rubrik | Zero Trust Data Security™

FINANCIAL SERVICES

WHITE PAPER

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

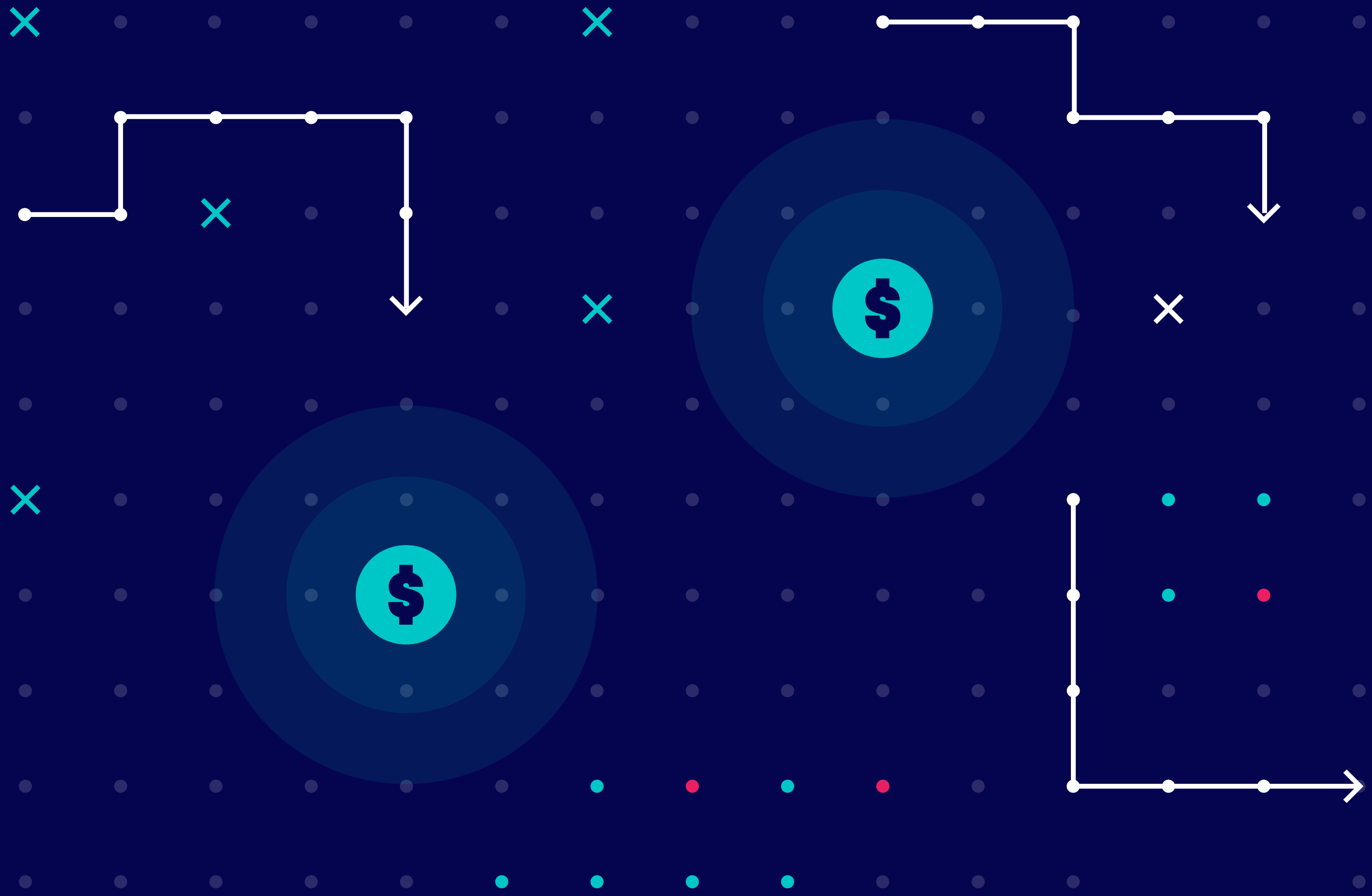


TABLE OF CONTENTS

THE NEED FOR CYBER RESILIENCE IN FINANCIAL SERVICES

Ransomware attacks have skyrocketed over the past few years and the financial services industry has been particularly hard hit. A recent report found that 74% of financial firms surveyed experienced one or more ransomware attacks in the past year, and 63% of affected firms paid a ransom. In 2021, CNA insurance reportedly paid $40 million to unlock its network, the largest ransom ever paid due to ransomware.

