rubrik

WHITE PAPER

Best Practices Guide: Prepare and Recover from a Ransomware Attack

Rubrik Technical Marketing
January 2023

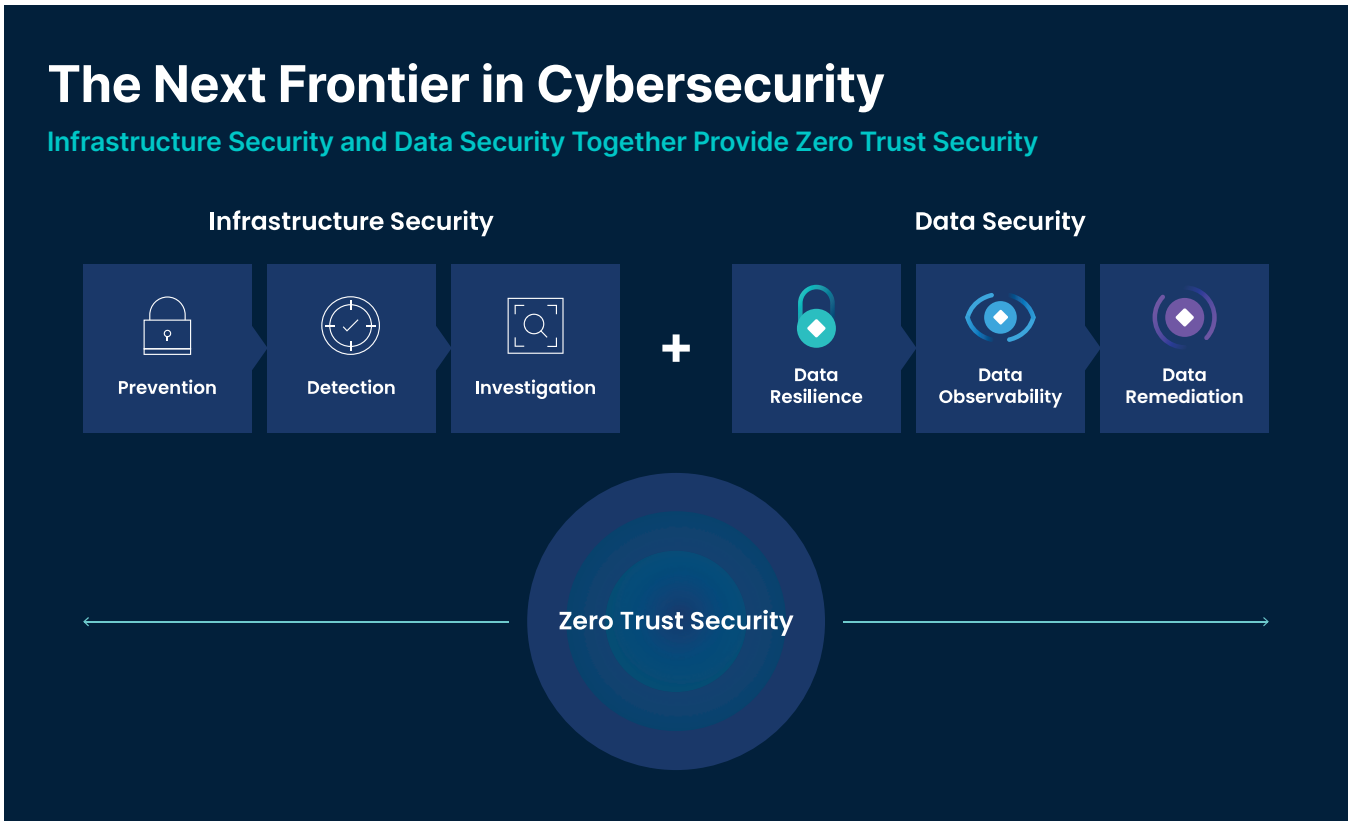
Table of Contents

THE NEED FOR CYBER RESILIENCE

While ransomware attacks are skyrocketing in number, Rubrik customers can quickly and effectively recover their data to minimize the 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. Then, you'll learn about deployment best practices that make it even more challenging for cybercriminals to attack. And, finally, we'll go through the recovery process should the unfortunate event of an attack occur.

