InBalance IT Transformation. Simplified.

SOLUTION BRIEF

Ransomware and Rapid Recovery Solution Blueprint

Data is an enterprise's most valuable asset. Modern enterprise's need to address data protection, growth, compliance requirements, and defense against cyber threats.

This document is a blueprint to address these challenges.

Ransomware attacks are growing at an alarming rate. You cannot turn on the news without hearing about yet another organization that has been affected. These attacks pose a severe threat to today's businesses.

A recent Gartner report, Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware, noted that "By 2025, at least 75% of IT organizations will face one or more attacks."

In 2023, we saw a staggering number of "double extortion" attacks, which both prevent access to the data by encryption and threaten to post the data online for ransom after exfiltration. Based on the Zscaler ThreatLabz 2023 Ransomware Report, these findings shown in Figure 1 below highlight the pervasive and evolving nature of ransomware attacks targeting a wide range of industries, including sectors with normally low attack rates experiencing sudden surges in ransomware incidents.

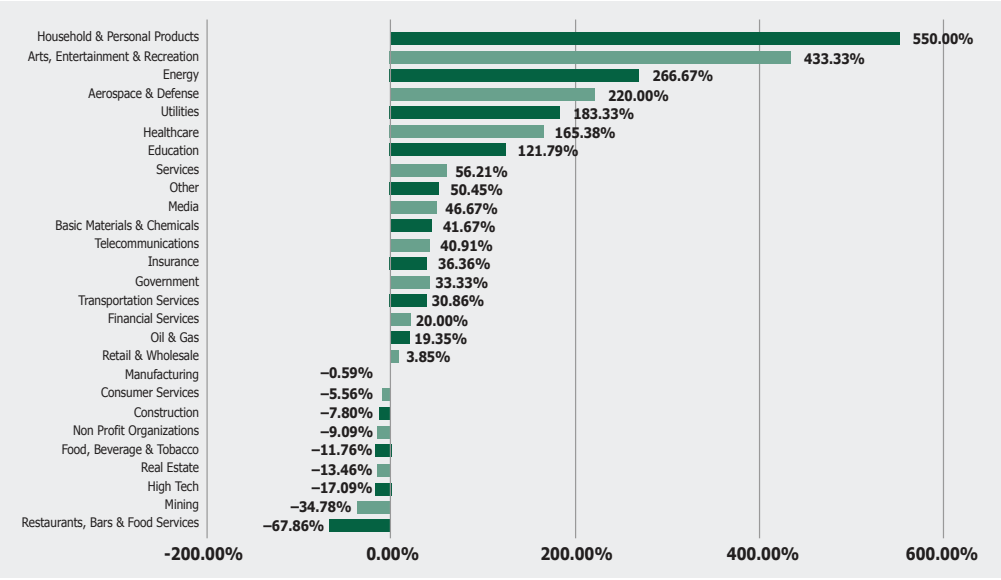
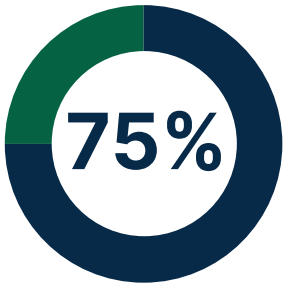


Figure 1: Year over year comparison of extortion attacks by industry, based on percentage of change.



By 2025, at least 75% of IT organizations will face one or more attacks

Gartner report, Detect, Protect, Recover: How Modern Backup Applications Can Protect You From Ransomware

In the battle against ransomware, traditional approaches to security and data protection are failing.

Two simple facts:

- Perimeter security is not enough to keep ransomware out.
- Traditional backups are vulnerable.

In the face of these grim realities, IT teams are turning to Zero Trust methods to protect against ransomware and other cyber threats. Zero Trust assumes that all users, devices, and applications are untrustworthy. While Zero Trust methods are a valid enhancement to data security, we take the concept of Zero Trust, and extend it to support Zero Access following the guiding principles and framework of the Sheltered Harbor organization. Sheltered Harbor is the most robust data protection framework ever devised for data protection.

The goals are clear…

- Safeguard your data from corruption, compromise, or loss.
- To meet business requirements, ensure timely restoration capability.
- Prevent ransomware vulnerability.
- Ensure data availability under all instances.

Though providing outstanding data protection via backup functionality, data backup software solutions do not generally meet all the requirements for data driven organizations.