An analysis by Check Point Research showed that the costs associated with a successful ransomware attack go far beyond the ransom itself. Whether a ransom is paid or not, additional costs can accrue, including response and restoration/remediation costs, legal fees, and the loss of revenue and reputation due to business interruption.

The financial services sector has a particular responsibility to ensure sensitive data is safeguarded from theft and disclosure. In recognition of the heightened threat, regulators around the world are increasing requirements for the disclosure of cyberattacks. As of May 2022, the United States Federal Deposit Insurance Corporation (FDIC) requires banks to report an incident that has or is likely to affect operations, services, or the finance sector no more than 36 hours after the breach occurs. In March 2022, the Cyber Incident Reporting for Critical Infrastructure Act of 2022 was signed into law. It includes reporting mandates for financial services companies.

Given increased threat levels and new regulations, it is important to assess the cybersecurity posture of your organization to ensure that all necessary precautions are being taken to protect critical services and data—and that you are able to satisfy new reporting requirements.

Rubrik helps banks and other financial institutions keep their data safe and easy to recover. This guide explains how the built-in capabilities of Rubrik Zero Trust Data Security protect your data from ransomware. You'll also learn about best practices that make it tougher for cyber criminals to attack successfully. Best practices for recovery after an attack are also discussed.

WHY FINANCIAL SERVICES CUSTOMERS CHOOSE RUBRIK

In the battle against ransomware, traditional approaches to security and data protection are coming up short. In a 2021 survey, 51% of affected financial services organizations said attackers succeeded in encrypting data. Of those whose data was encrypted, 62% relied on backups to recover.

- **Perimeter security is not enough to keep ransomware out.** Despite massive investments in perimeter, endpoint, and application-layer defenses, attackers continue to gain access.
- **Traditional backups are vulnerable.** Many ransomware attacks target backups to prevent recovery and force payment. Traditional backup methods were not built to withstand cyber threats and are therefore vulnerable.

In the face of these realities, financial services companies need to adopt Zero Trust methods to protect against ransomware and other cyber threats.

ZERO TRUST DATA SECURITY

Zero Trust Data Security is Rubrik's patented architecture that is modeled after the Zero Trust Implementation Model from NIST (National Institute of Standards and Technology). Rubrik utilizes a purpose-built file system that never exposes your 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 are built-in, so you can quickly recover the files and workloads impacted by an attack.

SECURE BY DESIGN

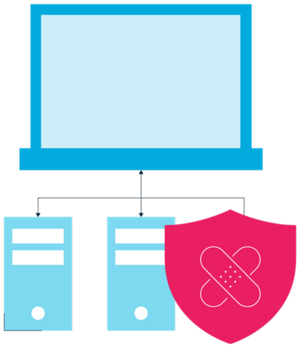
Rubrik's founders made security a core design principle from the very beginning of product development. They started with a custom file system to provide out-of-the-box immutability. And they also gave Rubrik a logical air gap to protect data from attackers and rogue admins. Additional protections were put in place such as a robust RBAC system, API authentication requirements, and disabling 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 have not been tampered with. As customer needs and cyber threats have continued to evolve, 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.

When PT BFI Finance Indonesia Tbk (BFI) was facing serious data protection challenges it turned to Rubrik. Now they dedicate just one or two IT staff to daily data backups. In recognition of rising issues of phishing, malware, and ransomware, BFI enabled Rubrik's advanced cybersecurity capabilities after it saw attempted attacks. With Rubrik, BRI improved efficiency by 60%, reduced staff costs by 40%, and achieved instant restores for VMs and critical SQL databases.

Backup data truly is the last line of defense and the key to recovering from a ransomware attack. Rubrik's approach makes it easy for financial institutions to achieve a superior security posture. Rubrik Zero Trust Data Security keeps the data of banks and other financial institutions safe and makes it easy to quickly recover from an attack.

