WHITE PAPER

# Best Practices Guide: Prepare and Recover from a Ransomware Attack with Rubrik

Rubrik Technical Marketing | July 2021

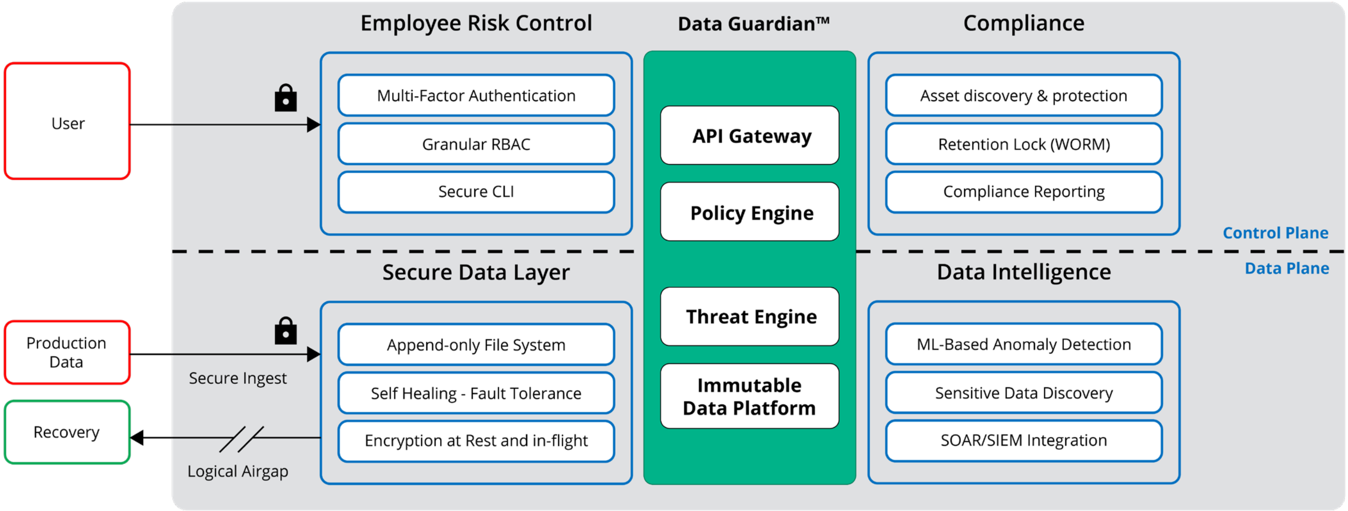
# TABLE OF CONTENTS

## THE NEED FOR CYBER RESILIENCE

While ransomware attacks are skyrocketing in number, Rubrik customers are able to quickly and effectively recover their data to minimize the damage to their business. This guide will explain Rubrik Zero Trust Data Management and how its built-in capabilities make protected data immune to ransomware. Then, you'll learn about deployment best practices that make it even tougher for cyber criminals to attack. And, finally, we'll go through the process of recovery should the unfortunate event of an attack occur.

## ZERO TRUST DATA MANAGEMENT

Zero Trust Data Management is Rubrik's patented architecture that is modeled after the Zero Trust Implementation Model from NIST (National Institute of Standards and Technology). At the core of Rubrik Zero Trust is Rubrik DataGuardian™ technology, which supports a purpose-built file system that never exposes backup data via open protocols. This creates a logical airgap that blocks data from being discoverable or accessible over the network.



Once data is written to the Rubrik system, it cannot be modified, deleted or encrypted by an attack, ensuring that a clean copy of data is always available for recovery. Multiple expert-guided recovery options, including LiveMount and Mass Recovery, are built-in so IT teams can quickly recover the files and workloads impacted by an attack.

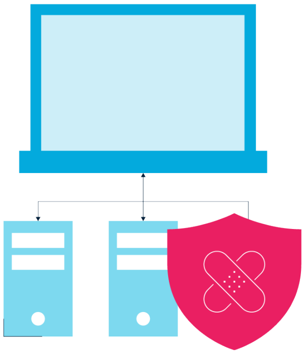
## SECURE BY DESIGN

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. And they also gave Rubrik a logical air gap to protect data from attackers and rogue admins. Additional protections were put in place such as a robust RBAC system, API authentication requirements, and disabling any unused ports. Rubrik also uses a minimalist JeOS Linux Operating System to reduce attack surface at the OS level and certificate signing to continuously validate the identity of Rubrik services to ensure that services and their identities have not been tampered with. As customers and threats have evolved, even more protections have been added including native multi-factor authentication that doesn't rely on 3rd party solutions and can be set up in seconds.

