rubrik | Zero Trust Data Security™

FINANCIAL SERVICES

WHITE PAPER

Definitive Guide to Zero Trust Data Security for Financial Services

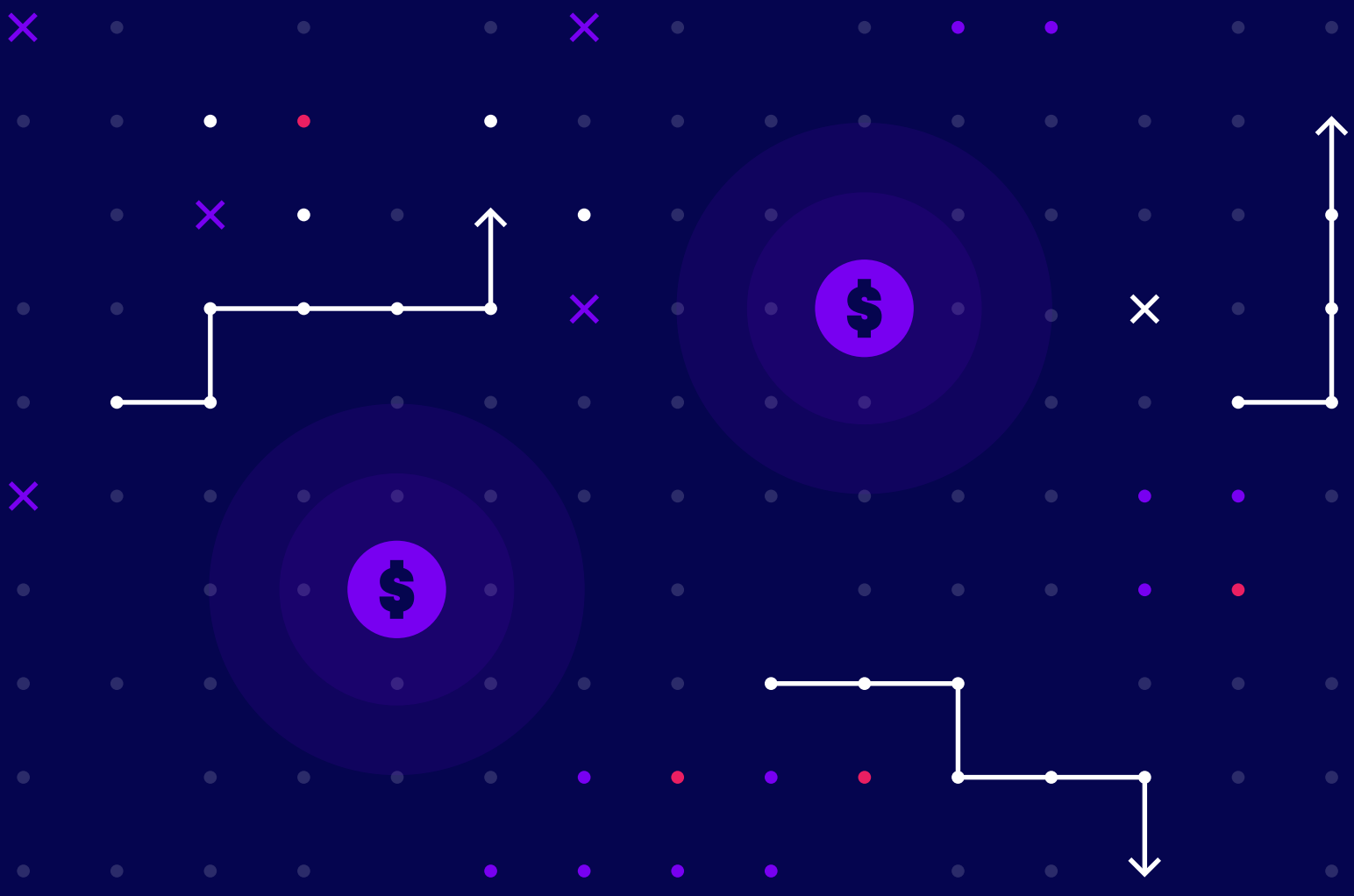


TABLE OF CONTENTS

TABLE OF CONTENTS

INTRODUCTION

Ransomware attacks are growing at an alarming rate. You can't turn on the news without hearing about yet another organization that has been affected. Financial services companies have been particularly hard hit. Attacks against banks were up a staggering 1,318% from 2020 to 2021.

$18.9M

average loss to a financial services company in the event of a ransomware attack

2nd

highest cost of a data breach per industry

1,318%

increase year over year in ransomware attacks

HIGH VULNERABILITY

The financial sector is under attack because, with large amounts of sensitive information—and operations that are increasingly digital—there are significant opportunities for large payouts. Financial firms are vulnerable to double-extortion attacks where data is stolen prior to encryption, and cyber criminals threaten to release sensitive data if ransoms aren't paid.

NEW REGULATIONS

In response to the heightened threat, regulators around the world are increasing requirements for disclosure of cyberattacks. In the United States, the 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.

The current geopolitical environment is also heightening risks. In March 2022 the Biden Administration issued a statement encouraging all private sector companies to strengthen cyber defenses and signed into law the Cyber Incident Reporting for Critical Infrastructure Act of 2022 which includes reporting mandates for financial services companies.

IS YOUR ORGANIZATION PREPARED?

All financial services companies must audit operations regularly to ensure compliance. Given elevated threat levels and new regulations, it's important to assess your cybersecurity posture to ensure that you are taking all necessary precautions to protect critical services and data—and that you are able to satisfy new reporting requirements. In the battle against ransomware, traditional approaches to security and data protection are coming up short.

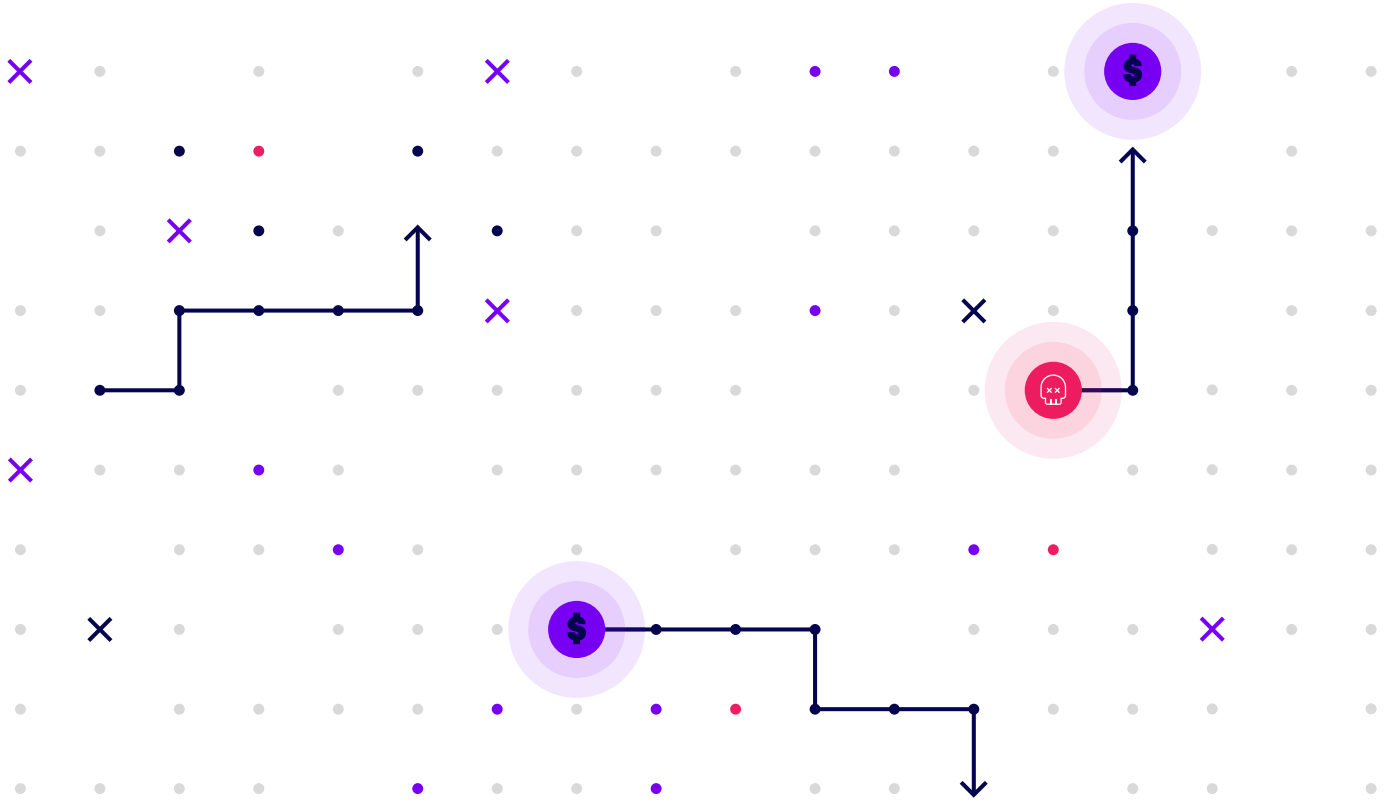
- **Perimeter security is not enough to keep ransomware out.** Despite massive investments in perimeter, endpoint, and application-layer defenses, attackers continue to gain access.
- **Traditional backups are vulnerable.** Many ransomware attacks target backups to prevent recovery and force payment.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