SECURE DEPLOYMENT BEST PRACTICES

There are a set of general best practices financial services companies should follow to minimize risk from cyber threats. These practices are discussed below, and we provide a 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 continuously patch infrastructure systems to keep them up to date, you can mitigate many common threats. This includes operating systems (Windows, Linux, macOS, etc.), appliances, storage, networking, and your servers' BIOS and firmware. Financial services organizations should work with all their hardware and software vendors to put documented procedures in place to patch systems in a timely manner.

SECURE ACCESS TO SYSTEMS

Access to systems must be tightened through authentication and authorization mechanisms. Authentication is how a user or service identifies itself to a system. There are some easy ways to provide secure authentication, starting with not allowing unauthenticated (or anonymous) access. In other words, all users and services must be required to provide authentication 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 they know) as well as a fingerprint (something they 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 provides MFA natively. It can be set up in just a few seconds, dramatically increasing the security of your backup data.

Authorization grants authenticated users and services access to system resources. 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 to configure RBAC. Financial services organizations should ensure that all 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 access to the least amount of resources they need to do their jobs. In other words, don't grant users more access than they need to prevent them from accidental or intentional misuse of a system. Attacks that gain access through a compromised account often try to exploit relaxed access privileges to do additional damage.

Always be sure network access is locked down by **disabling unused ports** on systems, properly 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 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.

ENABLE AUDITING

Restricting system and data access is only part of the solution when securing an environment. Financial services organizations are required to audit operations regularly to ensure compliance. Auditing provides visibility of all accesses, authorizations, and other activity within a system. This data can be as simple as an audit trail of who accessed what and when or 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. Financial services companies should employ centralized logging that can not only ingest data but also provide real-time alerting and analysis that provides actionable insights.

AUTOMATE EVERYTHING

Automating tasks in IT infrastructure is not just about saving time. Automation makes tasks repeatable and self-documenting. These aspects of automation are often overlooked, or their value is 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 to support financial applications. Be sure to choose tools and infrastructure that have APIs to support automation.

As with other activities, automation methods must be secure. 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. It is a recommended best practice to use token-based authentication for automation accounts to reduce the risk of compromised credentials. Be sure to store tokens in a secure vault so that an attacker can't stumble upon them in clear text in a script.

RECOVER FROM RANSOMWARE ATTACKS WITH RUBRIK

In 2020, global foreign exchange and travel insurance company, Travelex paid a $2.3 million ransom to recover from ransomware that had encrypted their worldwide network, deleted backup files, and copied sensitive personal data. The interconnections between Travelex and the international banking system created the potential for paralyzing downstream effects for customers and partners.

Rubrik understands that a ransomware attack is one of the worst-case recovery scenarios that a bank or financial services company can face. An impacted company will likely be dealing with widespread business issues resulting from the attack. Rubrik has developed a set of best practices to help financial services customers plan for, identify, and remediate attacks.

Plan & Prepare
Detect & Assess
Recover

The next several sections describe these steps in detail as well as specific actions for each phase. While the phases described are applicable to any company affected by ransomware, we've noted some specific considerations for financial services as well as areas where Rubrik capabilities are of benefit.

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 important.

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 can be valuable. By following an established plan during an attack, everyone knows what to do, limiting confusion. Having a plan helps expedite the identification and neutralization of the ransomware.

The plan should identify key stakeholders across management, public relations, IT, system/application teams, etc. who will be responsible for executing and managing your incident response. Make sure each person knows their responsibilities and how to execute their part of the recovery plan. Timely and thorough internal communication is a key success factor.

Finally, your plan should include methods of communication that will remain available during a ransomware event. Corporate email and phone systems may be impacted and unavailable. Provide for alternate means to communicate 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. Knowing which systems need attention first and how they interact with other business systems will allow for a smooth and orderly recovery. Based on each system's priority level, document a recovery plan specifying which systems should be recovered in which order. Tools such as Rubrik Sensitive Data Monitoring & Remediation allow you to identify where sensitive PII and other critical data are stored.

Implement tools such as Rubrik Ransomware Monitoring & Investigation to identify at a file or object level what data has been infected with ransomware. Having this data during an attack is invaluable for speeding up recovery and preserving uninfected data. Furthermore, classifying data with a tool like Rubrik Sensitive Data Monitoring & Remediation will help you 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. With this approach, all data needed for recovery will be in your data protection system. It's important that any backup method you use is as immune from ransomware as possible. Rubrik Zero Trust Data Protection ensures that backups are air-gapped, immutable, and access-controlled. For Rubrik customers, assigning Rubrik SLA Domains at the top-level of a hierarchy (for example vCenter Server, SQL Server, etc.) is an excellent way to ensure that all existing objects, along with any new objects, automatically inherit the appropriate data protection policy.