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 as it relates to backups and data management by reducing manual work post-deployment. This methodology, as part of Zero Trust Data Management, gives customers confidence not only that their data is safe but that they will also be able to quickly recover from an attack.

## SECURE DEPLOYMENT BEST PRACTICES

There are a set of general best practices IT Administrators should follow in order to minimize risk from cyber threats. Below, we'll discuss these practices and provide a simple checklist in Appendix A.



### PATCH SYSTEMS REGULARLY

A common attack vector for cyber criminals is out of date software. Exploits are continuously discovered and while many are responsibly disclosed to software manufacturers, many are used nefariously to penetrate networks and gain unauthorized access to systems and data. By having a plan to stay up to date by continuously patching infrastructure systems, organizations are mitigating many common threats. This includes operating systems (Windows, Linux, macOS, etc), appliances, storage, networking, and even BIOS and firmware of servers. Rubrik recommends you work with all of your hardware and software vendors to have documented procedures in place to patch systems in a timely manner.

Rubrik regularly releases patches and updates for its products. With CDM 5.3 and later, keeping on-premises clusters up to date is a snap with Rubrik Polaris. Polaris can centrally manage those clusters and enable administrators to update those systems with just a few mouse clicks. And, for systems using the Rubrik Backup Service (RBS), updates can be automatically pushed out when CDM is upgraded without needing to reboot the host systems. Keeping both Rubrik and the systems it is protecting up to date is a critical part of a sound security strategy.

### SECURE ACCESS TO SYSTEMS

Access to systems can be tightened through authentication and authorization mechanisms. Authentication is how a user or service identifies itself to a system. There are some very easy ways to secure authentication that start with not allowing unauthenticated (or anonymous) access. In other words, require all users and services to provide authentication. This could be through the use of passwords or passphrases, TLS certificates, or even biometric factors. Where possible, enforce multi-factor authentication (MFA) where multiple forms of identification are required to successfully authenticate. For example, users might be required to provide both a password (something you know) as well as a fingerprint (something you have). Another MFA method is to use a time-based one time password which uses a secure authenticator application like Google Authenticator or Microsoft Authenticator. Rubrik offers MFA natively and can be set up in just a few seconds.

Authorization grants access to system resources for authenticated users and services. So, once authenticated, it is the authorization process that controls what a user can see and do within a system. Role-based Access Control (RBAC) is a common authorization mechanism that makes it easier to manage permissions using predefined or custom roles. Those roles are then applied to users and services instead of having to manually set permissions for each individual. Rubrik provides a set of prebuilt roles to make it easier and organizations should ensure that all other infrastructure systems and applications use RBAC to make authorization manageable.

In addition, always use the principle of least privilege when assigning roles and permissions. Least privilege means that users and services are given the least amount of system access that they need to do their job. In other words, don't grant users more access than they need to prevent them from accidental or intentional misuse of a system. Attacks can exploit this to do additional damage through a compromised account.

Always be sure network access is locked down by disabling unused ports on systems, probably configuring access rules on firewalls, and restricting access from the internet. While those principles may seem like common sense, it is surprising how many organizations opt to make things easier on their users and attackers by deploying insecure networks. With insecure networks, attacks can move freely throughout the network and access everything from production systems to backups. Note that Rubrik systems come with all unused ports disabled by default so efforts and resources can be spent elsewhere on the network.

## ENABLE AUDITING THROUGH SYSLOG

Restricting system and data access is only part of the solution when securing an environment. Auditing brings visibility to access, authorization, and activity within the system. This data can produce something as simple as an audit trail of who accessed what and when, to a fully automated event-driven system that can take action when specific events occur. Generally, auditing data is recorded via a process called syslog which outputs those events in a structured, human readable format. It is important to make sure that syslog is enabled and that it is configured to log the appropriate event types.