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.



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, which prevents a bad actor from expiring any backup data prematurely. Multiple expert-guided recovery options, including Live Mount and Mass Recovery, are built-in so IT teams can quickly recover the files and workloads impacted by an attack.

SECURE BY DESIGN

Rubrik's founders made security a core design principle from the very beginning of product development. They started with a custom file system to provide out-of-the-box immutability. They also gave Rubrik a logical air gap to protect data from attackers and rogue admins. They put additional protections in place, such as robust role-based access controls (RBAC), API authentication requirements, and disabling unused ports. Rubrik CDM also uses certificate signing to continuously validate the identity of Rubrik services to ensure that services and their identities have not been tampered with or otherwise compromised. As customers and threats have evolved, Rubrik has added more protections, including native multi-factor authentication (MFA), which is enabled by default, that doesn't rely on third-party solutions. For enterprise use, where integrations with a third-party Identity Provider (IDP) may be desirable, SAML 2.0 based IDPs are supported (including for MFA).

Backup data truly is the last line of defense and the key to recovering from a ransomware attack. Rubrik's secure-by-design approach makes it easy for customers to implement a superior security posture related to backups and data management by reducing manual work post-deployment. As part of Zero Trust Data Security™, this methodology gives customers confidence not only that their data is safe but that they will also be able to recover from an attack quickly.

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 to respond to a ransomware attack. Hardening the Rubrik environment is a must after installation and configuration and before onboarding workloads to be protected. For more information on securing Rubrik against unauthorized use, please refer to the Rubrik Security Hardening Best Practices. You can find additional security hardening guides for archive (external) storage (e.g., S3 for AWS, Blob for Azure) on the Rubrik Support portal.

While Rubrik Security Cloud is SaaS, meaning Rubrik is responsible for updates, it is a recommended best practice that you keep Rubrik CDM up to the latest version. Security is an ongoing concern globally, and Rubrik adds new methods and features to each product release.

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.

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 risk. 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 event incidents.

The Rubrik RRT is a process driven global 24×7×365 support overlay composed of highly experienced individuals. The core virtual team consists of incident managers, senior support staff, and executive leadership. The RRT's primary objective is to provide around-the-clock technical assistance and recovery facilitation while closely collaborating with and complementing the customer's recovery plans and priorities.

Rubrik has 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.

RUBRIK GLOSSARY

Rubrik Solution	Description
 Ransomware Monitoring & Investigation	**Determine the scope of ransomware attacks using machine learning to detect deletions, modifications, and encryptions.** SaaS application that makes it faster and easier to recover from ransomware attacks by tracking how data changes over time. It uses machine learning to monitor data and generate alerts for anomalous activity (e.g., file changes, encryption, entropy). Alerts can be passed along to SIEM tools to help security teams respond to incidents. Includes ransomware strain identification for some of the most common tools.
 Sensitive Data Monitoring & Management	**Reduce sensitive data exposure and manage exfiltration risk by discovering what types of sensitive data you have, where it lives, and who has access to it.** SaaS application that discovers, classifies, and reports on what types of specific sensitive data (e.g., 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.** SaaS application that provides the capability to hunt for Indicators of Compromise (IOCs) in backups across time, giving users the ability to pinpoint which backups contain the IOC and which ones do not.
 Threat Containment	**Ensure safe and quick data recovery by quarantining data infected with malware as part of a state of the art incident response process.** SaaS application that allows the quarantine of backups and files. Disallowing their accidental recovery and reinfection. It provides peace of mind that reinfection, due to recovery, will not happen.
 Orchestrated Application Recovery	**Recover applications quickly with pre-built workflows and disaster recovery blueprints.** SaaS application that automates recovery, allowing IT organizations to restore applications and data with guided workflows. It provides orchestration of DR failover/ failback and testing, and together with application-focused ransomware remediation, simplifies recovery for services running in VMware vSphere environments. Orchestrated Application Recovery integrates with Ransomware Investigation to identify impacted applications and rapidly recover them in-place using the recommended points in time just before infection.
 Cyber Recovery	**Improve cyber readiness and response with faster recovery testing and validation in an isolated recovery environment.** SaaS application that enables the deployment of isolated recovery environments for testing of recovery processes, and can help to parallelize the forensics process for faster recoveries in the event of a cyber attack. Integrates with Threat Monitoring & Hunting, Threat Containment, and Ransomware Monitoring & Investigation to pinpoint both safe and malicious recovery points for recovery, dependent on the scenario.