This ebook explores the use of Zero Trust methods to protect backup data and minimize the impact of ransomware attacks, and it explains the foundational technologies behind Rubrik Zero Trust Data Security, describing how Rubrik keeps the data of banks and financial institutions safe and makes it easy to recover.

In a recent survey, 34% of financial services organizations surveyed were hit by ransomware in 2020, and 51% of the organizations impacted said the attackers succeeded in encrypting data. Of those whose data was encrypted, 62% used backups to recover.

Source: State of Ransomware in Financial Services 2021



BFI FINANCE

"Our implementation was previously legacy tape based. We had to allocate two to three senior IT staff to manage these crash-prone data backup tasks Now we can dedicate just one or two IT staff to the daily data backup process. Recovery times have also improved tremendously, from hours in the past down to just minutes."

Alexander Ekanayake
CTO, BFI Finance

READ FULL CASE STUDY

INCREASING SECURITY AND PERFORMANCE WITH RUBRIK

PT BFI Finance Indonesia Tbk. (BFI) is one of the oldest finance companies in Indonesia. When the company was facing data protection challenges—with lengthy tape backup and recovery times, error prone recovery processes, and high operating costs—it turned to Rubrik.

"Our implementation was previously legacy tape based. We had to allocate two to three senior IT staff to manage these crash-prone data backup tasks," said Alexander Ekanayake, CTO, BFI. With Rubrik, "we have reduced our costs and human resource utilization by up to 40%. Now we can dedicate just one or two IT staff to the daily data backup process. Recovery times have also improved tremendously, from hours in the past down to just minutes."

While cybersecurity was not the company's initial concern, the issues of phishing, malware, and ransomware have mounted quickly. "Cyber threats are real and escalating, especially in the pandemic where threat actors have heightened monetary needs [and are] exploiting the reduced resources of many organizations around the world," continued Ekanayake. "We immediately saw the inherent benefits of Rubrik." BFI enabled Rubrik's advanced cybersecurity capabilities after it saw attempted attacks against some of its nodes.

RUBRIK BENEFITS

60%

Improved efficiency by 60% (from days down to hours)

40%

Reduced staff costs by 40%

Seamless

Convenient management and seamless automation

Instant

Instant restore of VMs and SQL databases

WHY ZERO TRUST MATTERS TO YOU

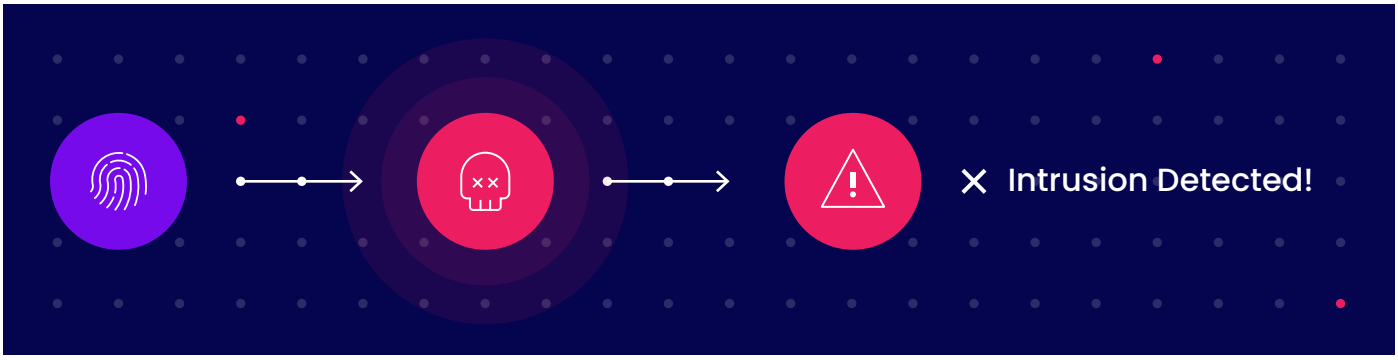
A Zero Trust architecture assumes all users, devices, and applications are untrustworthy and can be compromised. Only users that have been authenticated using multi-factor methods get access to data—and only to the data they need. Permissions and access are strictly limited, and users are unable to do anything malicious to stored data.

The Zero Trust model is defined by the National Institute of Standards (NIST), in the NIST SP 800-207 Zero Trust Architecture Specification. As NIST describes it, Zero Trust comprises "an evolving set of cybersecurity paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources."

When it comes to protecting the backup data of financial services companies, Zero Trust Data Security relies on six distinct capabilities.

Ransomware-related activity reported to the U.S. Treasury during the first 6 months of 2021 totaled $590 million, up from the $416 million reported for all of 2020.

Source: Ransomware Trends in Bank Secrecy Act Data



REDUCE INTRUSION RISK

The first line of defense in Zero Trust is preventing attackers from gaining access to data in the first place. There are multiple methods that banks should employ to reduce unauthorized access:

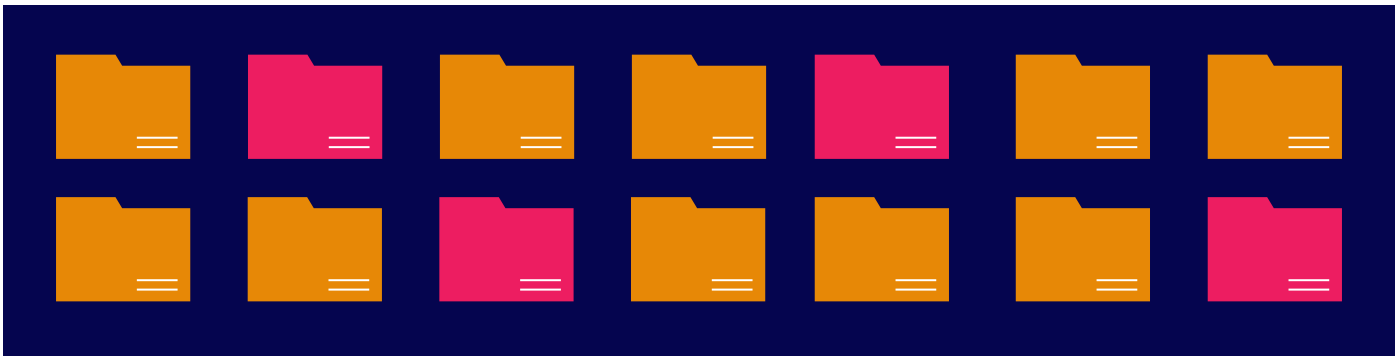
- **Multi-factor authentication (MFA).** MFA validates a combination of factors requested from a user. The most common factor is a user's credentials. The second factor might be a Time-based One-Time Password (TOTP), biometric identifier, or key card. More factors can be used to further increase security.
- **Role-based access control (RBAC).** RBAC restricts access based on an individual's role within your organization or based on a service account's function. (Service accounts are created to allow third-party tools to have the necessary privileges to perform their functions.) Limiting access based upon role can greatly reduce the amount of data affected if a ransomware attack or other intrusion occurs.
- **Least privileged access.** Employees and services only get access to the resources necessary to perform their specific job duties—and nothing more.