Functions required to meet the goals:

- Enterprise Data Protection
- Cloud Data Protection
- SaaS Data Protection
- Unstructured Data Protection
- Anomaly Detection
- Threat Monitoring and Alerting
- Threat Hunting
- Sensitive Data Monitoring
- Threat Containment
- Zero Trust Networking
- Encrypted Packet Inspection
- Data Loss Prevention
- Firewall Functionality with Port Control
- Rapid Recovery Functionality
- Data Recovery Procedure, Runbooks
- Policy and Procedure
- Long term retention – Archive / Tape

The requirements stated above will be addressed with a combination of several commercially available technologies as well as the design of a process workflow, policies, and procedures. We will explain why it is important to check for anomalies, add the ability to inspect encrypted data in-flight, and have a set of policies and procedures to maximize your ability to detect and stop cyber attacks.

Enterprise-Cloud-SaaS-Unstructured Data Protection

The first step in providing for these needs is to select a robust and contemporary backup software solution. Rubrik is both a leader and visionary in the Gartner Magic Quadrant for Backup and Recovery Software Solutions.

There are several reasons why a company might choose to buy Rubrik for data backup:

1. **Simplified backup and recovery:** Rubrik offers a simplified approach to data backup and recovery. Its intuitiv user interface and automation capabilities make it easier for businesses to back up and recover their data quickly and efficiently.

2. **Scalability:** Rubrik provides scalable backup solutions that can handle large volumes of data. As a company grows and generates more data, Rubrik can easily scale up to accommodate the increased backup needs.

3. **Cost savings:** Rubrik's all-in-one solution can help companies save costs by eliminating the need for multiple backup software, hardware, and storage devices. It provides a single platform for data management and ensures better data efficiency, resulting in cost savings.

4. **Cloud integration:** Rubrik seamlessly integrates with public and private cloud platforms, allowing companies to easily back up and recover their data in the cloud. This flexibility enables businesses to adopt a hybrid or multi-cloud strategy and leverage the benefits of cloud storage.

5. **Faster recovery times:** Rubrik's instant recovery capabilities enable businesses to recover their data in minutes rather than hours or days. This reduces downtime and improves business continuity, leading to increased productivity and customer satisfaction.

6. **Compliance and governance:** Rubrik helps companies meet regulatory compliance requirements by offering features like data encryption, access controls, and audit trails. It ensures data governance and helps businesses maintain data integrity.

7. **Enhanced data protection and security:** Rubrik provides robust data protection and security measures like encryption, access controls, role-based permissions, and secure transmission protocols. This ensures that the backed-up data is kept safe and secure.

Overall, Rubrik offers an efficient, scalable, and secure data backup solution that simplifies the backup process, reduces costs, and ensures business continuity. These benefits make it an attractive choice for companies looking to enhance their data backup and recovery capabilities.

Anomaly Detection, Threat Monitoring and Alerting, Threat Hunting

The most effective strategy for preventing and recovering from cyber-attacks is defense in depth. A defense in depth approach keeps your backups safe from threats, identifies when you are under attack, and accelerates recovery to minimize business impact in the event of an attack.

Anomaly Detection determines the scope of cyber-attacks using machine learning to detect deletions, modifications, and encryptions. Anomaly Detection helps you identify and investigate abnormal behavior faster by providing a simple, intuitive user interface that tracks how your data changed over time. It replaces manual recoveries with just a few clicks for minimal business disruption. It also increases intelligence by using machine learning to actively monitor and generate alerts for suspicious activity.

Anomaly Detection continuously scans the backup environment to provide insights on how your data has changed over time. in the event of an attack, you can quickly identify which applications, VMs, and files were impacted and where they are located through simple, intuitive visualizations. Using the UI, browse through the entire folder hierarchy and drill-down to investigate what was added, deleted, or modified at the file level. With Anomaly Detection, you minimize the time spent discovering what happened and the data loss with granular visibility into the latest unaffected files.

Identifying malware lurking in your infrastructure can be challenging. Rubrik Threat Monitoring accelerates investigations and reduces the risk of malware reinfection during recovery by automatically analyzing backup snapshots for threats using an up-to-date threat intelligence feed.

Protection against ransomware attacks: Rubrik is designed to protect against ransomware attacks. It offers advanced features like immutability, data validation, and anomaly detection to prevent unauthorized access and ensure data integrity.

Sensitive Data Monitoring

Sensitive Data Monitoring has two main concepts that are important to understand - Policies and Analyzers. Analyzers are where a user defines the type of sensitive data (ex. credit card numbers) that Sensitive Data Discovery should be discovering while Policies are a logical grouping of one or more analyzers that also associates those analyzers with specific objects (ex. VMware VMs) Sensitive Data Monitoring scans. In addition to VMware vSphere, Microsoft Hyper-V, Azure Stack HCI and Nutanix AHV VM policies can be associated with NAS file sets, Windows file sets, Linux file sets, Volume Groups, Microsoft 365 OneDrive and SharePoint, Rubrik Cloud Vault hosted NAS Cloud Direct, and Rubrik Cloud Vault hosted Azure VMs.

