Turbo Threat Hunting:** Turbo Threat Hunting utilizes the database of executable file hashes created by Threat Monitoring to very quickly lookup the existence of the file hashes provided by the user. Using this approach, Rubrik users can go from providing up to ten hashes to having a list of identified files in tens of thousands of backups in just a few minutes. This approach is very precise and results in high-confidence results.

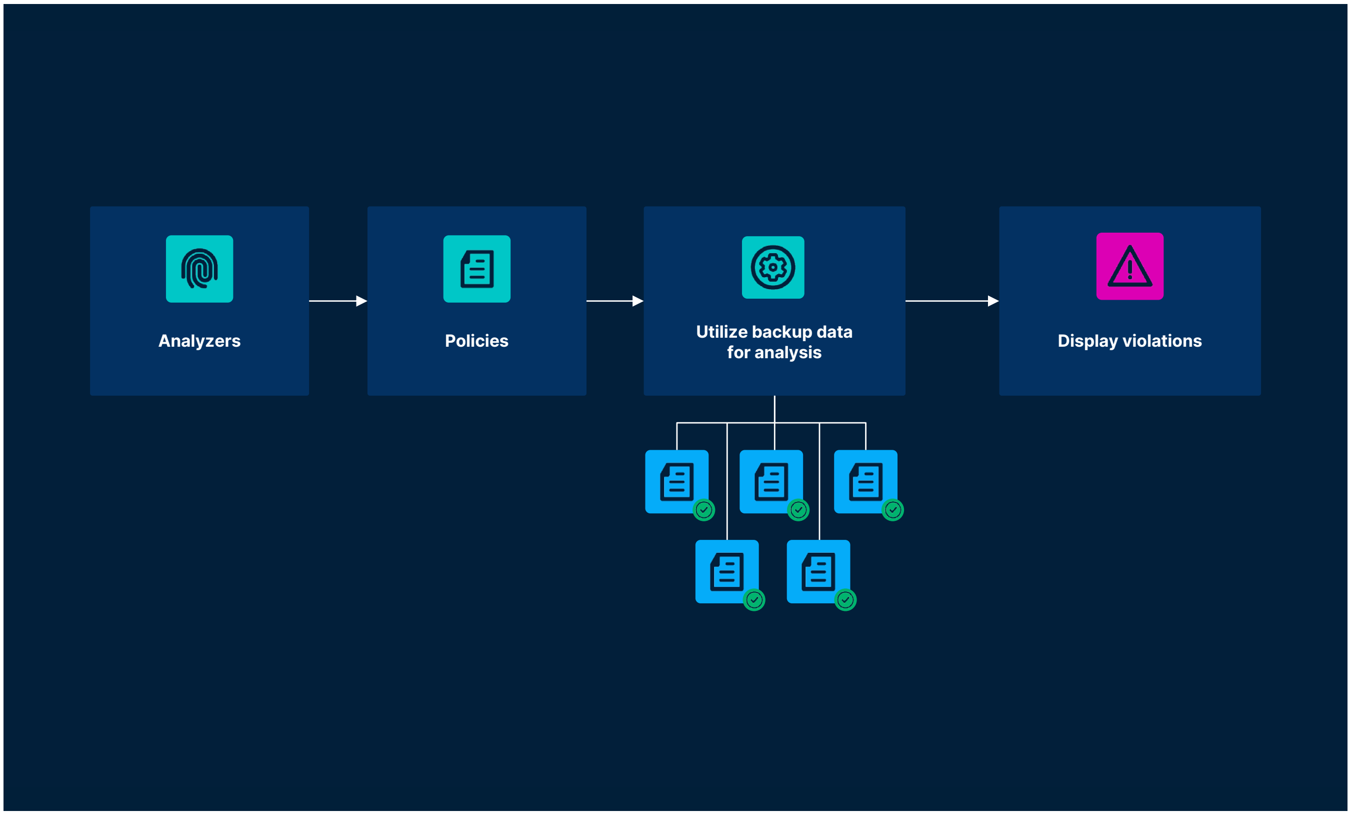
- **Advanced Threat Hunting:** Advanced Threat Hunting is a more resource-intensive process for identifying IoCs in backups. Users can provide up to ten IoCs that can be any combination of YARA rules, file path rules, or file hashes. Rubrik then mounts up each indicated point-in-time to apply those rules and generate and compare hashes of all files. This approach is more time consuming and more prone to false positives, and therefore recommended to be more precise on the objects and timespan to be evaluated.