ENSURE COMPLIANCE

As ransomware risks increase, banks and financial services organizations are required to comply with additional industry and government regulations designed to strengthen cyber protection. Compliance necessitates a dedicated effort to not only follow appropriate regulatory requirements, but to provide external auditors with proof that you are complying with multiple international regulations such as GDPR and the recent U.S. Cyber Incident Reporting for Critical Infrastructure Act.

Rubrik can help your organization protect, manage, and monitor data across all environments and automate your data retention and archival policies. A one-click procedure produces SLA reports that show proof of compliance with data retention and deletion policies.

PLAN YOUR RECOVERY STRATEGY

Determine what recovery methods will be used for each type of system or application. Options like Rubrik Live Mount can allow systems to be recovered in minutes. 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, Rubrik Mass Recovery may be the best choice. The appropriate method needs to be evaluated ahead of time so that it can be quickly selected during an attack.

Once a recovery plan and prioritization have been established, automation is the next step in building a robust recovery capability. Automation minimizes the risk of human error, speeds up recovery, and aids in progress tracking. Rubrik Orchestrated Application Recovery works in conjunction with Ransomware Monitoring & Investigation to accelerate recovery. It simplifies disaster recovery planning, testing, and execution, with orchestration of DR failover/failback using application-level blueprints that include all the resources associated with an application. 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.

TEST YOUR PLAN

Periodically test data recovery to ensure you are prepared for an actual incident. Unless you test your recovery plan, you have no assurance that recovery will work as expected if an attack happens. Testing also gives staff the experience and confidence that an attack can be successfully and quickly remediated. Tests should be as realistic as possible without disrupting business operations and performed at both planned and unplanned intervals. These types of tests are often referred to as tabletop exercises. They help financial services organizations satisfy regulatory requirements, prepare for the unexpected, and provide invaluable experience during the chaos created by an actual attack.

Various validation frameworks are provided by the Open Source community.

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 remain the weakest link, making detection of an attack crucial. Once an attack is detected, determining the blast radius of the attack is necessary so that damage can be mitigated, and recovery can commence.

If ransomware enters your network, processes and tools must be put in place to detect it before it has fully activated. The first line of defense is from real-time detection tools. Analysis of backup data is the second line of defense. Rubrik Ransomware Monitoring & Investigation helps detect the effects of ransomware using a deep neural network (DNN) to analyze what is going on with your backups. The network is trained to identify trends and classify new data based on similarities without requiring human input. The analysis is largely based on file system behavior and content analysis. Behavioral analysis on file system metadata looks at indicators like number of files added, number of files deleted, and entropy. Once outlier behavior is detected, file content analysis can be performed to determine if encryption has occurred. A list of infected files, along with their associated probability of being infected, is then presented.

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. Rubrik Threat Monitoring and Hunting can be used to identify the specific strain of malware. Tools such as Rubrik Threat Containment can help make sure that backups that contain infected data remain isolated and aren't restored.

For any systems that have been affected, snapshot expiration should be carefully reviewed to ensure that no valid snapshots expire that could affect your ability to 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 note the original retention periods so that they can be re-established after the ransomware event is over. As an additional 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 a ransomware attack as quickly as possible so that they can start to execute their portions of the recovery plan. Notification should include any regulatory entities you are legally required to report to. Early notification of stakeholders, Rubrik support, and other vendors—even while the attack is being assessed—will allow time for everyone to respond.

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

ASSESS AND NEUTRALIZE

When a ransomware attack occurs, it's essential to ascertain the attack's current status, impact, and scope. Failing to understand attack status can lead to restoring before the attack has been neutralized. If this happens you run the risk of reintroducing the ransomware and reinfecting systems and causing more damage or downtime as you recover 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 Ransomware Monitoring & Investigation can assist in determining the scope, or blast radius, of the attack so the attack can be contained, and only the affected systems have to be recovered. Otherwise, the safest option is to recover all systems and data. This can lead to more data loss than necessary since unaffected systems will be restored to a previous point in time. Rubrik provides insights that allow for a more surgical recovery, eliminating this unnecessary data loss. Ransomware Monitoring & Investigation can also automatically indicate the most recent, safe snapshot to make it easier to identify the best recovery point. Rubrik Threat Monitoring & Hunting determines what is causing the anomalies that Ransomware Monitoring & Investigation detects, ensuring that specific threats are appropriately contained.