Finding sensitive data in applications and files is key to helping you stay compliant and avoid unnecessary incident response costs. Here are some important sensitive data discovery capabilities this data security platform should have:

1. **Evaluate data exposure:** Find sensitive data that may be exposed during data exfiltration or other unauthorized access.

2. **Automate policy enforcement:** Select the types of personally identifiable information (PII) and other sensitive data you want to monitor for automated policy enforcement.

3. **Facilitate compliance:** Capable of documenting and reporting on where sensitive data is located and who has access to it, to maintain regulatory requirements and get alerts when data might violate policies.

Threat Containment

Threat containment ensures safe recovery by preventing reintroduction of malware that disrupts business operations. Safer recoveries lead to less downtime when hit by malware. Rubrik Threat Containment isolates the infected snapshots, by providing quarantine capabilities for entire snapshots or individual files, to reduce the risk of reintroducing the malware into the environment during a recovery operation. This feature also allows for quarantined data to be retained for post-incident reviews.

Zero Trust Networking

Zero Trust Data Security™ is the Rubrik proprietary architecture modeled after the Zero Trust architecture from NIST (National Institute of Standards and Technology), discussed in SP800-207 (see figure 2 below).

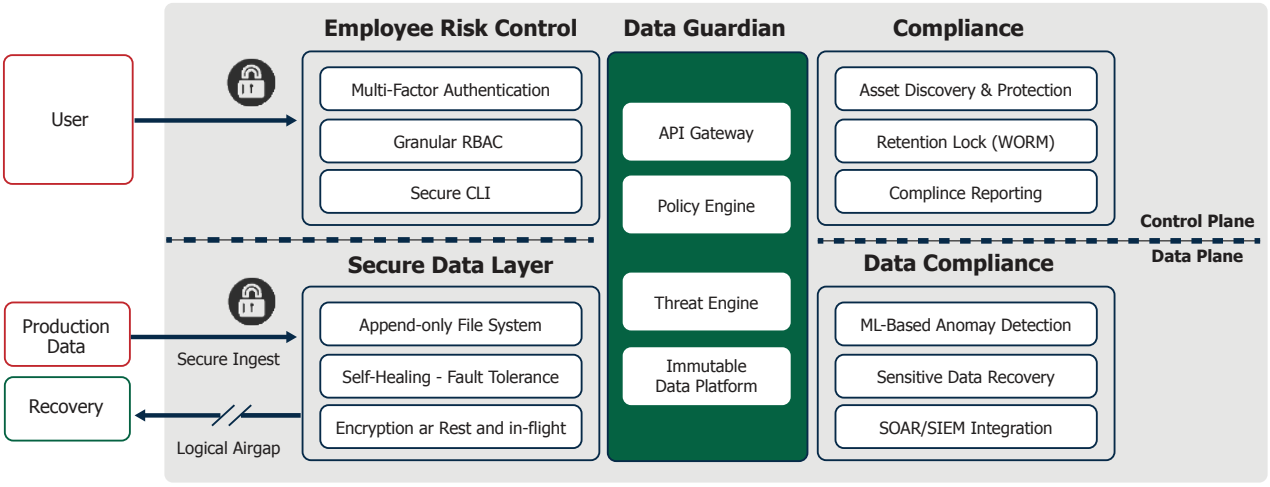


Figure 2: Rubrik Zero Trust Data Security™

The core architecture of the Rubrik platform is based on this Zero Trust model. It supports a purpose-built file system that never exposes backup data via open protocols. This approach creates a logical air gap that blocks data from being discoverable or accessible over the network. We take this concept a step further by providing physical air gaps, discussed later under Policy and Procedure.

Once data is written to the Rubrik platform, it cannot be modified or encrypted by an attack, ensuring that a clean copy is readily available for recovery. Additionally, it is possible to enable SLA Retention Lock, which prevents a bad actor from expiring any backup data prematurely. Multiple expert-guided recovery options, including Live Mount and Mass Recovery, are built-in so IT teams can quickly recover the files and workloads impacted by an attack.

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

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

Encrypted Packet Inspection and Data Loss Prevention

To further ensure protection of data in flight, Security Service Edge (SSE) solutions offer additional protections and benefits. SSE successfully modernizes technology architecture by converging Secure Web Proxy (SWG), Zero Trust Network Access (ZTNA), Cloud Access Security Broker (CASB), and Data Loss Prevention (DLP) into one, powerful, high-performing solution. To defend against double extortion ransomware attacks, Rubrik has partnered with Zscaler to combine data-at-rest intelligence with data-in-motion security to deliver end-to-end security.