Threat Containment

Once IoCs or anomalies are discovered, the files and objects can easily be quarantined en masse with Threat Containment. This applies role-based access controls around the detected files to prevent unauthorized users from restoring known malware. Users not authorized to restore anomalous or quarantined files can still restore other files from that snapshot, but will be unable to restore the quarantined files. They will also be blocked from restoring the full object (e.g. an entire VM).

By maintaining these known contaminated points in time, some users can be granted the ability to restore these quarantined snapshots for analysis in a clean room environment.

RUBRIK DATA DISCOVERY AND CLASSIFICATION



Another component of the Rubrik Security Cloud platform is Data Discovery and Classification, a data classification engine that actively scans the contents of backups looking for specific sensitive data (as outlined below). Data Discovery and Classification leverages the systems and data within a Rubrik backup environment and uses that data to determine where this sensitive data exists and who has access. By utilizing backup data, it can classify specific sensitive data without the arduous deployment of individual agents or interfering with production systems. In contrast, point solutions for data classification can tax the underlying production infrastructure and are unwieldy to govern.

Data Discovery and Classification foundationally uses a concept of an analyzer and a policy. It uses an analyzer to define what the system should identify in the contents of the data, and policies enable the bundling of multiple types of analyzers into a single report. Many built-in analyzers are available out-of-the-box for common classifications such as social security numbers, email addresses, passport numbers, and credit card numbers. As every customer's needs are different, every customer can create custom analyzers to ensure discovery of the data that is important to them. They can be tailored with customized dictionary terms or regular expressions to meet your particular needs.

A policy is a collection of analyzers that provide a flexible deployment model of the definitions used during scan operations. There are predefined policies available, such as: PCI DSS, CCPA, HIPAA, and US and UK PII. Once configured, you can apply policies to protected systems and data throughout Rubrik.

RUBRIK ORCHESTRATED RECOVERY

Orchestrated Recovery is a data recovery orchestration tool that can take advantage of the added intelligence provided by Data Threat Analytics, specifically Threat Containment. Orchestrated Recovery uses the concept of a blueprint that groups the systems, resources, and logic to recover multiple virtual machines in a single executable plan. Blueprints also provide the flexibility of selective recoveries based on the results of Anomaly Detection and Threat Containment.

Orchestrated Recovery provides multiple options to recover to different target environments, depending upon the scenario. Doing so supports the traditional scenario of a complete site failure to a disaster recovery site, replacing an entire application due to an attack or mistake, or performing an isolated recovery in response to a cyber attack, all in the same interface.

VERSION HISTORY

Version	Date	Summary of Changes
1.0	December 2021	Initial Release
2.0	January 2023	Add new features
3.0	November 2025	Significant rewrite to account for new features, updated product names, and latest ransomware tactics, techniques, and procedures (TTPs)

APPENDIX

RESOURCES

- Best Practices for Ransomware Recovery with Rubrik
- Rubrik Support Portal
- Government Agencies

    a. 🇺🇸 CISA Stop Ransomware Guide

    b. 🇺🇸 NSA Zero Trust Security Model

    c. 🇺🇸 NIST Muti-Factor Authentication Overview

    d. 🇪🇺 ENISA Cyber Threats

rubrik

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

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

IMS
CLOUD SERVICES

IMS Cloud Services is a leading provider of backup and disaster recovery services. Banks and credit unions throughout the United States rely on IMS for business resumption in the event of a cyberattack or any type of man made or natural disaster. IMS has been serving banks and credit unions for over 25 years. For more information please visit imscloudservices.com.