Technical Review

Zero Trust Data Security with Rubrik

Date: January 2022 **Author:** Tony Palmer, Senior Validation Analyst

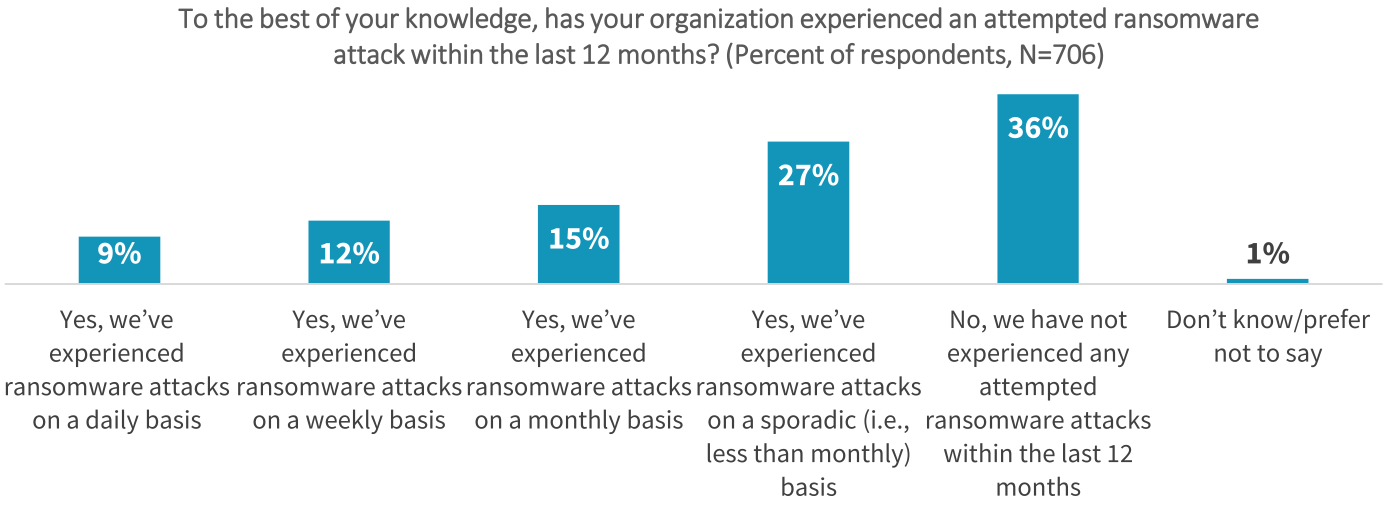
Abstract

This ESG Technical Review documents hands-on analysis and review of the Rubrik Zero Trust Data Security architecture. We examine how Rubrik protects backup data from ransomware attacks and accelerates the post-attack recovery process with its zero trust architecture.

The Challenges

Ransomware is pervasive and represents a serious threat to organizations of every size across industries. According to the U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN), U.S. organizations reported paying more than $590 million in the first half of 2021 to ransomware criminals in order to retrieve their data.[1] It's important to note that many organizations don't report ransomware attacks, so this number is likely much higher. In addition, the same report states that the 10 most commonly reported ransomware variants have driven the transfer of approximately $5.2 billion in Bitcoin transactions over the past three years. In fact, ESG's *2022 Technology Spending Intentions Survey*, which analyzes data collected from senior IT decision-makers at midmarket (i.e., 100 to 999 employees) and enterprise (i.e., 1,000 or more employees) organizations across North America, Western Europe, and Asia, revealed that a majority of organizations have had to deal with ransomware attacks over the past 12 months.[2] Specifically, 63% of organizations reported experiencing ransomware attacks at some point over the past 12 months, while 36% cited experiencing probing attacks on at least a monthly basis, including 9% that said they were targeted daily (see Figure 1).

Figure 1. Rate of Ransomware Attacks



Source: Enterprise Strategy Group

[1] Source: FINCEN Report, Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021, October 2021.
[2] Source: ESG Research Report, *2022 Technology Spending Intentions Survey*, November 2021. All ESG research references and charts in this report have been taken from this research report, unless otherwise indicated.

Further, nearly half (48%) of all organizations reported at least one *successful* ransomware attack, while 22% said their organization had been hit by successful ransomware attacks multiple times.

Moreover, nearly two-thirds (64%) confirmed that their organization has paid a ransom to attackers to regain access to its data, applications, and/or systems. Consequently, it should come as no surprise that 46% of organizations reported that ransomware readiness is one of their top five overall business priorities, and more than one in five (22%) say it is their most important priority.