Taking assessment one step further, Rubrik Sensitive Data Monitoring & Remediation 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 data protection. This will limit the impact to only the parts of the business which were attacked. For Rubrik Zero Trust Data Protection, it will also minimize impact to snapshot chains and minimize subsequent full and 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 affected systems and data to be recovered quickly and in accordance with your business needs.

Finally, determine if local copies of the necessary backups are available or if they will need to be brought back from archives. The recovery point that was established for each system based on when infection occurred helps to determine this. Also, verify that the archival and/or cloud data has not been compromised. If it is compromised, 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, you can use a file-based recovery method. 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 below, along with general best practices for all recoveries.

Export

Traditional recovery process involving copying a complete point-in-time backup from the Rubrik platform back to production. Results in a new instance of the projected object.

In-Place Recovery

Rubrik circulates only blocks which have changed between production and the desired point-in-time. Copies only changed blocks back to the original source.

Instant Recovery

Provides near-zero RTOs by temporarily leveraging the Rubrik platform to host the recovered point-in-time while powering off and deprecating original instance. A new instance is created on the source, utilizing Rubrik as the underlying storage platform.

Live Mount

Similar to Instant Recovery in the fact the Rubrik platform is leveraged to host the underlying storage for the desired point-in-time, however the original instance remains untouched in the event of a Live Mount.

File-Level Recovery

Allows for the restoration of individual files and folders from the desired point-in-time backup. Files may be restored back to the original, or a new location. When restoring from archive, only those identified blocks making up the file are retrieved from the backup.

GENERAL BEST PRACTICES

These best practices apply to all recovery scenarios.

- **Begin recovery operations only 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 only alternative is to recover where systems cannot be reinfected.
- **Recovery may not be necessary if there is a decryptor for the ransomware strain that was identified:** If a decryptor exists, 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.
- **Assess how much isolation you need for recovery:** Often ransomware infections 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 gain access is the best prevention from a secondary attack.
- **The order of recovery should be based on priority.** A prioritized list of applications and lines of business to recover should have been created during assessment based on the recovery plan created during the Preparation 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.
- **Automated recovery can reduce downtime and risk of human error.** Automation tools such as Rubrik Mass Recovery and Rubrik Orchestrated Application Recovery and tools/scripts that utilize Rubrik's APIs and SDKs will speed up recovery times. Use the tested automation that was developed during the Preparation phase. Proven and tested automation will also improve the accuracy of your recoveries.
    - 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 file sets across multiple servers to at or near the same point in time.

FILE-ONLY RECOVERY BEST PRACTICES

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.

- **Identify sensitive information:** Tools like Rubrik Sensitive Data Monitoring & Remediation can help identify which files contain sensitive information. Ensure these files are adequately secured no matter where they are restored.

- **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 Ransomware Monitoring & Investigation to identify which files were attacked by the ransomware and recover them.

VIRTUAL MACHINE AND DATABASE RECOVERY BEST PRACTICES

These best practices apply when the VM itself cannot be used. This may happen if the 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 of VMs:** Instant Recovery is a good option for a smaller number of VMs, which may include mission-critical systems. A Rubrik cluster is not a substitute for primary storage. Care should be taken with Instant Recovery to make sure the Rubrik cluster is not overloaded. For VMs, the time and resources required to move VMs back to primary storage with Storage vMotion 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 of databases:** 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 moved to primary storage with Storage vMotion. 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 a single Rubrik Cluster, but it 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 instances with the appropriate support team to ensure a smooth recovery.

- **vCenter Recovery:** Care must be taken if vCenter has to be recovered or when recovering VMs into a new vCenter. Rubrik 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 has been compromised, it is better to restore it from backup than to create a new empty vCenter 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:** 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 recovery of the individual VMs.

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.