Using Zscaler Internet Access (ZIA), it provides a secure internet and web gateway delivered as a service from the cloud.
Think of ZIA as a bridge to a secure internet experience. Whether you are in the office, on the go, or using a virtual desktop, ZIA acts as your internet gateway, inspecting all traffic for threats with multiple security layers, even within encrypted connections. It offers features like firewalls, intrusion prevention, sandboxing, data loss prevention, and browser isolation, letting you choose the level of protection you need now and scale up later.

The Rubrik Zscaler Data Loss Prevention (DLP) integration automatically sends sensitive files found by Rubrik's Sensitive Data Discovery feature and protected by Rubrik to Zscaler's service for DLP.

Zscaler offers a detailed view of potential DLP violations via its Data Discovery Dashboard (see Figure 3 below). It provides high-level visibility and insight into your company's DLP content, enabling you to analyze and monitor DLP data in a single location. On this page, you can look at the following:

1. Choose a time frame from the menu. By default, the data is displayed for the last 7 days, but it can also show 1-day, 30-day, and 90-day time frames.
2. Set filters to the data displayed.
3. View information about your DLP data based on a series of widgets, like Files in Top 10 Categories.

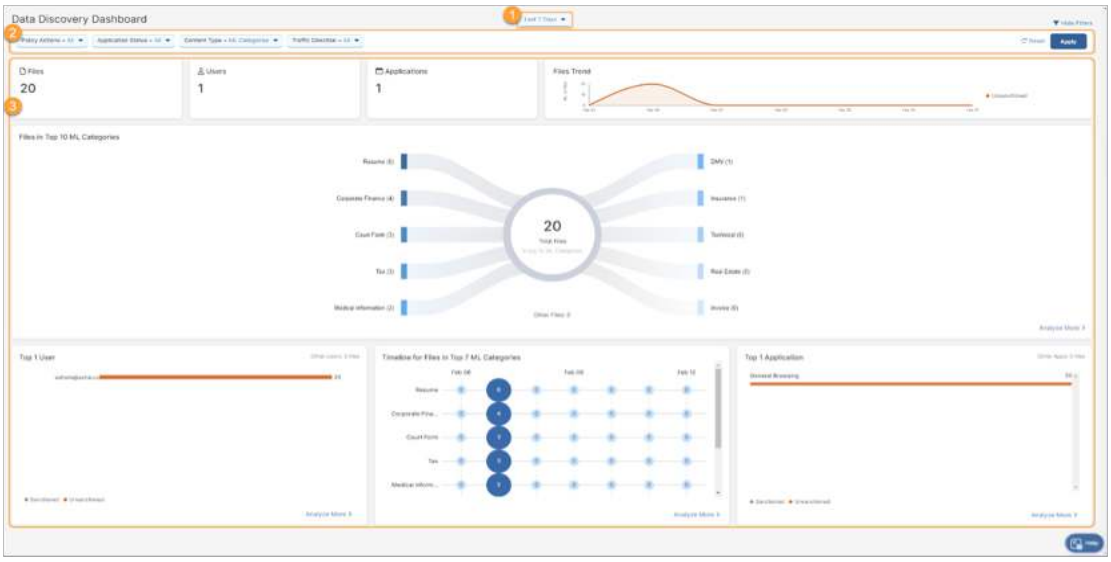


Figure 3: Zscaler Internet Access (ZIA) DLP Data Discovery Dashboard

Gartner has positioned Zscaler as a Leader in the Magic Quadrant™. See 2023 Gartner Magic Quadrant for SSE for the full report.

Zscaler's sophisticated security has the deepest visibility and granular context across applications, users, and data with the Zero Trust Engine as the foundation for their Intelligent SSE services. Upon this foundation are unique capabilities that create the structure and attributes that are key to effective SSE in action, including AI/ML enabled web and cloud app categorization and private app discovery enable strong, granular policy enforcement.

Firewall Functionality with Port Control

Continuing with our theme of utilizing best in breed products, Palo Alto Networks firewalls offer an array of extra measures that enable the implementation of controls at the port level. This allows for the restricted flow of data in a single direction, ensuring that backup data is allowed to enter the secondary site or vault while preventing unauthorized egress of data.