The Solution: Rubrik Zero Trust Data Security

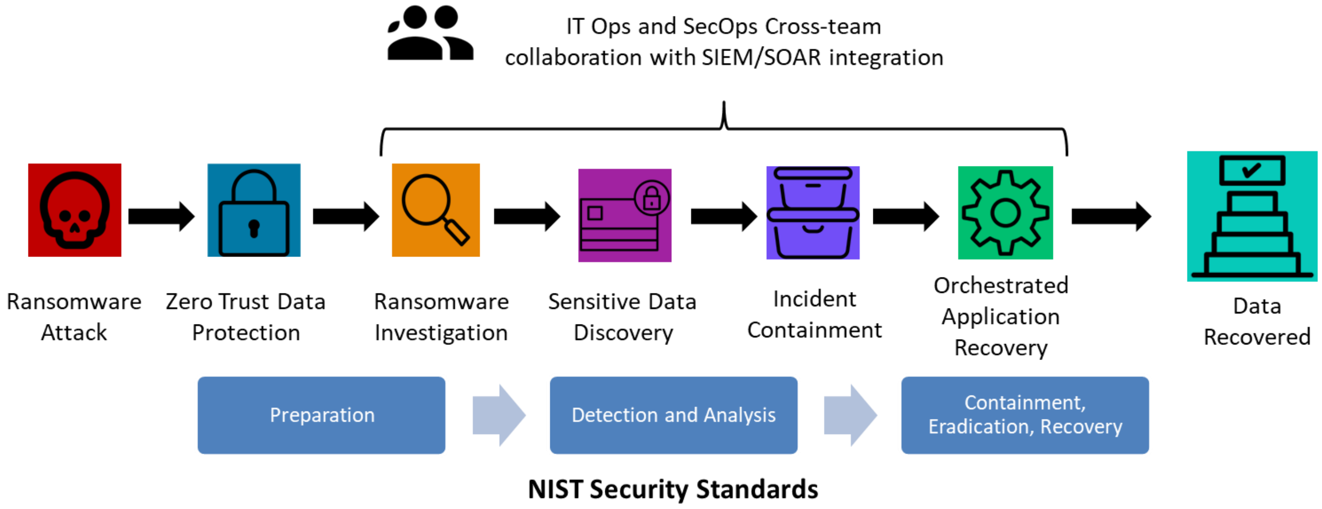
When people think about ransomware, they often wonder why people pay the ransom. The truth is that many data protection solutions don't have the capabilities to protect organizations from malware and, once attacked, there are limited recovery scenarios. When data is compromised, most companies find themselves doing a quick cost-benefit analysis of their options. If the right data protection solution is not in place, the organization must often pay the ransom. A big part of this analysis includes the consideration that, on average, it takes at least seven days for an organization to recover its data. This amount of time without the use of business-critical systems is often sufficient to put a company out of business.

Advanced ransomware is now targeting online backups, encrypting and/or deleting them completely. Recovering offline backups, such as tape, often takes too long and forces organizations to pay the ransom in order to return to operations. Additionally, many organizations don't have visibility into their backups. Because they are unable to view what they can recover, they may inadvertently reintroduce the malware—making the ability to investigate ransomware quickly and accurately vitally important.

Rubrik Zero Trust Data Security protects an organization's backup data from ransomware by design. The Rubrik Zero Trust Data Security architecture is modeled after the zero trust implementation model from the National Institute of Standards and Technology (NIST). At the core of Rubrik Zero Trust Data Security is a purpose-built file system that never exposes backup data via open network protocols. All access to the data written to this file system is proxied through the authentication engine, enforcing the zero trust model. This model creates a logical airgap that prevents data from being discoverable or accessible over the network, and prevents ransomware from ever accessing and encrypting or deleting the backups—an essential part of any modern protection strategy.

As shown in Figure 2, when ransomware locks down data, the IT Ops and SecOps teams come together to leverage Rubrik Zero Trust Data Security for data recovery. Once these teams verify that Rubrik Zero Trust Data Security was protecting the compromised systems, the teams will be able to use Rubrik Ransomware Investigation to identify the last clean recovery point, and use Sensitive Data Discovery to determine if the bad actors had accessed any sensitive/business-critical data on the systems. With Rubrik Orchestrated Application Recovery, organizations can recover all parts of their application with just a few clicks. Rubrik Zero Trust Data Security helps customers identify recovery points that are not compromised to protect them from reinfection. This is done highly efficiently thanks to Rubrik's machine learning capabilities and incremental forever backup architecture.