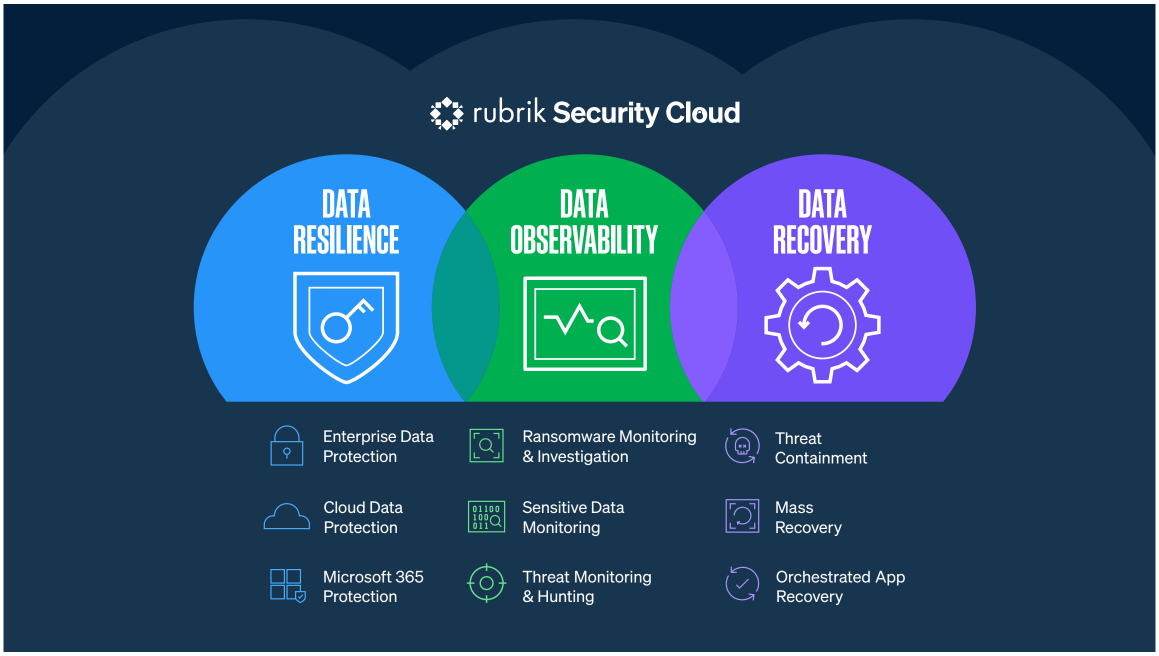
- **Coordinate and evaluate:** Prior to any orchestrated recovery of an application or group of systems, ensure that all infected systems are isolated from the production environment. Validate your target recovery location for compute and storage resources required for the recovery. Take note and understand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

  Utilize Rubrik Ransomware Monitoring & Investigation and Orchestrated Application Recovery: For Rubrik customers, data from Ransomware Monitoring & Investigation can provide guidance for the best point in time from which to recover while minimizing data loss. The target resources and application dependencies are already configured within an application blueprint, providing 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 pre-requisite before sign-off. These policies often include: user authentication, data validation, and system dependency checks noted earlier.

RUBRIK ZERO TRUST DATA SECURITY: HOW RUBRIK SECURES DATA AND IDENTIFIES RANSOMWARE

At Rubrik, cybersecurity and ransomware protection are based on zero trust principles. No one is trustworthy. No user. No application. No device. Zero trust is essential to protect the backup data of banks and financial services companies against cyber threats. Only users that have been authenticated using multi-factor methods get access to your backup data—and only to the data they need. Permissions and access are strictly limited, and users are unable to do anything malicious to stored data, ensuring backups are always available for recovery.



The Rubrik Security Cloud enables you to secure data across enterprise, cloud, and SaaS applications, keeping your data secure against cyber threats, proactively monitoring risks to your data, and facilitating fast recovery. Rubrik divides its ransomware capabilities into three categories:

- **Data Resilience.** Cyber-proof your data with air-gapped, immutable, access-controlled backups
- **Data Observability.** Continuously monitor your data for ransomware, remediate sensitive data exposure, and find indicators of compromise
- **Data Recovery.** Surgically and rapidly recover your apps, files or users while avoiding malware reinfection

Data Resilience and Data Observability are critical to Data Recovery. Data Resilience defends financial services data against threats, so you always have trusted backup data you can recover from. Data Observability allows you to monitor for cyber threats continuously and analyze data to detect threats quickly, so business operations can be recovered if necessary.