SAFEGUARD BACKUP DATA FROM COMPROMISE

The next line of defense is to ensure your backup data is protected to the greatest extent possible—even when ransomware gains access:

- **Encryption.** Ensures that if malware or a hacker gains access to your backup data, it cannot be read, reducing the risk that sensitive customer and employee data or valuable intellectual property (IP) will be breached.
- **Immutability.** Because the goal of ransomware is to encrypt data (even if it's already encrypted) and make it inaccessible, immutability is necessary to protect backup data. An immutable backup cannot be modified in any way or deleted—either for a set period of time or forever.

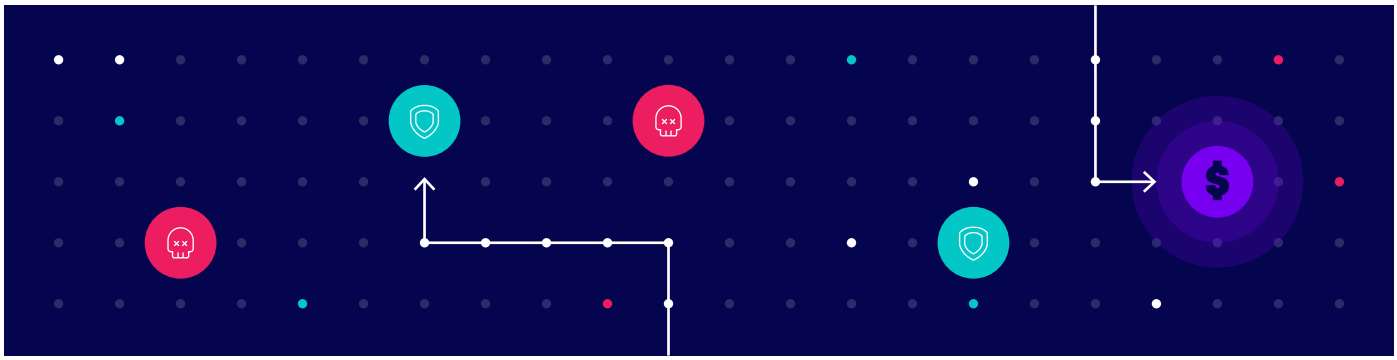
Combining encryption and immutability ensures that even if ransomware gains access to your data, it can neither render your backups unreadable nor exfiltrate data that compromises your company, your employees, or your customers.



DETECT ANOMALOUS ACTIVITY FOR FASTER INVESTIGATION

Delays in detection give hackers more time to find and exploit vulnerabilities within your operations and can extend the time needed to recover fully.

Modern technologies that leverage machine learning can help detect security threats sooner. Backups include rich metadata that can be securely analyzed to detect and generate alerts on anomalous activity.



DISCOVER AND MANAGE SENSITIVE DATA

Another important line of defense is to identify and manage sensitive data assets ahead of time. At a minimum, this should include ensuring compliance with the laws and regulations of the region(s) in which you operate (such as GDPR and CCPA), industry-specific regulations like H PCI-DSS, and your own internal governance. If you suffer a ransomware attack, being out of compliance only adds to your troubles.

In practice, you need to make sure that you:

- Properly protect all new workloads
- Enforce data retention periods
- Have the ability to quickly identify any sensitive data that may have been exfiltrated

CONTAIN INCIDENTS AND RECOVERY QUICKLY

INCIDENT CONTAINMENT

Incident containment ensures that after an attack occurs you can fully contain it and avoid reinfection. Once ransomware enters your systems, it is necessary to quickly identify the scope of the infection, isolate all infected systems, and track signs of the infection backwards in time to the point of infiltration.

RAPID RECOVERY

Rapid recovery is essential to get your business back on its feet as quickly as possible with minimal disruption to business functions. No organization is immune to cyber attacks, but a long recovery time after an incident may create significant impacts to your business and its reputation.

InLife
INSULAR LIFE

"I have seen Rubrik's instant recovery capabilities and how simple this feature is to use. This is exactly what we need to be as efficient as possible. Rubrik has helped make my team more efficient in complying with data archiving requirements."

Larry C. Delos Santos
SAVP, Head of Technical Services, Insular Life

READ FULL CASE STUDY

LIFE INSURANCE COMPANY ACCELERATES RECOVERY, SIMPLIFIES COMPLIANCE

Insular Life is the first and largest Filipino life insurance company with over 110 years of experience providing financial protection, savings, investments, and retirement solutions to customers.

Rubrik has enhanced Insular Life's ability to restore data instantly, as well as ensure data availability at all times. "I have seen Rubrik's instant recovery capabilities and how simple this feature is to use. This is exactly what we need to be as efficient as possible," said Larry C. Delos Santos, SAVP, Head of Technical Services for Insular Life's Information Technology Division.

Rubrik helps Insular Life adhere to regulatory compliance requirements for data backup, disaster recovery, and archiving. "Rubrik has helped make my team more efficient in complying with data archiving requirements," added Delos Santos. "We can stay within our committed industry availability requirements with quicker maintenance periods, which has a big impact in terms of system availability to internal users."

RUBRIK BENEFITS

83%

Management time savings of 83% (mins vs. hours)

90%

90% reduction in data center footprint

Instant

Instant server recovery

RUBRIK ZERO TRUST DATA SECURITY

Modeled after the Zero Trust Implementation Model from NIST, Rubrik Zero Trust Data Security implements all of the capabilities just described, providing maximum protection against hackers and rapid recovery from ransomware attacks for financial services companies.

Data written to the Rubrik system cannot be modified, deleted, or encrypted by an attack, ensuring that backup data is readily available for recovery. Multiple expert-guided recovery options—including Live Mount, Mass Recovery, and Orchestrated Application Recovery—enable you to quickly recover files and workloads impacted by an attack.

NWB BANK

"Live Mount is one of our team's favorite features. We can restore a full virtual machine (VM) from a backup in a matter of seconds."

Rob Heemskerk
Network Engineer, NWB Bank

Rubrik Zero Trust Data Security goes to the heart of data protection—keeping hackers out of your backup system, identifying ransomware activity, and making sure all data has a clean backup that can be recovered quickly.

Rubrik Zero Trust Data Security Benefits	
IT Teams • Protect critical data from ransomware attacks • Recover data and applications quickly • Avoid ransom payments	**Security Teams** • Leverage secure backup data for attack forensics • Initiate recovery from security operations center
Application Owners • Rest easy knowing business data is protected • Applications can be restored quickly to maintain business continuity	**CIOs and CFOs** • Ransomware recovery supported by Zero Trust • Minimize cyber insurance costs • Prevent reputational damage

At the core of Rubrik Zero Trust is a purpose-built filesystem that never exposes backup data via open network protocols. Because Rubrik backup storage is not online nor is it accessible over the network, there's a logical air gap that blocks data from being discoverable or accessible. This approach offers similar protection without the impact to recovery time of a physical air gap.

The remainder of this ebook describes the various technologies that underlie Rubrik Zero Trust Data Security.