Figure 2. Rubrik Ransomware Recovery Overview


IT Ops and SecOps Cross-team collaboration with SIEM/SOAR integration
Ransomware Attack
Zero Trust Data Protection
Ransomware Investigation
Sensitive Data Discovery
Incident Containment
Orchestrated Application Recovery
Data Recovered
Preparation
Detection and Analysis
Containment, Eradication, Recovery
NIST Security Standards

Source: Enterprise Strategy Group

Rubrik Zero Trust Data Security is designed as a single platform for data security and management. Immutability is built in; once written, data cannot be read, modified, or deleted by anything outside the Rubrik platform. True immutability is a critical part of any effective ransomware protection strategy. Strong authentication of users—including multi-factor authentication (MFA)—helps to safeguard the system from intrusion. Fine-grained role-based access control (RBAC) improves the overall security of the platform, granting least-privilege access based on the specific role of a user or a service.

The Rubrik SLA policy engine simplifies and secures the protection of organizations' data, allowing thousands of backup jobs to be replaced by a small number of policies that can be tailored to specific application and business requirements. Rubrik SLA Retention Lock ensures that no single person can clear or shorten retention policies or delete archival or replication locations. The security of Rubrik's retention-locked SLAs is controlled through a validation process where modifications must be authenticated and acknowledged with the Rubrik support team. This key capability limits what an attacker or rogue administrator can do. This is especially important in strictly regulated industries requiring WORM compliance as mandated by the SEC (Securities and Exchange Commission) or FINRA (Financial Industry Regulatory Authority).

ESG Validated

This ESG Technical Review documents hands-on testing and analysis of the Rubrik Zero Trust Data Security platform. We validated the solution by leveraging multiple Rubrik-hosted demo sessions, reviewing case studies, attending an architecture briefing, and navigating the different components of Rubrik, which when combined, form an integrated ransomware protection strategy.

Cyber Resiliency Basics

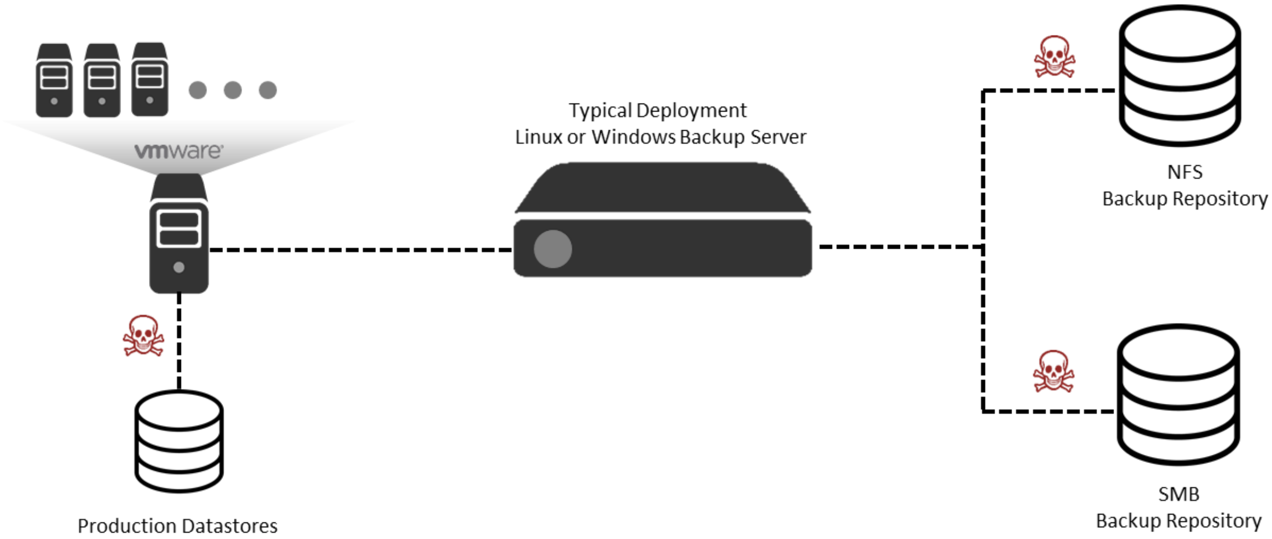
ESG began its testing by looking at "traditional" backup and recovery architectures, as seen in Figure 3, and understanding where ransomware vulnerabilities exist. There are three major categories of ransomware:

- *Crypto* ransomware prevents users from accessing files by encrypting them.
- *Locker* ransomware does not encrypt files, but rather locks the victim out and prevents access to the system.
- *Doxware* extorts victims by threatening to release stolen sensitive information if a ransom is not paid.