Palo Alto firewalls provide granular control over traffic by examining the application, user, and content. They allow you to create security policies that define how traffic should be handled in both directions (ingress and egress) on specific ports. These policies can be based on various criteria such as source IP, destination IP, application, user, or other attributes, enabling you to effectively control the flow of data.

A unique feature that also secures vaulted data and provides for a physical airgap is the ability of a Palo Alto firewall to disable a port after a specific task or function. Automation tools like the Palo Alto Networks API allow you to programmatically disable ports based on scheduling or specific triggers. By interacting with the API, you can send commands to the firewall to enable or disable ports as desired. This method offers flexibility and the ability to automate port status changes based on various conditions.

Rapid Recovery Functionality

Naturally one of the keys to providing rapid recovery functionality is the utilization of fast data storage.

Backups, restores, and recoveries at the enterprise level require data storage without compromise. VAST Data and Rubrik partner to deliver an all-flash modern data protection solution that enables organizations to affordably recover in near-real time from any data loss event.
Today the focus is on when, not if, a ransomware attack will occur and how organizations can rapidly restore at datacenter-scale following an attack. VAST Data and Rubrik partner to deliver an all-flash modern data protection solution that enables organizations to affordably recover in near-real time from any data loss event.

By combining hyperscale flash, revolutionary data reduction, and highly efficient erasure coding, VAST Data makes flash storage affordable for backup use, eliminating the economic arguments for mechanical media and providing customers with a high-performance backup target. Combining Rubrik Zero Trust Data Protection with the all-flash VAST Data Platform enables organizations to rapidly restore and recover entire IT estates and minimize the threat of extensive downtime in an era of unprecedented cyberthreats.
VAST's new Disaggregated and Shared-Everything Architecture is designed to break the conventional scaling limits of distributed systems. Because the VAST Data Platform is a multi-protocol system and disaggregates the storage control layer from the data storage layer, unique capabilities are possible.

VAST's Protocol Manager exports S3 objects using HTTP GET and PUT semantics to transfer an entire object via a single request across a flat namespace. Each object is identified and accessed by a URI (Universal Resource Identifier). While the URIs identifying files can contain slashes (/s) like file systems, object stores do not treat the slash character as special, so that it can emulate a folder hierarchy without the complexity a hierarchy creates – slashes are just another character in an internal element identifier.

VAST Objects are stored in a comparable manner to files, with the difference being that an S3 object includes not just its contents, but also user-defined metadata that allows applications to embed their metadata about objects within the objects themselves.

This unique feature enables the ability to write the backup data as object storage while presenting the data utilizing the NFS protocol. By providing for "restore in place" functionality, we can immediately present backup data for BC/DR functionality without moving the data from a backup storage tier to a production storage tier.

Data Recovery Best Practices and Procedure

Ransomware attacks can cripple your operations, but with Rubrik's proven best practices, you can be prepared. At In Balance, we have helped organizations navigate the recovery process and get back on track, faster. Our comprehensive approach covers everything from proactive planning to rapid remediation, giving you the peace of mind, you deserve in the face of cyber threats. General ransomware attack planning best practices consist of the following:

1 Preparation

Pre-empt the panic: Build your defenses beforehand with a robust ransomware response plan.
Fortify your fortress: Harden systems, train users, and back up data diligently to withstand a siege.
Become an architect of resilience: Design your infrastructure for rapid recovery and minimal disruption.

2 Detection

Shine a light on the shadows: Implement effective threat hunting and anomaly detection tools to pinpoint ransomware activity.
Do not let the infection fester: Early identification of compromised systems is crucial for swift containment and remediation.
Isolate the outbreak: Quickly quarantine infected systems to prevent further spread of the ransomware.

3 Prevention

Keep the gates locked: Deploy advanced security tools to block ransomware from entering your network.
Stop the invaders at the border: Utilize multi-layered defenses like endpoint protection and intrusion detection to catch attacks early.
Neutralize the threat before it takes root: Proactive monitoring and vulnerability management can disarm ransomware before it infects your systems.

4 Assessment

Prioritize the critical: Identify and prioritize critical systems and data for immediate recovery.
Triage the damage: Assess the extent of the attack and the impact on your operations.
Chart the course to recovery: Develop a clear and actionable plan for restoring affected systems and data.

5 Recovery

Rise from the ashes: Restore critical systems and data with minimal downtime and data loss.
Close the security gaps: Patch vulnerabilities and address the root cause of the attack to prevent future breaches.
Become immune to future threats: Learn from the attack and continuously improve your security posture.

Attackers Target High-Value Accounts: In ransomware attacks, compromised directory services and individual accounts often serve as key entry points. Attackers prioritize seizing control of privileged accounts and directory services to infiltrate your environment.