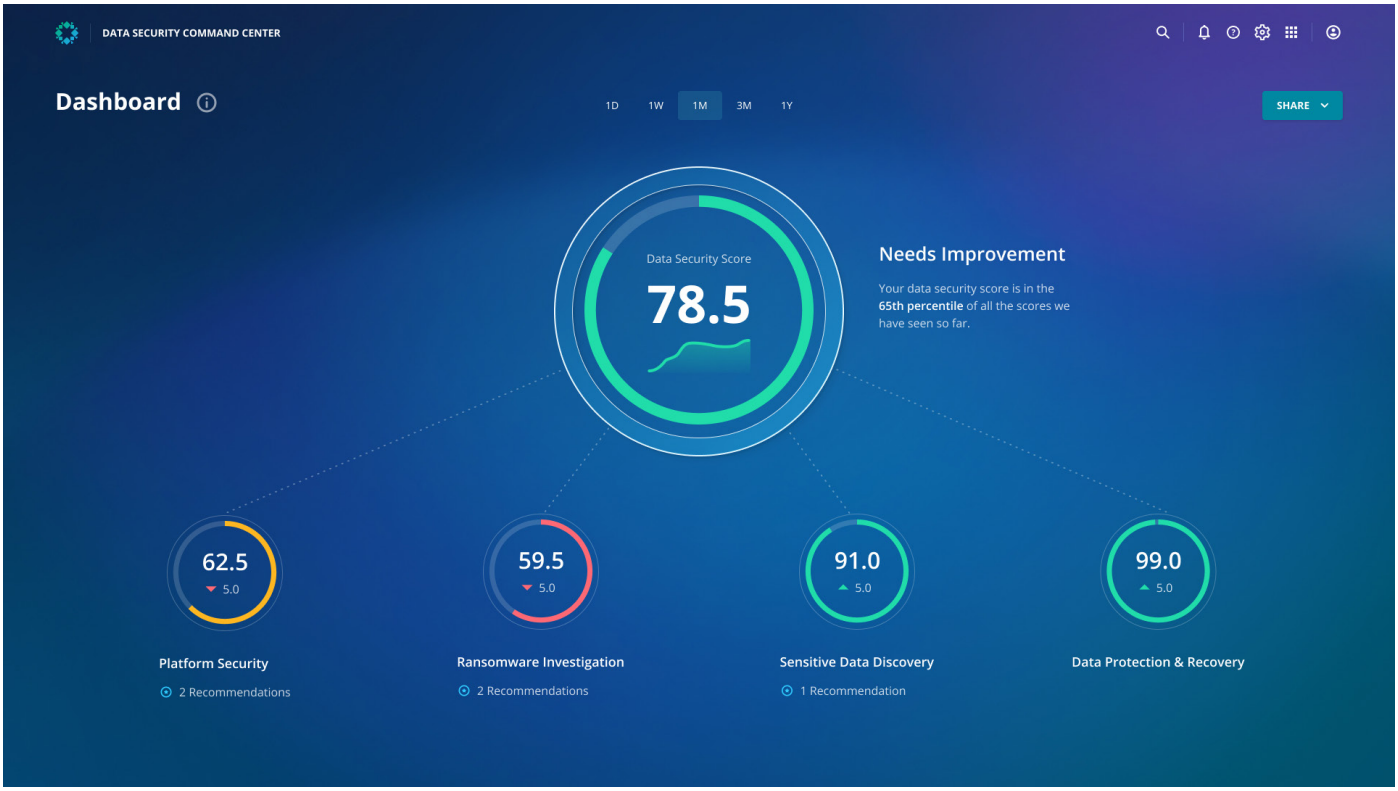
These technologies fall into three categories:

- **Data Resilience.** Prevent and protect against ransomware infection
- **Data Observability.** Detect and identify ransomware attacks quickly
- **Data Recovery.** Contain ransomware after infection and recover efficiently

All capabilities are accessible from the Rubrik Data Security Command Center—and via Rubrik APIs for easy integration.

DATA SECURITY COMMAND CENTER

The Rubrik Data Security Command Center allows your team to access all of the capabilities of Rubrik Zero Trust Data Security, helping your organization determine whether your data is safe and protected. A data security score is calculated across four major risk categories, providing a breakdown of scores by category, with details that enable you to assess data risk properly.



A convenient and easy-to-use SaaS service, DSCC provides visibility into your organization's data risks and security gaps, with recommendations to improve overall security posture. It radically simplifies data risk management by providing a single control plane for global visibility and collaboration. As a result, you can reduce the complexity of data risk management, avoid unnecessary costs and make smarter, data-driven business decisions around data security.

DATA RESILIENCE

When it comes to ransomware protection, backups can be a significant point of vulnerability for financial services firms.

- **Manual backup management** for hundreds of applications creates too many opportunities for error
- **Backup access** may not be restrictive enough, and credentials to gain access may be easily compromised
- **Under- or un-protected applications** increase risk from a successful attack
- **Inadequate security tools** leave backup data vulnerable to compromise

Rubrik automates and simplifies data management to address these challenges.

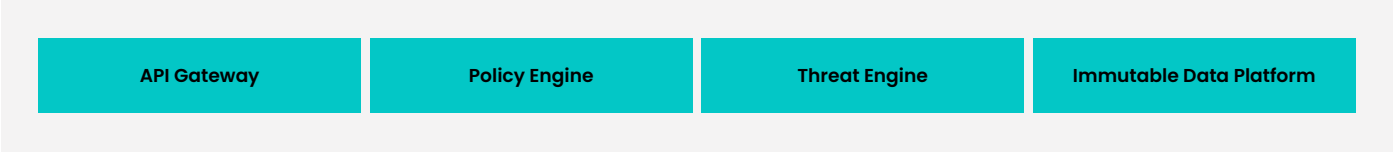
- A scalable platform manages data throughout its entire lifecycle, delivering better economics and simpler operations
- Rubrik eliminates the overhead of managing legacy backup jobs, replacing them with just a handful of easy-to-define and manage policies
- The Rubrik platform integrates easily into your environment

Rubrik ensures the resilience and security of your critical data with:

- **Rubrik Zero Trust Data Protection.** Safeguard your data against internal and external threats
- **Rubrik Cloud Vault.** Ensure a clean copy of your data is stored off site and easily accessible and available for recovery

RUBRIK ZERO TRUST DATA PROTECTION

Rubrik Zero Trust Data Protection ensures the security of critical financial apps and data by preventing attackers from discovering your backups, ensuring backup data can't be encrypted, and controlling access to all backups.



Rubrik Zero Trust Data Protection builds on the principles of Zero Trust, unifying protection across on-prem, multi-cloud, and SaaS environments, while protecting your data via *intrusion risk control and a secure data layer.*

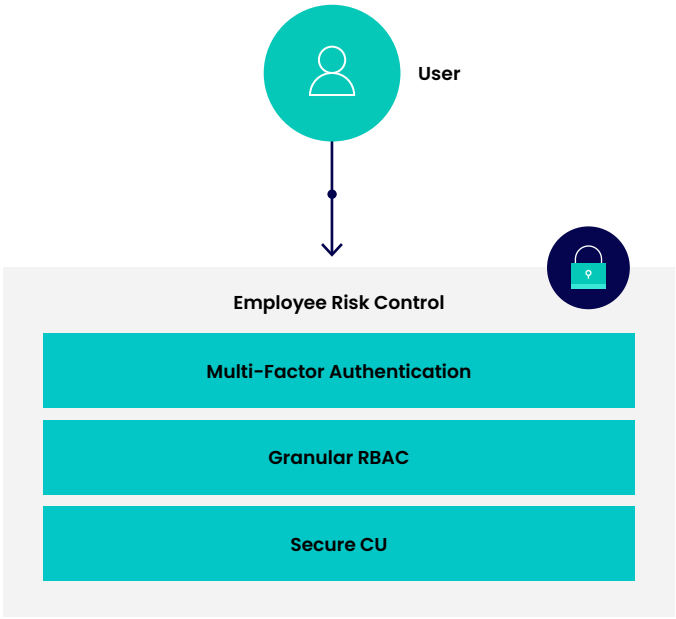
INTRUSION RISK CONTROL

Intrusion risk control is a critical component of Rubrik Zero Trust Data Protection.