Enabling and configuring processes such as auditing and syslog can often seem like daunting tasks. Every system is different so planning needs to occur for managing the configuration as well as the flow of audit and syslog data. If possible, employ a centralized syslog tool that can not only ingest data but also provide real time alerting and analysis that provides actionable insights. If it is not possible to use such a tool, it is still recommended to enable auditing of events and syslog so, at the very least, those logs can be analysed when needed. Also be sure to secure the storage and transmission of syslog data so that an attacker cannot discover important information about the system.

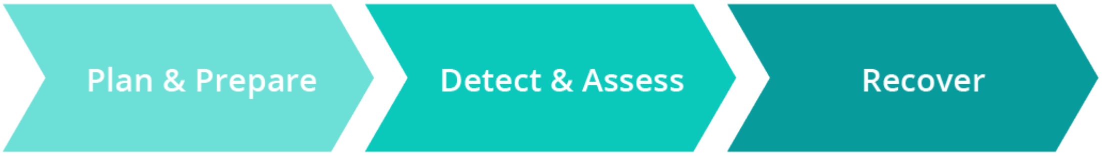
## AUTOMATE EVERYTHING

Automating tasks in IT infrastructure is not just about saving time. Automation makes tasks repeatable and self-documenting. These aspects are often forgotten or their value downplayed. When a task is automated, it is done the same way every time and there is a documented set of instructions that was followed to perform the task. This consistency and paper trail are two very valuable attributes when deploying, configuring, managing, and securing infrastructure. So, be sure to work with tools and infrastructure that have APIs and can support automation.

Just like with other activities, automation mechanisms still need to be secured. Make sure that API endpoints require authentication (i.e. disable anonymous API calls) and accounts used for automation use least privilege just as with regular user accounts. To take things a step further, it is recommended to use token-based authentication for automation accounts to reduce the risk of compromised credentials. And, finally, be sure to store those tokens in a secure vault so that an attacker can't stumble upon them in a script sitting in clear text on the network.

# RECOVER FROM RANSOMWARE ATTACKS WITH RUBRIK

As guardians of our customer's data, Rubrik understands that a ransomware attack is one of the worst-case recovery scenarios that customers can face. An impacted customer will likely be dealing with widespread business and logistics issues caused by the attack. Rubrik has helped a number of our customers successfully recover from ransomware attacks. As a result, a set of best practices has been developed to help other customers plan for, identify and remediate ransomware attacks.



## PLAN AND PREPARE

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 that Rubrik has found to be successful.

## BUILD A PLAN

Develop a ransomware response and recovery plan and supporting playbook. This plan should be updated and reviewed periodically. Additionally, the plan should be stored in a secure location that cannot be attacked by ransomware. A printed copy is good for this. By following an established plan during an attack, confusion will be limited as everyone will know what to do. Also, a plan will help expedite the identification and neutralization of the ransomware, to reduce the impact by reacting in an efficient and effective manner.

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 responsibility and how to execute their portion of the recovery plan. A key success factor is timely and thorough internal communication within the affected organization.

Finally, the plan should include methods of communication that will be available during a Ransomware event. Corporate email and phone systems may be impacted and unavailable 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 and its data to the business, along with any upstream dependencies it relies upon. Knowing which systems in the business need attention first and how they interact with other business systems will allow for a smooth and orderly recovery. Based on each system's criticality level, document a recovery plan of what systems would be recovered in which order.

Implement tools like Rubrik Radar to identify at a file or object level what data has been infected with ransomware. Having this data during an attack will be invaluable to speeding up recovery and preserving uninfected data. Furthermore, classifying this data with a tool like Rubrik Sonar will help organizations determine if any of the compromised data is sensitive in nature, along with who has access to it.

Ensure all necessary systems and data are being protected with the required levels of data retention. Here it is better to include extra data and exclude as needed rather than only including targeted systems/data. In this manner, all data needed for recovery will be in the data protection system. Assigning Rubrik SLA Domains at the top-level of a hierarchy (i.e. vCenter Server, SQL Server, etc) is an excellent way to ensure that all existing, along with any new objects automatically inherit the data protection policy.