THE RUBRIK DATA SECURITY COMMAND CENTER

The Rubrik Data Security Command Center (DSCC) provides a single interface that allows authorized users to access the capabilities of Rubrik Zero Trust Data Security to manage platform security, data protection and recoverability, ransomware protection, and sensitive data protection.

The DSCC can monitor and manage security configurations, access controls, audit logs, encryption scanners, security logs, and more. It can also perform intensive analysis using Rubrik's Ransomware Monitoring & Investigation and Sensitive Data Monitoring services. All information is presented via a simple-to-use SaaS-based console.

DATA RESILIENCE

Legacy backup solutions can be unreliable, difficult to manage, and often result in failed backups. These limitations put banks and financial services businesses at risk of non-compliance. Valuable financial data and personally identifiable information (PII) must be protected from compromise to ensure an effective ransomware response. Rubrik Zero Trust Data Protection ensures that backup data is always available, immutable, and logically air gapped, so it cannot be modified, encrypted, or deleted by ransomware.

Financial institutions benefit from Rubrik's military grade encryption and immutable file system. Because every file is read-only, cybercriminals cannot delete or use ransomware to encrypt your backups.

Multi-factor authentication (MFA) is used to reduce intrusion threats that could compromise backup data. Role-based access control (RBAC) with granular role definitions further reduces the risk of a data breach. Rubrik retention lock prevents any single person from clearing or shortening retention policies or deleting snapshots, archives, or replication locations.

Enterprise Data Protection

Cloud Data Protection

Microsoft 365 Protection

Safeguard your data so it can always be available for recovery

- Immutable from the first copy
- Append Only File System
- Logical Air Gap – No Open Protocols
- Encryption Everywhere
- Zero Trust by Design (MFA)
- Retention Locks and Two-Person Integrity

A secured and isolated off-site location for data backup is an important part of a comprehensive data protection strategy. Rubrik Cloud Vault extends the capabilities of Rubrik Zero Trust Data Protection and Rubrik's Secure Data Layer to isolated, off-site cloud archival.

Cloud Vault is a fully managed cloud service, enabling you to safely archive backups in the cloud so that a secure and isolated copy of backup data is available for recovery in the event of a malicious attack or natural disaster.

DATA OBSERVABILITY

Data Observability is critical in the battle against ransomware. A Rubrik backup isn't just a passive repository. Your backup data is actively scanned and analyzed as it is backed up. This provides information about where data is located, what it is, and how it has changed since the last snapshot, providing enormously useful intelligence for defense against cyber-attacks. Unique scanning and indexing spots patterns that may indicate an attack and allows organizations to understand what attackers have done so they can stop an infection and easily recover.

The Rubrik Data Observability Engine utilizes a portfolio of prebuilt scanners, combined with machine learning algorithms, to turn Rubrik backup systems into active weapons for cyber defense. Based on years of R&D and customer insights, Rubrik enables customers to leverage data-level insights to identify when, where, and how cyber threats have impacted systems, so they can be remediated as quickly as possible.

Sensitive Data Monitoring

Threat Monitoring & Hunting

Ransomware Monitoring & Investigation

Monitor data risks continuously and remediate threats quickly

- High Fidelity ML Model using Data Time-Series
- Full data view User/App/Content over time
- Anomaly and encryption detection vs baseline
- Data Insights integrate into your SecOps tools

Sensitive Data Monitoring & Remediation scans backup snapshots to discover, classify, and report on sensitive data in files and applications using pre-built policy templates to identify common data types based on regulations and standards. Rubrik uses GDPR, PCI-DSS, HIPAA, and GLBA, or custom dictionaries, expressions, and policies. It employs various techniques to minimize false positives. With almost no learning curve, users can set up policy-driven automation via the Rubrik UI to gain greater insights. There is nothing to install, no agents, and no production impact. Rubrik's reporting and compliance tools make it easy for financial services firms to demonstrate compliance. For example, Compeer Financial, one of the largest US farm credit associations, relies on Rubrik to prove to regulators that it is backing up data and storing it securely.

As part of Data Observability, Sensitive Data Monitoring for Microsoft 365 builds on the collaboration between Rubrik and Microsoft to discover and classify sensitive data within Microsoft 365 to better assess risk and help maintain compliance with regulations.