Rubrik incorporates:

- Multi-factor Authentication
- Granular Role-based Access Controls
- Disablement of Factory Reset
- Secure Command-Line Interface (CLI)

These security techniques reduce the inevitable risks inherent in having multiple user, employee, and service accounts.



MULTI-FACTOR AUTHENTICATION

Zero Trust requires every user's identity to be verified to a level beyond a simple username and password. Should a user fall prey to a phishing attack, for example, their compromised credentials could allow an attacker to access privileged systems—including your backup systems.

Rubrik includes native Multi-Factor Authentication that doesn't require the use of a third-party provider such as Okta. Using a Time-based One-Time Password (TOTP) method to implement MFA, our algorithm automatically generates an authentication code which changes after a certain period of time.

GRANULAR ROLE-BASED ACCESS

Rubrik makes it easy to assign granular RBAC permissions and integrate with Active Directory. MFA first verifies identity, then the policy engine grants least-privilege access based on a user's or service's role. If an attacker somehow manages to steal credentials with approved access to your data, RBAC can drastically reduce the potential impact.

FACTORY RESET IS DISABLED

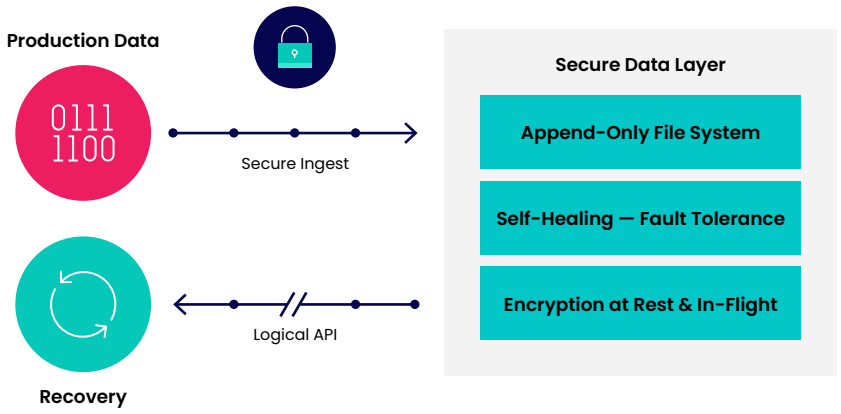
Factory reset commands are proactively disabled, providing important additional security. Even if a hacker is somehow able to access a Rubrik system using stolen credentials, they are unable to reset the system to compromise data access or recovery.

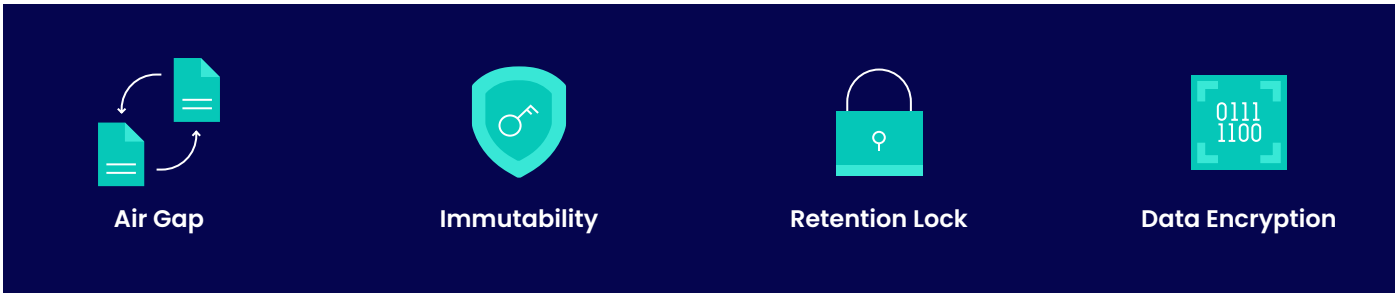
SECURE COMMAND-LINE INTERFACE

Rubrik is built to secure and protect all system interfaces. This includes protection for the Command Line Interface (CLI) via one-time passcode functionality.

THE RUBRIK SECURE DATA LAYER

The Rubrik Secure Data Layer applies security best practices to ingest, manage, and store data immutably, providing a last line of defense against ransomware.





ENCRYPTION

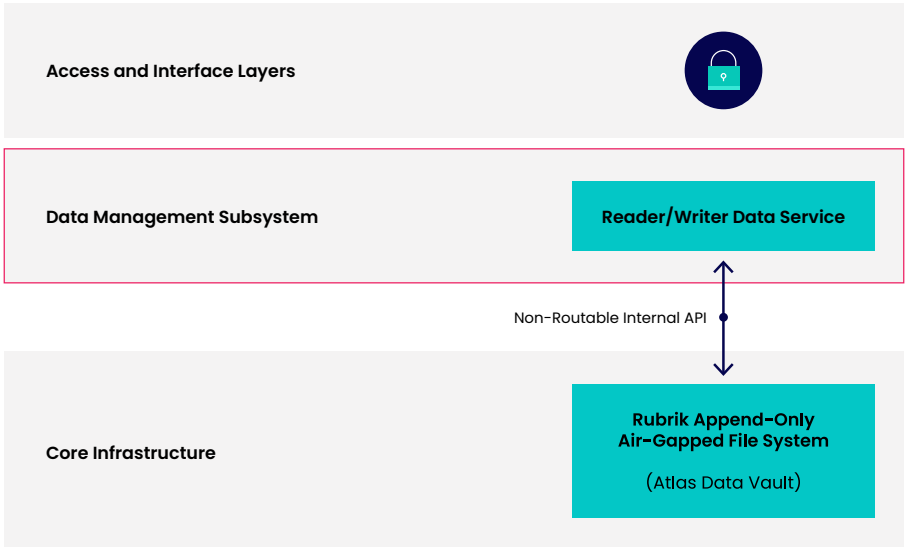
Rubrik offers data encryption at rest and in-flight so that data is never exposed to untrusted users. If your organization is compromised, data encryption is the best way to ensure that data cannot be read and misused by malicious actors.

IMMUTABILITY

With Rubrik, immutability goes beyond simple file permissions, folder ACLs, or storage protocols. Our architecture combines an immutable filesystem with Zero Trust cluster design.

Immutable filesystem. The Rubrik filesystem is immutable and prevents unauthorized access to or deletion of backups, ensuring your team can quickly restore to the most recent clean backup with minimal business disruption.

Rubrik immutability is baked into the filesystem so it is on by default for all data managed by Rubrik and can't be disabled. Other solutions rely on the administrator to enable or disable immutability or WORM for the desired data sets.



BFI FINANCE

"We immediately saw the inherent benefits of Rubrik having an immutable file system where every file looks like 'read-only' so hackers cannot encrypt them in ransomware attacks, and that every transaction is encrypted with military grade encryption."

Alexander Ekanayake
BFI Finance

Zero Trust cluster design. Operations within a Rubrik cluster can only be performed through authenticated APIs. Other cluster designs rely on a full-trust model in which all members of a cluster are able to communicate freely with one another. Once a single node has been penetrated in a full-trust cluster, backup data can be compromised to make restores impossible.

ERASURE CODING

An important aspect of the Rubrik filesystem is the way it uses erasure coding—a method of storing redundant data to ensure full recoverability from storage failures—to write data to disk.

When disks or cluster nodes fail, erasure coding ensures continued data availability with self-healing. Rubrik can typically self-heal in less than an hour, reducing the probability of simultaneous node failures in large, distributed systems.