## KNOW YOUR RECOVERY STRATEGY

Determine what recovery methods will be used for each type of recovery. Options like Rubrik Live Mount will allow systems to be recovered in minutes as they run on the Rubrik CDM storage. This method, however, rolls entire systems back to a safe point in time. Uninfected data may be lost. File-level and database level restores for infected data may be more desirable. For more widespread attacks, Polaris Radar's Mass Recovery might be the best choice. For each situation, the appropriate method needs to be evaluated ahead of time so that it can quickly be selected 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 AppFlows you can define application level blueprints that include all the resources associated with that application to allow for unified automated recovery. Rubrik also provides a full 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 both planned and unplanned intervals. These kinds of tests are often referred to as tabletop exercises and can help IT organizations be prepared for the unexpected which can be an invaluable experience during the chaotic events caused by an attack.

Various validation frameworks are provided by the Open Source Community. One such framework is provided on Rubrik Build.

## DETECT AND ASSESS

Ransomware continues to evolve at breakneck speeds. It is reasonable to suggest that no organization is completely immune. Even with the best prevention tools, humans are undoubtedly the weakest link and make detection of an attack crucial. Once an attack is detected, determining blast radius of the attack is important so that damage can be mitigated and recovery can begin.

Rubrik Polaris Radar helps detect ransomware by leveraging a Deep Neural Network (DNN) to build out a full perspective on what is going on with the backups through analysis. The network is trained to identify trends that exist across all samples and classify new data by their similarities without requiring human input. The analysis is largely based on file system behavior and content analysis. Radar's file system analysis performs behavioral analysis on the file system metadata information looking at items like number of files added, number of files deleted, and entropy. Once outlier behavior is detected, file content analysis can be performed on the backup to identify if encryption has occurred. A list of the infected files, along with their associated probability of being infected is then presented to the system administrator.

### ISOLATE INFECTED SYSTEMS

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

For the affected systems that will be isolated, it is also recommended to carefully review snapshot expiration to ensure no valid snapshots expire which would affect data recovery. SLAs with near term retention policies should be extended to at least one year for the duration of the ransomware event. Be sure to make note of the original retention periods so that they can be set back after the ransomware event is over. As a second precaution, Rubrik Support can pause the expiration of snapshots until the event has ended. Contact Rubrik Support as soon as a ransomware attack is suspected to request this service. These steps will help prevent the accidental expiration of backups that may be needed for recovery.

### 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 time for them to respond even while the attack is still being assessed.

Engage Rubrik Support and open a priority 1 support case at your first opportunity. Even if the event is still in the investigative and/or neutralization phase, Rubrik Support may be able to be of assistance. Ensure management, technical stakeholders, and all technology vendors such as 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 is very happy to collaborate with all other technology vendors to assist in your environment's recovery. Rubrik Support always has the latest information regarding attacks and can help should you plan have gaps or you encounter a situation that wasn't planned for.

### ASSESS AND NEUTRALIZE

Ascertain the current status, impact, and scope of the situation. Failing to understand the current status can lead to restoring before the attack has been neutralized. This can reintroduce the ransomware and reinfect systems causing more damage or downtime by causing a cycle of recovering the same systems over again.

It is important to identify the scope of the attack. This includes understanding which business functions, systems, and data were compromised. Rubrik Polaris Radar can assist in determining the scope, or blast radius, of the attack so the attack can be contained and only the affected systems can be recovered. Otherwise, the safest play would be to recover all systems and data which could lead to more data loss than is necessary because systems that were unaffected by the attack would also be restored from a previous point in time. Radar's insight allows for a more surgical recovery eliminating unnecessary data loss. Radar can also automatically indicate the most recent, safe snapshot to make it easier to know the best recovery point.

Taking assessment one step further, Rubrik Polaris Sonar can be used to determine what, if any, sensitive data has been exposed or compromised. This can help prioritize recovery efforts, help to determine if additional procedures need to be followed, and if customers need to be notified.

As the scope of the ransomware attack is understood, the appropriate action must be taken to stop the spread or reintroduction of the ransomware. When possible, pause protection on only the compromised infrastructure vs. a global blanket pause in protection. This will limit the impact to only the parts of the business which were attacked. For Rubrik CDM it will also minimize impact to snapshot chains and minimize subsequent full & deltas, which can result in more cluster space being utilized and jobs taking longer to run.