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 will help expedite the identification and cleanup of the ransomware by reacting 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. 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 Sensitive Data Monitoring & Management can provide visibility into this and forms a vital part of the ongoing risk management process and incident response in a ransomware attack.

Implement tools like Rubrik Ransomware Monitoring & Investigation 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. The data is encrypted; however, the hackers may have been in the system for quite some time beforehand, gathering intelligence, installing malware, establishing command and control, and planning the attack. Furthermore, classifying this data with a tool like Rubrik Sensitive Data Monitoring & Management will help determine if any of the compromised data is sensitive in nature, along with who has access to it.

Ensure to protect all critical systems and data 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 workload. For example, Rubrik Instant Recovery instantiates the recovered workload from backup, running live on the Rubrik cluster storage. Because of this, the workload can be recovered much quicker than it would be in the event that recovery of a full backup to production storage would be required. This method, however, rolls entire systems back to a safe point in time. With this approach to recovery, you may lose data that was not infected or encrypted. File-level and database level restores for infected data may be more desirable. For more widespread attacks, Mass Recovery might be the best choice. For some workloads, leveraging Live Mount to stand up a VM based on a point in time backup for recovery of transaction logs or forensics purposes would be the best approach. In addition to recovering production, there is a need to recover systems into an isolated environment. This allows for deeper inspection of systems for compromises. For this there is Rubrik Cyber Recovery, a tool that allows instantiation of point in time images of systems for forensic analysis. For each situation, evaluate the appropriate method ahead of time so that you can quickly select the proper course of action during an attack.

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 Application Recovery, you can predefine application-level blueprints that include all the resources associated with that application to allow 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

Periodically test data recovery to be prepared for an actual incident. 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. These tests are known as tabletop exercises. Rubrik offers a generic tabletop exercise called Save the Data. They can help IT organizations prepare for the unexpected, which can be an invaluable experience during the chaotic events caused by an attack.

The Open Source Community provides various validation frameworks. Rubrik GitHub community provides one such framework.

DETECTION AND ANALYSIS

Determine Blast Radius

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 Ransomware Monitoring & Investigation helps detect ransomware by leveraging unsupervised machine learning to analyze backup data. The model is designed to analyze many recent snapshots and identify outliers, without requiring human input. The analysis is primarily based on file system behavior and content analysis. 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. Once outlier behavior is detected, Ransomware Monitoring & Investigation can perform file content analysis on the backup to identify if encryption has occurred. A list of the impacted files, and their associated probability of being infected, is then presented to the user. Finally, several of the most used ransomware tools can be identified by Ransomware Monitoring & Investigation. Integration with security orchestration, automation & response (SOAR) platforms such as Palo Alto Networks Cortex XSOAR and Microsoft Sentinel can assist investigations from a Security Operations perspective.

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.

For the affected systems that you will isolate, it is also recommended to carefully review snapshot expiration to ensure no valid snapshots expire, affecting 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 cluster(s) 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

All stakeholders should be notified of the ransomware attack so that they can start to execute their portions of the recovery plan. Early notification of stakeholders, Rubrik, and other 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 for further recovery.

In preparation for the recovery process, strongly consider establishing an isolated quarantine environment. Rubrik Cyber Recovery can help recover host(s) into this isolated environment, giving automation and repeatability to the process. This approach allows for restorations to be thoroughly scanned for malware and validated as clean before releasing into the production environment.

Scoping the attack involves understanding which business functions, systems, and data were compromised. Rubrik Ransomware Monitoring & Investigation can help determine the blast radius of the attack to be contained, meaning 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. Doing so would also restore systems unaffected by the attack from a previous point in time. Rubrik's insight allows for more surgical recovery, avoiding unnecessary data loss and restoring service more quickly. Rubrik Ransomware Monitoring & Investigation can also automatically indicate the most recent snapshot without anomalous activity to make it easier to identify potential recovery points.