SLA DOMAINS

Some people believe that tape is more immune to ransomware than other forms of backup, but how long does it take to recover from offsite tape? Extended recovery after a ransomware attack creates a significant financial and business impact. Rubrik's robust SLA Domains ensure that data is where it needs to be, when it needs to be there, enabling Rubrik to deliver rapid recovery.

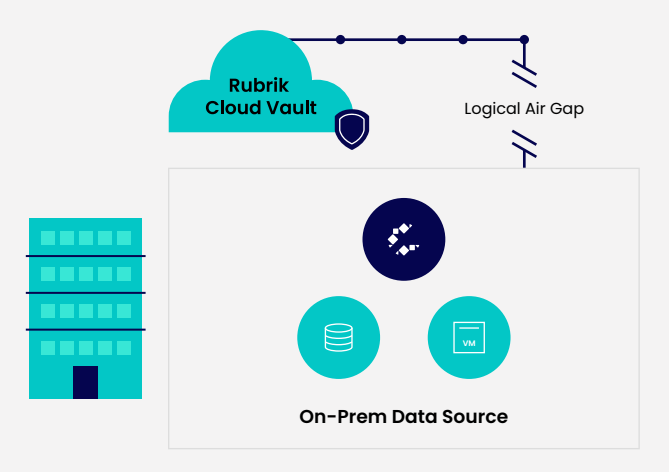
NWB BANK

"We needed a product that would simplify our data management tasks while offering us the data protection that our business requires. In the end Rubrik proved to be the most simple solution for us when it came to setting up SLA policies."

Michel Vaessen
NWB Bank

RUBRIK CLOUD VAULT

Rubrik Cloud Vault extends the capabilities of Rubrik Zero Trust Data Protection and Rubrik's Secure Data Layer to isolated, off-site cloud archival. The fully managed service removes operational complexity while providing a logically air-gapped archive solution with predictable costs. Built on Azure storage, you simply create one or more SLAs that utilize Rubrik Cloud Vault. All data protected with those SLAs are automatically stored on-premises and in the cloud. All storage and egress charges are included in the service.



DATA OBSERVABILITY

Once you've created a backup environment that's secure and resilient, the next step is to ensure that you can detect any attempted attacks quickly.

This can be a challenge with traditional approaches:

- **Failure to identify sensitive data** ahead of time increases risk and cost
- **Locating where and when threats entered** your environment can be time consuming
- **Reinfection of production systems can occur** during recovery
- **Data risks** spread unchecked

Rubrik Zero Trust Data Security addresses these challenges with comprehensive capabilities that reduce risk and save time for busy financial services IT teams:

- **Sensitive Data Monitoring.** Classify data and assess exfiltration risk
- **Ransomware Monitoring & Investigation.** Use machine learning to detect anomalies
- **Threat Monitoring & Hunting.** Find malware and avoid reinfection

SENSITIVE DATA MONITORING

Rubrik Sensitive Data Monitoring scans backups and locates sensitive data in files and applications to help you stay compliant. Rubrik provides visibility into the content of your data, where it lives, and who has permission to access it. If data is breached, the ability to know what data may have been exfiltrated can guide IT teams in any negotiations with cyber criminals.

Rubrik's discovery, classification, and reporting have zero impact on your production environment. Rubrik processes backup data and metadata with zero additional infrastructure and without installing any agents. Rubrik enables you to identify at-risk data and better withstand a data breach or ransomware attack to avoid reputational, financial, or legal consequences.

COMPEER FINANCIAL

"Rubrik makes it easy for us to prove to regulators that we're backing up our data and that it's secure. The reporting and compliance tools keep improving with every release."

Scott Ament
IT Operations Lead, Compeer Financial

ASSET DISCOVERY AND PROTECTION

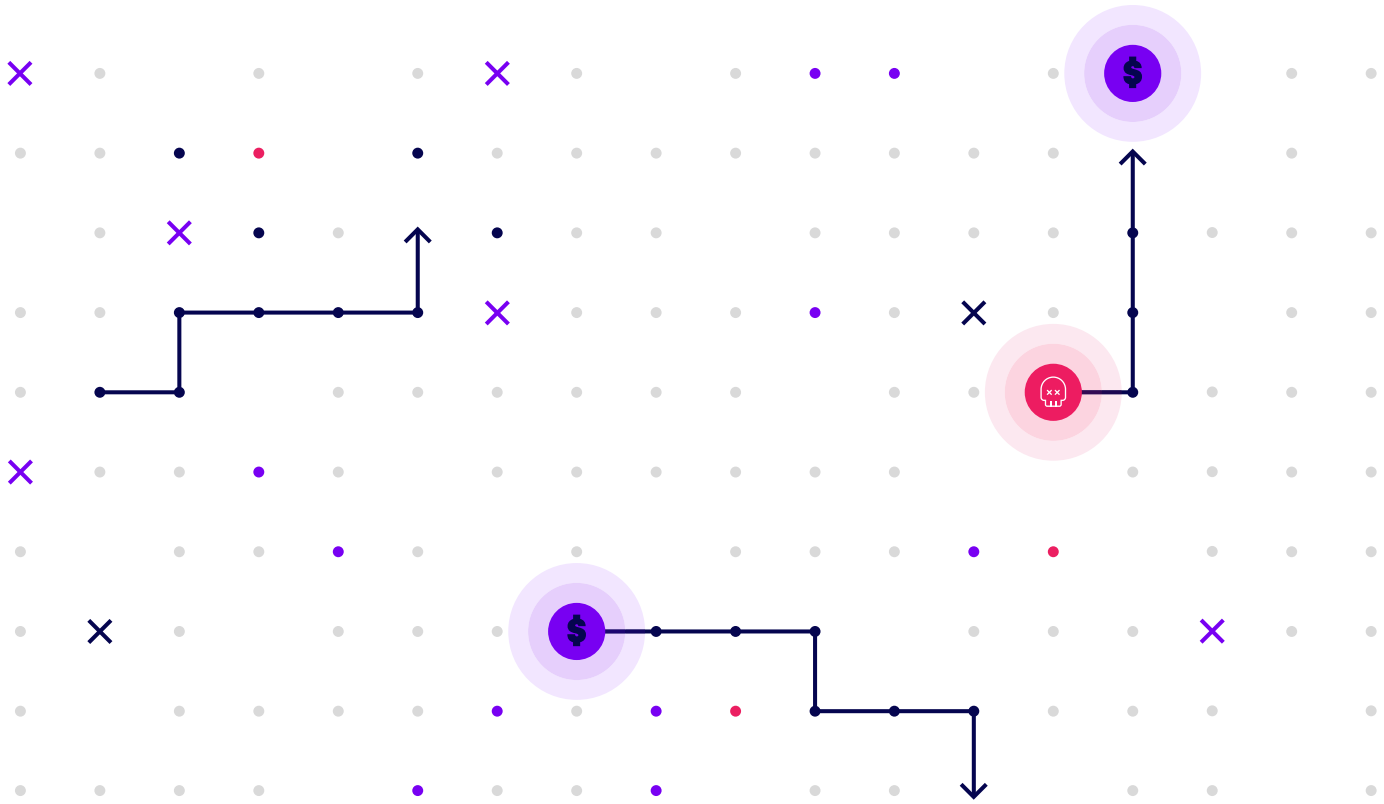
Rubrik helps you minimize vulnerability by discovering all data across your environments—from the datacenter to public cloud—and can automatically apply SLA policies to protect newly created assets. Rubrik discovers virtual machines, databases, or cloud workloads without an assigned SLA so that the right level of protection can be applied.

RETENTION LOCK

Rubrik helps prevent malicious actions by rogue users by ensuring that no single person can clear or shorten retention policies or delete archival or replication locations If a modification to a retention-locked SLA is requested, two appointed individuals from your organization are required to authenticate and acknowledge the modifications with the Rubrik Support Team. This is especially important in heavily regulated financial industries requiring WORM compliance as mandated by regulations such as SEC Rule 17a-4(f) or FINRA Rule 4511(c).