As mentioned earlier, proper prioritization during recovery ensures the business can get back online as soon as possible. Once the affected systems and data have been identified, prioritize recovery based on the established recovery plan. This will allow those systems and data to be recovered quickly and in accordance with the business' needs.

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

## RECOVER

Before starting the recovery process, it's important to know what type of recovery is required. If the ransomware only attacked files on servers or user shares on a NAS, a file-based recovery method can be used. If, however, the ransomware attacked the virtual disk images for a hypervisor or the MBR records of a physical system, a full system recovery may be needed. The best practices for recovering from each of these attacks is 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 the ransomware has been neutralized. This may mean that data needs to be recovered in isolation or to new systems. Restoring systems or data before the ransomware has been neutralized may result in the system/data being attacked again. If the ransomware cannot be isolated and neutralized in a timely manner, the alternative is to recover where systems cannot be reinfected.

- **Decrypt data:** Recovery may not be necessary if there is a decryptor for the ransomware strain that was identified. When possible, decrypt existing data to prevent data loss. Decryption should be done in a safe environment. If the ransomware could not be neutralized, decryption in isolation may be required.

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

- **Prioritized recovery:** As planned for in the Prevention phase, recovery will be based on the prioritization of applications and lines of business. The prioritized list of what to recover and when should come from the Assessment phase. Ensure that foundational services required for basic functionality, such as DNS, DHCP, and Authentication, are running or restored first. Without these, the recovered systems may not function properly.

- **Use automation:** Use the tested automation that was 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 may not be required for all types of recoveries. Some examples of where automation can be particularly helpful 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 to be recovered.

- **Verify the operating system:** Verify that the underlying operating system can be trusted and was not compromised by the ransomware attack.

- **Recover to clean systems:** If the original system cannot be trusted, recover files to a known good system. This may be a newly-built system that is in isolation.

- **Identify files for recovery:** Use a tool like Rubrik Polaris Radar to identify which files were attacked by the ransomware and recover them.

- **Identify sensitive information:** Tools like Rubrik Polaris Sonar can help identify which files contain sensitive information. Ensure these files are adequately secured no matter where they are restored.

### VIRTUAL MACHINE AND DATABASE RECOVERY

These best practices apply when the VM itself cannot be used. This may happen if the NAS storage that the VM is running on has been compromised. It may also happen if the ransomware renders the VM unbootable.

- **When to use Instant Recovery:** (Smaller data sets) Recovery efforts can be sped up by utilizing Rubrik's Instant Recovery feature. This allows VMs and databases to be mounted directly from the Rubrik storage, saving the time that it takes 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 be run until a planned outage can be taken 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. This is due to the storage vMotion protocol and the ability for multiple users to access the VMs at the same time.

  Instant Recovery is a good option for smaller numbers 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 access to the database immediately needs to be weighed against having 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 the database or VM can be brought back online. This method provides the fastest data transfer performance back to primary storage and is best for recovering many VMs. The entire Rubrik cluster's performance can be used 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. Doing so should be done with extreme care. Exports will utilize the full resources of the Rubrik cluster to move data back to primary storage. Instant Recovery may have to contend with the traffic that is being recovered. This may cause degraded performance in the databases and VMs that have been Instantly Recovered. Use of this mixed workload should be evaluated on a case-by-case basis.

### HYPERVISOR MANAGER RECOVERY

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

- **vCenter Server Recovery:** Care must be taken if vCenter Server has to be recovered or when recovering VMs into a new vCenter Server. Rubrik CDM uses the 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 to create a new empty vCenter Server and recover the VMs into it. Rubrik snapshots of vCenter Server can be recovered directly to an ESXi host. Contact Rubrik Support for more details. After restoring the backup file, contact VMware Support for more details on recovery options using this method.
- **Recovery and/or re-installation of non-vSphere Hypervisor Managers(s):** When 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 an entire application is impacted.

- **Coordinate and evaluate:** Prior to 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, as well as the system dependencies required for the application. If applicable, leverage existing DR plans and runbooks to facilitate these efforts and coordinate with application owners to prepare for recovery.