Taking assessment one step further, Rubrik Sensitive Data Monitoring & Management can help determine which sensitive data have 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. For Rubrik CDM, it will also minimize impact to snapshot chains and minimize subsequent full and incrementals, resulting in less cluster space being consumed and jobs running faster. 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.

Finally, determine if local copies of the backups are available or if they will need to be recovered from archives. The recovery point determined for each system based on when the ransomware payload was activated will help dictate this. Also, determine if the archival or cloud data has been compromised. If so, recovering from an alternate copy will be necessary.

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. Data may need to be recovered 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. 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 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 Ransomware Monitoring & Investigation to identify which files were attacked by the ransomware and recover them.
- **Identify sensitive information:** Tools like Rubrik Sensitive Data Monitoring & Management 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.

- **When to use Instant Recovery:** (Smaller data sets) Recovery efforts can be sped up by utilizing Rubrik's Instant Recovery feature. Instant Recovery allows 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 is a good option for a smaller number of VMs, which may include mission-critical systems. Care should be taken with Instant Recovery so that the Rubrik cluster is not overloaded. The Rubrik cluster 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 is a good option 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 or copies 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 with Exports:** Instant Recovery 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 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. 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. As well as authentication services, it 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 hit by ransomware. Due to these factors, it is typically one of the first pieces of infrastructure that needs to be recovered.

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.

For more information about recovering Active Directory with Rubrik, please see Surviving Microsoft Active Directory Failures with Rubrik.

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 CDM 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 instead to 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. When recovering vCenter Server from a native backup file, follow the process detailed in the VMware documentation, paying particular attention that the recovery media must be of the correct version.

- **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 production 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.

  Rubrik Ransomware Monitoring & Investigation and Orchestrated Application Recovery are helpful during this process. Data from Ransomware Monitoring & Investigation can guide you to the safest point in time to recover from while minimizing data loss from the event. The target resources and application dependencies are already configured within an application blueprint and provide details for orchestrated recovery.

- **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 disaster 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 three core elements of the Rubrik Zero Trust Architecture.

NATIVE IMMUTABILITY

Rubrik engineered a purpose-built, natively immutable file system to protect its customers' 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.

SLA RETENTION LOCK

SLA Retention Lock is an additional layer of the Rubrik Zero Trust architecture that provides data resilience. Once enabled, Retention Lock strictly prohibits any modification to an SLA domain policy resulting in deleted backup data. This includes outright deletion or data expiration and data redirection via Rubrik's archival and replication policies.

During a ransomware attack, privileged accounts are often compromised and can leave legacy solutions exposed to the tampering of backup data. In Rubrik, the security of retention locked SLAs is managed through a validation process within Rubrik's compliance team. If a customer requests a modification to a retention locked SLA, two appointed individuals from the customer's organization must authenticate and acknowledge the alterations with the Rubrik Support Team.

TWO PERSON RULE

Rubrik offers a capability that requires two people's input to make certain changes. The two person rule 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 the following can be configured to require two people 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, Enterprise mode and Compliance Mode.

In Enterprise mode, a requester requests the change then the designated approver must approve of the change before it goes into effect. The designated approver role is a special role that can not be assigned to a user that also has administrator capabilities and can not request any changes. This allows for separation of duties between requesters and approvers. In Compliance mode, changes to a policy protected by a two person rule 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 that snapshots are kept 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 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. 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 CDM

CDM is a software service built on top of the previously mentioned natively immutable file system. Instead of conventional backup jobs, CDM 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, or datasets.

In addition to the natively immutable file system ensuring attackers can't modify or steal your data, CDM uses the Zero Trust architecture to mitigate attack vectors that cybercriminals are known to exploit. This architecture includes immutability, SLA Retention Lock, and native TOTP for MFA. The result is a secure data protection platform with minimal manual work post-deployment.

CDM is also a powerful metadata engine that brings 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 CDM's purview, including on-premises, remote sites, 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.