COMPLIANCE REPORTING

Rubrik helps mitigate sensitive data exposure by proactively scanning backups to identify sensitive data and facilitate compliance with applicable privacy laws, such as GDPR and PCI-DSS. Rubrik helps gain valuable insight into what data lives where and can quickly produce reports on regulated data or policy violations.



Gruppo MutuiOnline

"Rubrik has also allowed us to increase operational efficiency by streamlining our data management processes, allowing us to utilize our team's resources on projects that can offer additional value to the company."

Fabrizio Tuveri
Senior System Administrator,
Gruppo MutuiOnline

READ FULL CASE STUDY

MEETING DEMANDING SLAS WITH RUBRIK

Gruppo MutuiOnline S.p.A. (GruppoMOL) is a holding company for a group of Italian firms that distribute credit and insurance products to private customers. It also outsources services to handle complex processes for financial institutions.

"We needed a solution that was both consistent with recent technological advances and compatible with existing solutions," said Fabrizio Tuveri, Senior System Administrator. "Our external customers, which include financial and insurance companies, are asking us to adhere to strict SLAs. Thanks to Rubrik's automated SLA policy engine, we are confident that our customer data is always safe."

"Rubrik has also allowed us to increase operational efficiency by streamlining our data management processes," Tuveri continued, "allowing us to utilize our team's resources on projects that can offer additional value to the company."

RUBRIK BENEFITS

4x

4x faster backup performance

Minutes

Restore time reduced from hours to minutes

3

Unified data protection across three remote sites

0

Near-zero RTOs

Reduced

Reduced data center footprint

RANSOMWARE MONITORING & INVESTIGATION

Rubrik's ransomware monitoring and investigation capabilities help you discover and contain attacks quickly by monitoring for encryption, analyzing unusual access patterns, and alerting you of signs of potentially malicious activity in your backup data.

Rubrik:

- **Uses machine-learning-based anomaly detection** to discover potential threats automatically.
- **Scopes the blast radius of an attack** and makes recommendations about the best recovery points.
- **Provides API integration** with popular security operations tools, enabling strong collaboration between IT and security groups for faster incident response.

Rubrik enables you to quickly identify and locate which applications and files were impacted by ransomware, so you only restore the files and applications that have been affected.

ANOMALY DETECTION USING MACHINE LEARNING

Backup data is rich with information, including the content itself along with metadata such as path, size, ACL details, UIDs, GIDs, and other attributes. Rubrik feeds this information into a machine learning pipeline that provides intelligent insights that streamline the decision-making process during ransomware recovery.

A deep neural network (DNN) is used to build out a full perspective of each workload. The DNN is trained using supervised learning and can identify trends across all samples and classify new data based on similarities to existing data without human input.

The DNN analysis consists of an anomaly detection model and an encryption detection model:

- **Filesystem Behavior Analysis.** Performs behavioral analysis on filesystem metadata by looking at things like number of files added, number of files deleted, and so on.
- **File Content Analysis.** If there is an anomaly in filesystem behavior, a second analysis is performed to determine if there is a characteristic sharp increase in file entropy that signals a ransomware attack. This model also looks for signs of encryption and computes an encryption probability.

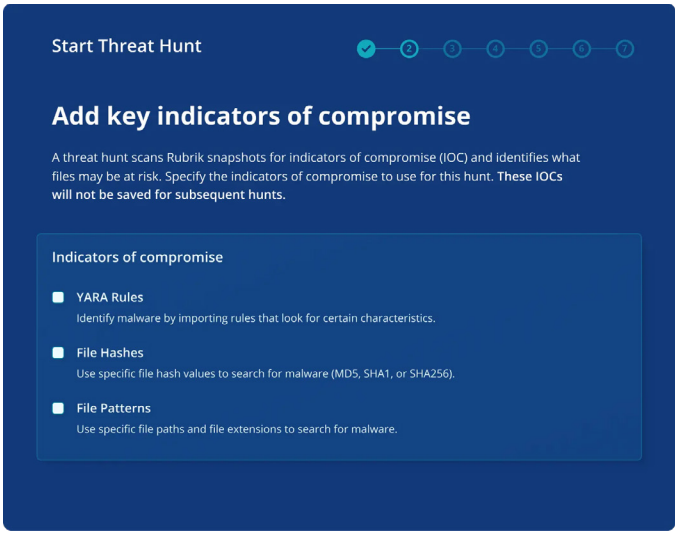
Every time you perform a backup, Rubrik looks for signs of ransomware and other anomalies, enabling you to detect attacks and initiate recovery more quickly.

THREAT MONITORING & HUNTING

Rubrik Threat Monitoring & Hunting is designed to help you spot malware and avoid reinfection. It searches your backups, looking back in time at your VMs and file sets to help pinpoint when an infection started and to avoid reinfection during recovery.

Rubrik Threat Monitoring & Hunting enables you to discover threats, find malware based on YARA rules, file hashes, and file patterns, establish safe recovery points, and document evidence for internal and external cyber investigations.

Ransomware protection tools can't interfere with the performance of financial applications that customers rely on. Rubrik differs from competing solutions because it has no impact on your production environment. An intuitive UI eliminates the learning curve that comes with other solutions, making it possible to execute complex searches and achieve greater insight in less time.



DATA RECOVERY

Recovery is where a ransomware solution really proves itself. Unfortunately, traditional backup solutions come up short when it comes to ransomware recovery:

- **Different recovery approaches** may be needed for data center vs. cloud vs. SaaS recovery.
- **Threats aren't quarantined** from the active backup set.
- **It is difficult to recover data** at file, user, object, or system level.
- **Success is uncertain** and restore times are long.

Rubrik Zero Trust Data Security quarantines malware and automates recovery to restore business operations in less time and with far less uncertainty using:

- **Threat Containment.** Quarantine data to prevent reinfection
- **Mass Recovery.** Identify affected data and initiate recovery in minutes
- **Orchestrated Application Recovery.** Recover apps and data quickly and easily with guided workflows

NWB BANK

"With Rubrik's Google-like search, we can instantly search for and recover files across all snapshots. This feature is instrumental in reducing our data management time and was not available in our legacy solution."

Rob Heemskerk
Network Engineer, NWB Bank

THREAT CONTAINMENT

Containing ransomware attacks is important for two reasons. First, attackers may continue to extend their reach and encrypt new systems even after encrypting an initial set of systems and declaring their presence. Second, containment can prevent attackers from coming back and launching a new attack.

ANALYZE THREAT IMPACT

Rubrik continuously scans your entire environment to provide insights on how your data is changing over time. In the event of an attack, you can quickly identify which applications and files were impacted and where they are located through simple, intuitive visualizations. Rubrik helps you minimize time spent discovering what happened and provides granular visibility into the files affected.