  Polaris Radar and AppFlows are useful during this process. Data from Radar provides guidance to the 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 the automated 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 should be a requisite 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. This led to the creation of our resilient file system called Atlas, which stores all backup data and backup metadata in an immutable format, which means that once data is written it cannot be changed. Atlas is also a distributed 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. This gives customers an out-of-box solution that minimizes the effort needed to take their security posture to the next level. When it comes to ransomware, the Rubrik Zero Trust Architecture provides several advantages to ensure rapid recovery during an incident. The following are three key 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 the way in which this file system operates, having data immutability built-in reduces complexity, operational overhead, and increases security. Native immutability means that, once written, data cannot be changed in any way and, since Rubrik stores data in a non-native format, data cannot be easily read or exfiltrated. This is in stark contrast to most other solutions where data is readily accessible in its native format making it easy for attackers to either modify or steal the backup data.

### 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 that results in backup data being deleted. This includes outright deletion or expiration of data, 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 are controlled through a validation process within our Rubrik compliance team. If a modification to a retention locked SLA is requested by a customer, two appointed individuals from the customer's organization are required to authenticate and acknowledge the modifications with the Rubrik Support Team.

### MULTI-FACTOR AUTHENTICATION

Compromised directory service platforms and individual accounts are hallmarks in a ransomware attack strategy. Privileged accounts and directory services are of high target value during a ransomware event, and attackers will intently focus on compromising either one to gain further control of an environment. To defend against these vulnerabilities, Rubrik provides multi-factor authentication that can be enabled 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 access is granted. 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 the Rubrik platform, there is no dependency on external 3rd party identity providers allowing customers to be up and running with just a few clicks. With that said, we do support additional third-party MFA providers should you already have one in place.

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

All MFA solutions adhere to the account lockout and lockout duration policies defined within the Rubrik system. Logging for 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 potential malicious threats that are looking to crack a password 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 help protect your data while also ensuring a quick recovery from an attack.

### RUBRIK CLOUD DATA MANAGEMENT

Rubrik Cloud Data Management (CDM) is a software service built on top of the aforementioned natively immutable file system. Instead of conventional backup jobs, CDM uses a declarative policy engine to maintain a set of user-defined SLA policies. In short, 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. A single SLA policy can then be applied to any number of different applications, hypervisors, or data sets.

In addition to the natively immutable file system ensuring attackers can't modify or steal your data, CDM takes advantage of the Zero Trust Architecture to mitigate attack vectors that cyber criminals are known to exploit. This includes immutability, Retention Lock, and native TOTP for multi-factor authentication. The result is a data protection platform that has a secure profile out of the box without having to do an arduous amount of 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 data on-premises, remote and edge sites, and in the cloud. This pool of metadata also contributes to Rubrik's global search capabilities which aids in both granular recovery down to the file level, as well as an audit or discovery capabilities 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.

Next, we'll talk about how the metadata is further used by Rubrik Polaris Radar to aid in ransomware recovery.

### RUBRIK POLARIS RADAR

Rubrik Polaris Radar is a component of the Rubrik Polaris software-as-a-service (SaaS) control plane that is used to centrally manage CDM instances as well as other cloud-native offerings such as Microsoft 365 protection. As part of the Polaris SaaS platform, Radar's primary purpose is to analyze metadata from CDM in order to determine anomalous activity. Unlike many file system anomaly detection systems Rubrik uses both data change rates as well as randomness indicators (data entropy). This removes the usual false positive seen with data seasonality application. Giving Rubrik customers more confidence in the event of a notification or alert.

Through its metadata analysis, Radar provides administrators with the ability to quickly determine the blast radius of an attack resulting in a simpler, more efficient recovery. With the knowledge of what is and is not affected by an attack, administrators can then make the call of what files, folders, or systems to recover minimizing loss of data that are not affected by the attack. Other solutions force uncomfortable decisions to be made because they don't have the capability to restore individual files or confidence in their one-dimensional analysis is low. For example, the restoration of a multi-terabyte virtual machine may be required to simply recover a single file or folder.

Radar's metadata analysis means that administrators will not only know what systems are affected by an attack, but they'll also be able to surgically recover just the data they need. Recovery is fast, efficient, and minimizes the amount of data lost with unneeded image restores.