Ransomware Monitoring & Investigation enables teams to discover attacks quickly so they can be contained. It accomplishes this by monitoring for encryption, analyzing unusual access patterns, and identifying signs of potentially malicious activity in your backup data.

- **Machine-learning-based anomaly detection** discovers potential threats automatically. Rubrik algorithms analyze application metadata to establish normal baseline behavior. Systems are proactively monitored by looking at behavioral patterns and flagging any activity that varies significantly from the baseline. Ransomware Investigation analyzes file change rates, abnormal system sizes, and entropy changes. If an anomaly is detected, it provides alerts to the unusual behavior via the UI and by email. Rubrik continuously refines its anomaly detection model to stay ahead of the most advanced threats.
- **Rubrik determines exactly what has been affected** and makes recommendations about the best recovery points. This enables teams to quickly identify and locate the applications and files impacted by ransomware, so only the files and applications that have been affected have to be restored.
- **API integration** with popular security operations tools enables better collaboration between IT and security groups for faster incident response.

Rubrik Threat Monitoring & Hunting provides tools to scan for malware to avoid reinfection during recovery. Threat Hunting discovers threats by analyzing backups using file patterns, file hashes, and YARA rules for indicators of compromise allowing financial services institutions to identify uninfected backups and avoid the risk of reintroducing malware.

DATA RECOVERY

Rubrik Threat Containment isolates infected snapshots to reduce the risk of reintroducing malware during a recovery operation. Individual files or entire snapshots can be quarantined. Access to quarantined data for investigation is limited using granular role-based access control.

After a ransomware attack, Rubrik Mass Recovery helps organizations rapidly recover their systems, restoring VMs and applications within minutes. A flexible recovery approach helps teams recover only affected files, ensuring that RTOs can be met.

Rubrik Orchestrated Application Recovery is an integrated disaster recovery solution that helps teams rapidly recover applications from a ransomware attack. With an intelligent design and focus on data security, it simplifies disaster recovery planning, testing, and execution, providing granular

Threat Containment

Mass Recovery

Orchestrated App Recovery

Quarantine malware and automate recovery so business operations can be restored quickly

- In-Place Recovery-of only changes
- Instant Recovery/Live Mount gracefully migrates back to production storage
- Automated orchestrated recovery of VMs (War Time for sub 10 min recovery)
- Peace time isolated recovery testing for proactive testing
- Surgical Recovery Malware Free "Last Known Good Copy"

and efficient recoveries. It provides orchestration of DR failover/failback and works together with Ransomware Monitoring & Investigation to radically simplify recovery. As a result, you can eliminate multiple point solutions, management complexity, and unnecessary costs.

While all financial services companies have to cope with the reality of ransomware threats, many organizations face heightened danger from natural disasters as well. With Rubrik, South Florida's Grove Bank & Trust has the flexible tools it needs to recover from hurricanes and ransomware attacks. Their old backup solution was hard to use and made it difficult to backup and archive data for multiple years. Rubrik makes it much easier to prove to regulators that they are backing up critical data, that they can recover that data when necessary, and that they are performing adequate recovery testing.

EMBRACE ZERO TRUST

Zero Trust security is vital in the escalating threat environment that banks and other financial institutions face. Cyber criminals are targeting financial services companies as a growth strategy. It may be time to rethink data protection, implement new backup and recovery processes, and make the necessary IT investments to secure high-risk data and better protect your organization against serious breaches of sensitive data and ransomware. With Rubrik Zero Trust Data Security, you can more quickly detect attacks, assess the extent of the damage, and recover quickly. As a result, your organization is better able to comply with changing threats and new regulations, while controlling the costs of cyber risk management.

APPENDIX A - SECURITY HARDENING BEST PRACTICES CHECKLIST

RUBRIK SOFTWARE VERSION

- Ensure the most recent version of Rubrik software 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 a 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 Rubrik Security Cloud 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

- REnsure legacy SMB protocols are disabled and Secure SMB (SMB 3.0) is being utilized.
- 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
- Leverage 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 RUBRIK SECURITY CLOUD

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

rubrik

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

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

wtpr-best-practices-guide-prepare-recover-ransomware-finserv / 20220815