Rubrik's MFA - Your Built-in Security Shield:

- **Multiple Layers of Protection:** Rubrik's native Time-based One Time Passwords (TOTP) feature erects a robust defense against these vulnerabilities. By requiring a secondary authentication step for all system access (GUI, CLI, and API), it blocks unauthorized entry even if primary accounts are compromised.
- **Seamless Setup, No Third-Party Dependencies:** This native MFA solution eliminates the need for external identity providers, streamlining setup and activation in just a few clicks.
- **Flexibility for Existing Systems:** Already have a third-party MFA provider? Rubrik seamlessly integrates with them through SAML 2.0, ensuring a smooth transition.

As an organization, you must be prepared to address a ransomware attack by having an effective ransomware recovery plan.

1. **Disarm the Attack**
   Search and Destroy: Begin by methodically locating and removing any trigger files from all affected devices. This crucial first step helps halt further damage.

2. **Know Your Enemy**
   Identify the Threat: Accurately determine the specific type of ransomware you are facing. This knowledge will guide your subsequent recovery actions. Common types include screen-locking and encryption-based ransomware.

3. **Contain the Outbreak**
   Isolate the Infection: To prevent the ransomware from spreading further, promptly disconnect all vulnerable devices from your network. This containment strategy buys you time to plan your response.

4. **Explore Recovery Options**
   Seek Expert Guidance: Work with In Balance IT on consulting with malware experts to explore potential data recovery methods. These might include web-based software or specialized ransomware encryption removal tools.

5. **Restore with Caution**
   Prioritize Clean Data: Use your backed-up data to restore as much of the affected information as possible. However, proceed with extreme caution. Ransomware can dwell undetected for months, potentially compromising even archival backups.
   Scrutinize Before Restoring: Always scan all systems with a reputable anti-malware package before initiating any data restoration processes. This thorough check helps ensure you are not inadvertently reintroducing malware into your systems.

Specific Workloads:

File Level Recovery

When malware strikes, swift and careful action is crucial. However, always remember that malware can remain hidden before unleashing its attack. Reinstalling a clean operating system followed by file-level recovery is often the safest course of action unless you are certain the OS is uncompromised.

Key Steps for Safe Recovery:

Verify OS Integrity

Meticulously examine the operating system to ensure it has not been tainted by the ransomware.
If any doubt exists, consider reinstalling from a known clean template. Build automation can make this process significantly easier.

Recover to a Secure Haven

If the original system's trustworthiness is uncertain, restore files to a system you can confidently rely on.
This might involve building a new, isolated system or deploying a clean OS from a trusted template.

Pinpoint Attacked Files

Employ tools like Rubrik Ransomware Investigation to accurately identify the files targeted by the ransomware and initiate their recovery.

Protect Sensitive Data

Utilize Rubrik Sensitive Data Discovery to locate files containing sensitive information.
Implement robust security measures for these files, regardless of where they are restored.
Consider conducting further forensic analysis to determine if data exfiltration has occurred. If so, promptly notify the appropriate authorities.

Virtual Machine and Database Recovery

1. **Instant Recovery within Rubrik Brik (Ideal for Smaller Data Sets or Databases):**
   - **Swift Access:** Mount VMs and databases directly from Rubrik storage, bypassing lengthy copying to primary storage.
   - **Resume Operations ASAP:** VMs can provide services while being moved to primary storage in the background. Databases can function until a scheduled outage for relocation.
   - **Cautions:**
     - Best suited for smaller numbers of VMs or databases due to potential Rubrik cluster overload (not designed as a primary storage substitute).
     - Consider performance implications for VMs during Storage vMotion and the need for offline database movement during maintenance windows.

2. **Instant Recovery within VAST (Optimized for Speed and Large Data Sets):**
   - **Swift Access:** Swift Access: Mount VMs directly from VAST storage, bypassing lengthy copying to primary storage.
   - **Resume Operations ASAP:** Best choice for recovering numerous VMs, as it avoids contention with workloads writing data. maintenance windows.

3. **Mixing Instant Recovery with Exports (Proceed with Caution):**
   - Possible, But Plan Carefully: Exports prioritize full cluster resources, potentially impacting performance of VMs running from Instant Recovery.
   - **Manage Congestion:** Strategically schedule and monitor workloads to minimize performance degradation.

Policy and Procedure

This section will discuss a more contemporary approach to data protection policy and the procedures on how to attain maximum data security.
From US-CERT – United States Computer Emergency Readiness Team:

Large businesses or organizations should consider keeping one backup copy onsite and another offsite, either through a separate data service (such as a cloud service provider or remote server backup) or on the organization's own offsite servers or digital tape system. This "3-2-1" concept has become recognized as industry standard, and we suggest following these guidelines at a minimum when considering data protection policy.