RUBRIK RANSOMWARE MONITORING & INVESTIGATION

Ransomware Monitoring & Investigation is a component of the Rubrik Security Cloud control plane used to centrally manage CDM instances and cloud-native offerings such as Microsoft 365 protection. Ransomware Monitoring & Investigation's primary purpose is to determine anomalous activity by analyzing metadata from CDM. Rubrik uses both data change rates and randomness indicators (data entropy). Doing so removes the usual false positives of data seasonality, giving Rubrik customers more confidence in notifications and alerts.

Through its metadata analysis, Ransomware Monitoring & Investigation 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.

Metadata analysis means that administrators will not only know what systems are affected by an attack, but they'll also be able to recover only the data they need. Recovery is fast and efficient, and it minimizes data loss due to unnecessary restores.

RUBRIK SENSITIVE DATA MONITORING & MANAGEMENT

Another component of the Rubrik Security Cloud platform is Sensitive Data Monitoring & Management, a data classification tool that actively scans the contents of backups looking for specific sensitive data (as outlined below). Sensitive Data Monitoring & Management leverages the systems and application data within a Rubrik backup environment and uses that data to determine where this sensitive data exists and who has access. It can also 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 infrastructure and are unwieldy to govern.

Sensitive Data Monitoring & Management 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. 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. At the time of writing, there are 55 out-of-the-box analyzers, with new analyzers constantly added. As every customer's needs are different, if you find that the shipped analyzers don't meet your needs then you can create custom analyzers to ensure discovery of the data that is important to you. 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 APPLICATION RECOVERY

Orchestrated Application Recovery is a disaster recovery orchestration tool that combines a framework for recovering applications and can take advantage of the added intelligence provided by Ransomware Monitoring & Investigation. Orchestrated Application Recovery uses the concept of a blueprint that groups the systems, resources, and logic to recover an application. Blueprints also provide the flexibility of selective recoveries with the added benefit of anomaly detection from Ransomware Monitoring & Investigation. Most disaster recovery solutions rely on infrastructure provided by the IT organization and often result in operational drag to support the security, compatibility, and management of the system.

Orchestrated Application Recovery also provides multiple options to recover to different target environments, depending upon the scenario. Doing so supports the traditional scenario of a complete site failure and the localized recovery scenario of a malicious attack.

RUBRIK THREAT MONITORING & HUNTING

Threat Monitoring & Hunting allows for the searching, across time, of backups for indicators of compromise (IOCs). These IOCs are left behind by malicious software and can be signs of a cyber attack. Threat Monitoring & Hunting takes in IOCs as file and directory names, hashes, and YARA rules. Once the IOC is defined, Threat Monitoring & Hunting searches through the flagged backups for the indicators. This allows for pinpoint location of malicious software and confirmation of type or strain. Once identified, users know where and when the malicious software is located. So recovering to a known safe state can be confirmed and reinfection can be avoided and data loss can be minimized.

RUBRIK THREAT CONTAINMENT

Threat Containment allows for the quarantining of backups and files that contain malicious software from accidentally being restored and thus reinfecting environments. Once backups are identified to include IOCs by Threat Monitoring & Hunting they can be quarantined so that only roles with the specific permissions can restore, download, or remove them from quarantine. This will remove the chance of a reinfection due to accidental restoration of malicious software.

RUBRIK CYBER RECOVERY

Cyber Recovery allows for testing and validation of cyber recovery plans, giving users the ability to quickly build plans and run deployment testing in an isolated environment. During an attack, Cyber Recovery allows users to deploy a copy of production data into an isolated environment for forensic investigation, allowing for the simultaneous investigation and recovery of production systems. The result is reduced downtime for the business and peace of mind for SecOps teams that critical evidence has not been lost.

APPENDIX

RESOURCES

- Best Practices for Ransomware Recovery with Rubrik
- Rubrik Security Hardening Best Practices
- Government Agencies
    a. CISA Ransomware Guidance
    b. NSA Zero Trust Security Model
    c. NSA MFA Overview
    d. ENISA Ransomware

rubrik

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

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

wp-best-practices-guide-prepare-and-recover-from-a-ransomware-attack / 20230125