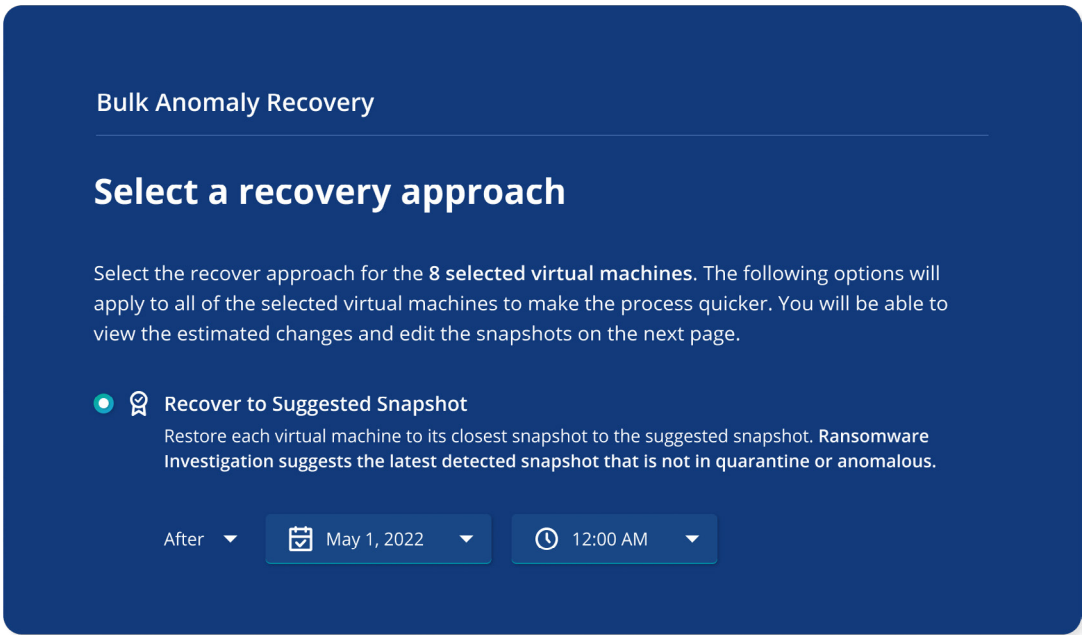
Rubrik can pause all access and activities in the event of compromise or threat. This gives you the ability to contain affected data, so it does not reinfect the environment. Rubrik enables you to scan for Indicators of Compromise (IOCs) on multiple systems and across time to provide insights from system and data backups, helping you identify clean backups for recovery.

MASS RECOVERY

When a disaster or ransomware attack strikes, a simple, scalable path to full recovery is essential to avoid costly interruptions. Rubrik Mass Recovery enables you to ensure business continuity with secure recovery of your data and applications to meet your stringent recovery time objectives.

With Rubrik Mass Recovery you can:

- **Minimize downtime.** Recover hundreds of VMs or restore tens of thousands of files to a clean state in minutes.
- **Avoid reinfection.** By identifying files and applications infected by ransomware, Rubrik enables you to quickly identify a clean snapshot and recover your data with no reinfection.
- **Recover only what you need.** Recover only the data that has been compromised with guided workflows for file-level, object-level, application-level, and system-wide restore.



Many ransomware recoveries proceed slowly because they depend on the expertise of one or a few "experts" within your organization to decide on a plan and carry out restores. Rubrik's mass recovery wizard uses machine learning technology to quickly identify the latest clean snapshot(s), and enables your team to execute smooth mass recovery operations without relying solely on internal experts or requiring a lot of specialized knowledge and skills.

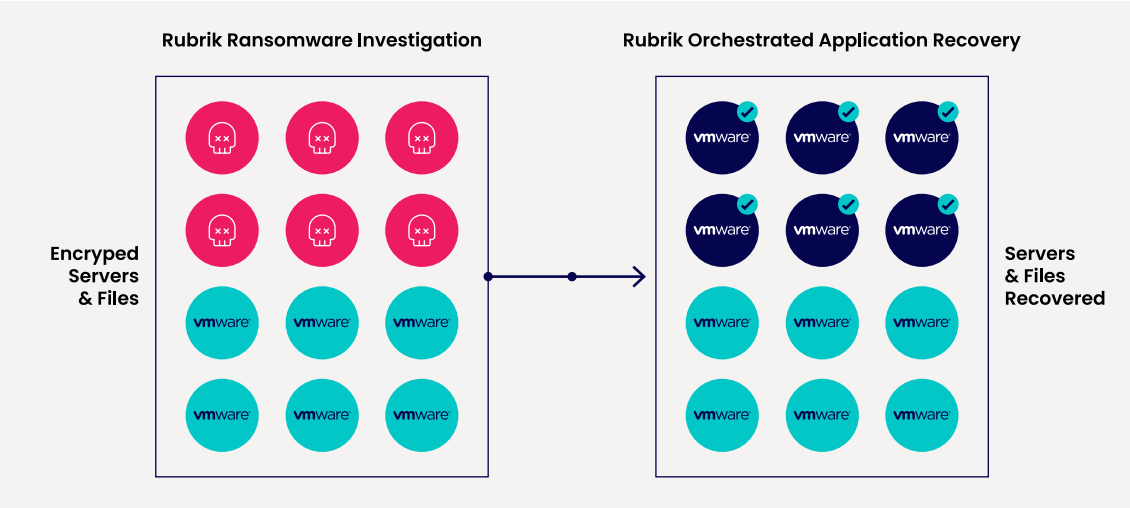
ORCHESTRATED APPLICATION RECOVERY

Executing manual recovery plans for applications with multiple tiers and interdependencies slows down the recovery process and introduces opportunities for error. Rubrik Orchestrated Application Recovery is a tightly integrated and automated DR service that provides orchestration of DR failover/failback and testing. It leverages application-focused Ransomware Monitoring & Investigation that radically simplifies recovery.

Rubrik utilizes application Blueprints that contain information on an application's VM recovery sequence and resource mapping configurations (compute, storage, and network) to provide application-level orchestration.

For example, suppose you have a three-tier application with a web server front end, a middleware server, and a backend database. A Blueprint recovery allows you to individually roll back the necessary servers to a clean state. Depending on the date of infection, you could roll back your middleware server to 2 days ago, and roll back your front and back ends to 3 days ago. Blueprints can encompass hundreds of VMs for recovery at scale, with groups of Blueprints making up a Recovery Plan to enable failover for an entire datacenter.

When combined with Rubrik Ransomware Monitoring & Investigation and Threat Containment, you can accelerate recovery from ransomware by analyzing and then selecting all impacted applications and files and restoring to the most recent clean version with a few clicks. Orchestrated Application Recovery automates the restore process.



For more on Orchestrated Application Recovery, see the white paper, An Introduction to Rubrik Orchestrated Application Recovery.

NWB BANK

"As a financial institution, we are required to protect our clients' data by enforcing strict SLAs. We need to provide external auditors with proof that we are complying with European Central Bank (ECB) and De Nederlandsche Bank (DNB) regulations. [With Rubrik] we have a one-click procedure to produce SLA reports, which show we are indeed compliant with regulatory requirements."

Michel Vaessen
ICT Manager, NWB Bank

IT'S TIME FOR ZERO TRUST

The message from security experts and the highest levels of government is clear—the bad guys are getting through traditional security defenses, and they are targeting financial services companies as a growth strategy. If you haven't done so already, it is time to rethink your data protection strategy, implement new backup and recovery processes based on Zero Trust principles, and make the necessary IT investments to secure your data and help ensure your organization never has to pay a ransom.

Rubrik Zero Trust Data Security provides the essential capabilities to protect your backup environment against ransomware attacks while ensuring that you can accelerate recovery. Rubrik helps you reduce the risk of intrusion and secure your backup data in an immutable form while also making it much simpler to detect anomalous behavior and enforce compliance with the latest laws, regulations, and policies.

Rubrik also offers a unique Ransomware Recovery Warranty to provide further peace of mind. To find out how Rubrik can help you enhance the security of your data protection environment, with maximum protection from hackers and fast recovery from ransomware attacks, visit rubrik.com/ ransomware.

ADDITIONAL RANSOMWARE RESOURCES

And be sure to check out our complete set of ransomware-related resources (registration required):

Framework for a Comprehensive Ransomware Recovery Plan

DOWNLOAD NOW

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

DOWNLOAD NOW

VERSION HISTORY

Version	Date	Summary of Changes
1.0	July 2022	Initial Release

rubrik

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

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

Rubrik is a cybersecurity company. We are the pioneer in Zero Trust Data Security™. Companies around the world rely on Rubrik for business resilience against cyber attacks, malicious insiders, and operational disruptions. Rubrik Security Cloud, powered by machine intelligence, enables our customers to secure data across their enterprise, cloud, and SaaS applications. We automatically protect data from cyber attacks, continuously monitor data risks and quickly recover data and applications.

20220722_v1