We prefer to take this a step further into a concept we call the Zip Code of Availability as described herein:
Whatever data protection options you choose, organizations need to ensure they have an immutable copy of their data in the age of ransomware and follow the "3-2-1-1-0" rule for total data protection (see Figure 4):

3 – Keep 3 copies of any important file: 1 primary and 2 backups.
2 – Keep the files on 2 different media types to protect against different types of hazards.
1 – Store 1 copy offsite (e.g., outside your home or business facility).
1 – Air-gapped or immutable copy using WORM media
0 – Tools to verify full recoverability of backups

As part the zero access approach to accessing a data vault, it is also recommended that an administrative procedure is in place requiring a minimum of 2 authorized stakeholders approve access to the air gapped or immutable copies of the data in your vault in a documented manner.

Figure 4: 3-2-1-1-0 Rule for Data Protection

Policies should include data retention concepts that meet each company's business needs. We have designed and presented the concept of categorizing data, to determine its value to the business, for many companies and organizations. This can inform data retention policies that will vary, based on each organization's requirements. Here is an example of a simplified retention policy guide (see Figure 5):

Data Classification Decision Matrix

Data Classification	Description	Recovery Point Objective	Recovery Time Objective	Data Protection	Data Retention
Level 4 Platinum	Highly sensitive data; highest level of protection	Near zero	4-8 hours	Hourly backups; replication stored offsite	7-10 years
Level 3 Gold	Confidential data; protection required	1-2 hours	1-2 days	Daily backups; replication stored offsite	5-7 years
Level 2 Silver	Non-publicly released, non-sensitive data	1-2 days	1-2 days	Daily backups	2-5 years
Level 1 Bronze	Publicly released, non-sensitive data	7 days	7 days	Daily or weekly backups	1-2 years or less

Figure 5: Data Classification Decision Matrix example

Long Term Retention – Archive / Tape

Keeping data for long periods of time requires careful data management that must last longer than the archivists. This means your organization must have a plan for its long-term management and ongoing platform infrastructure today. How can it be easily curated, accessed, and analyzed in the future when the current experts are no longer present. Plus, how can it be ensured that data is always durably protected? The solution requires implementing an evolutionary storage architecture that can seamlessly adopt and decommission across multiple generations of platforms and technologies.

Archives also favor the most cost-effective digital storage (and perhaps the greenest technology that requires less energy for long term data storage). In 2024, the data storage landscape will undergo a transformative shift, with active archive solutions gaining even more prominence. Leveraging the power of LTO Tape technology for frozen data, organizations will adopt a tiered storage approach, seamlessly balancing performance, and cost efficiency.

Active archives will continue to integrate Tape libraries as a reliable and cost-effective solution for long-term preservation of infrequently accessed data, ensuring durability and data integrity.

Active archives can also be an important element in ransomware protections strategies. In 2024, continued attacks on critical infrastructure will drive organizations to rearchitect their approach to ransomware protection, placing equal emphasis on both prevention and recovery plans, and focusing on active archives to facilitate that. The trend will be towards immutable storage which can't be encrypted, greater focus on air-gapped storage which can't be reached by electronic viruses, practicing recovery events, and maintaining an accessible and current archive for all data.

Reference Architecture

Here is a reference guide to the integration between Rubrik, Zscaler, and VAST. Please see diagram below (see Figure 6):