## RUBRIK POLARIS SONAR

Another component of the Polaris SaaS platform is Rubrik Polaris Sonar, a data classification tool that actively scans the contents of backup data looking for sensitive data. Sonar leverages the systems and application data within a Rubrik backup environment and uses that data to determine where sensitive data exists and who has access. Sonar can also classify sensitive data without the arduous deployment of individual agents or interfering with production systems whereas point solutions for data classification can tax the underlying infrastructure and are unwieldy to govern.

Sonar foundationally uses a concept of an analyzer and a policy. An analyzer is used to define what the system should identify in the contents of the data. Built-in analyzers are often used for common classifications (PII, PHI, NPI, etc.), but they can also be tailored with customized dictionary terms or regular expressions to meet an organization's particular needs. A policy is a logical grouping, or collection, of analyzers that provide a flexible deployment model of the definitions to be used during scan operations. Once configured, policies can be applied to protected systems and data throughout CDM.

## RUBRIK POLARIS APPFLOWS

Rubrik Polaris AppFlows is a disaster recovery orchestration tool that combines a framework for recovering applications wrapped with the added intelligence provided by Radar. AppFlows 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 Radar. 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.

AppFlows also provides multiple options to recover to different target environments, depending upon the scenario. This supports the traditional scenario of a complete site failure, but also the localized recovery scenario of a malicious attack.

# APPENDICES

## APPENDIX A - SECURITY HARDENING BEST PRACTICES

### RUBRIK SOFTWARE VERSION

- ☐ Ensure the most recent version of Rubrik has been deployed

### LOCAL ACCOUNT SECURITY

- ☐ Use unique and strong passwords
- ☐ Rotate password frequently (30-90 days)
- ☐ Syslog/Alert upon admin level login attempts and failures
- ☐ Enable MFA on local admin accounts
- ☐ Store credentials in an encrypted vault or key store
- ☐ Separate primary and secondary credential storage in separate encrypted vaults

### DOMAIN ACCOUNT SECURITY

- ☐ Only use domain accounts for application or end-user level accounts
- ☐ Align RBAC permissions by need and enforce principle of least privilege access
- ☐ Enable MFA for all domain accounts
- ☐ Enable upstream MFA with SSO provider via SAML

### AUTOMATION SECURITY

- ☐ Create new user account for each automation task
- ☐ Enforce limited scope of privileges via RBAC
- ☐ Ensure automation account does not have data expiry or SLA change permissions unless absolutely necessary
- ☐ Use TOKEN authentication over Basic authentication when programmatically connecting to Rubrik cluster
- ☐ Store TOKEN and access keys in a secure vault or key store system

### AUDITING/SYSLOG

- ☐ Enable auditing via syslog for off appliance and out of band recording of activity
- ☐ Enable TLS support encrypted syslog traffic with imported certificate
- ☐ Leverage Polaris GPS for federated reporting and auditing of events and activity logs

### SECURING NTP

- ☐ Leverage an encrypted NTP Stratum-1 time source where available
- ☐ Enable primary and secondary NTP time sources for redundancy

### SECURING IPMI

- ☐ Ensure all systems are running the latest IPMI framework (https://support.rubrik.com/s/article/000002021)
- ☐ Ensure the default IPMI interface password has been changed to a secure and complex password

### LOGIN BANNERS

- ☐ Enable pre-login banners where desired or required
- ☐ Set security classification notification banners where desired or required

### NFS/SMB SECURITY

- □ Use Secure SMB (SMB 3.0) for SMB shares utilized for Live Mounts and Managed Volumes
- □ Use IP allow-lists for all NFS archival locations and clients
- □ Use Client Patterns with Managed Volumes to define IPs or hostnames of the system being protected

### S3/ARCHIVE SECURITY

- □ Leverage the principle of least privileged access
- □ Store archival location credentials securely
- □ Store the archival location encryption key securely
- □ Lever auditing tools for continuous monitoring

### PHYSICAL SITE SECURITY

- □ Secure Rubrik nodes in locked racks or cages where possible
- □ Limit physical access to only authorized personnel
- □ Enforce principle of 3-2-1 rule for data protection (3 copies of data, 2 different locations, 1 offsite) by leveraging Rubrik site-to-site replication or CloudOut

### SECURING POLARIS

- □ Apply IP restriction to addresses from which system can access the Polaris account

## APPENDIX B - RESOURCES

- Best Practices for Ransomware Recovery with Rubrik
- 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**

20210806_v1