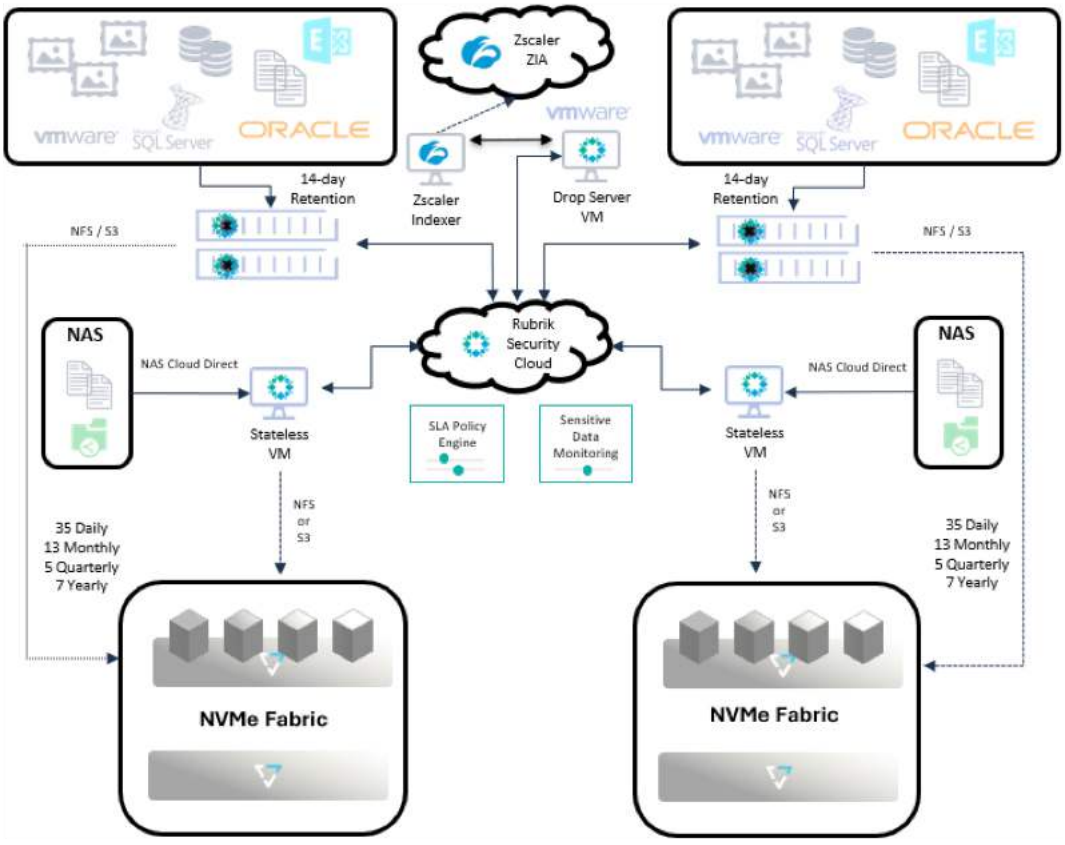


Figure 6: Rubrik, Zscaler, and VAST Integration

1 Configuration in Rubrik:

Rubrik maintains extensive Security Hardening Guides that must be followed to secure the Rubrik environment. This approach is necessary to keep bad actors from compromising the Rubrik infrastructure, which must be available to respond to a ransomware attack. Hardening the Rubrik environment is required after installation and configuration and before onboarding workloads to be protected.

Enable Sensitive Data Discovery (SDD): Activate the SDD feature within the Rubrik platform to scan for sensitive data within backups.

Create Compliance Policy: Define a compliance policy that specifies the types of sensitive data to be identified and protected (e.g., personally identifiable information, financial data, health records).

Create Rubrik Integration Configuration: Establish a connection between Zscaler and Rubrik by setting up an integration configuration. This involves providing API credentials for Rubrik to enable communication.

2 Configuration in Zscaler:

Configure Indexed Document Match (IDM) Template: The IDM template fingerprint which critical documents contain sensitive data in your organization.

Enable Data Loss Prevention (DLP): Ensure DLP rule is configured and set to Block mode within your Zscaler environment.

3 Integration with VAST:

Establish Connection: Connect VAST Data's Universal Storage platform to Rubrik's environment for seamless data transfer.

Configure Data Placement: Configure Rubrik to store backups on VAST's high-performance storage, enabling rapid recovery.

4 Data Scanning and Sharing:

Rubrik Scans for Sensitive Data: Rubrik initiates a scan of backups based on the defined compliance policy, locating sensitive data that matches the specified criteria.

Data Sharing with Zscaler: Sensitive files discovered during the scan are securely transmitted to Zscaler's IDM service for fingerprinting and indexing.

5 Indexing in Zscaler:

Fingerprinting: Zscaler IDM creates unique fingerprints for the received sensitive files, enabling accurate identification and tracking.

Indexing: The fingerprints are stored within a comprehensive index that serves as a reference for Zscaler's DLP policies.

6 Policy Enforcement in Zscaler:

DLP Policy Creation: Establish DLP policies that leverage the index of sensitive data to control and monitor data movement within your network.

Traffic Inspection: Zscaler's DLP engine continuously inspects outbound traffic, comparing data against the indexed fingerprints.

Policy Enforcement: If a match is found, the DLP policy is enforced, preventing the transmission of sensitive data to unauthorized destinations or services. This can include blocking uploads to cloud storage, email attachments, or file transfers.

In summary, ransomware attacks are growing at an alarming rate. However, using Rubrik's proven best practices, you can be prepared. At In Balance, we can help your organization navigate the recovery process and get back on track, faster.