In all cases, once the system is compromised, the attacker will then demand payment with the threat of deleting or releasing your data to the public.

ESG explored the components of a common DIY data protection deployment. As shown in the middle of Figure 3, we see the server where the backup application is deployed. Usually, this would be any available server in the data center connected to the same network as the backup clients. Like the clients it is intended to protect, the backup server typically has some kind of access to the internet for patch management and remote administration. The backup server is where the backup application is installed, and it usually inherits the credential schema on which the IT organization has standardized. In addition to these access and credential issues, backup servers often leverage shared filesystems (NFS or SMB) to store backup images, which can make the backup application just as vulnerable as the systems it is intended to protect.

Figure 3. Traditional Backup Architecture



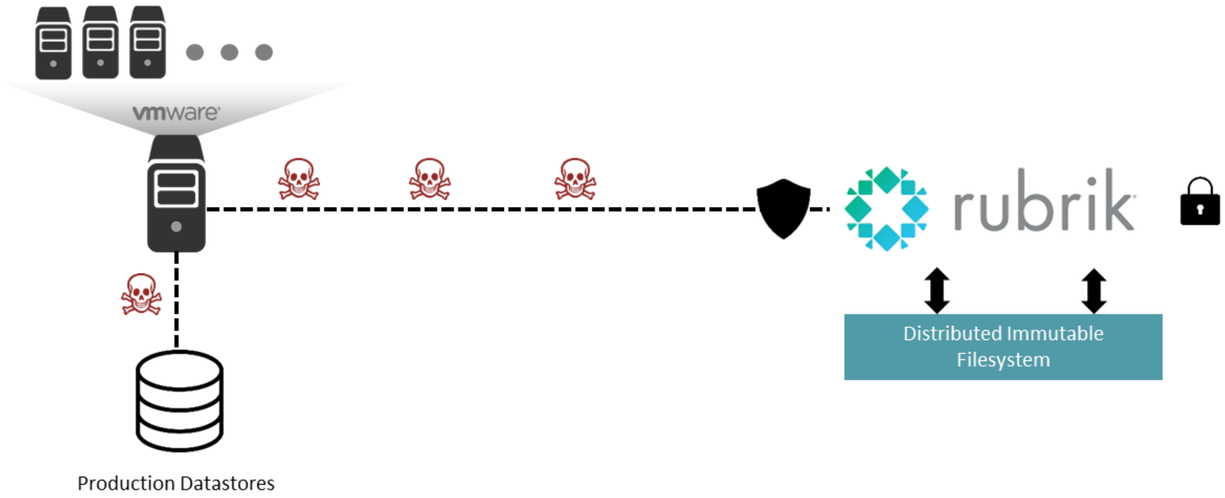
Source: Enterprise Strategy Group

It's a challenge to prevent a ransomware attack from happening, and attackers are constantly looking for—and finding—vulnerabilities. When malware can elude preventative measures like firewalls, endpoint detection and response (EDR) solutions, and intrusion prevention systems (IPS), recovery from backups is key. If a backup is not immutable, once data is written, it can still be modified or deleted. In a traditional backup and recovery architecture where backup software is not decoupled from the typical storage system, a vulnerability may exist that allows the ransomware to enter. Most backup solutions use NFS or SMB storage as their backup target. If the ransomware successfully targets the shared filesystem, backups become vulnerable to encryption, deletion, or denial of access. Rubrik Zero Trust Data Security has a purpose-built, append-only file system that is tightly integrated into its backup appliance and its security schema, which does not expose the filesystem to ransomware attackers.

Figure 4 shows an overview of Rubrik Zero Trust Data Security resiliency features. Under normal operations, without true immutability, disk-based backup solutions run the risk of becoming infected with ransomware. This can include both existing backups and new backups currently being written. Unlike some traditional designs that use standard storage protocols for connectivity, Rubrik's zero trust design, coupled with a custom-built filesystem, prevents direct access to the underlying storage. Rubrik has an API-first design that requires authentication to all endpoints that are used to operate the solution. Authentication can be handled via credentials, security token, or service account. This authentication requirement also applies to environments using role-based access control (RBAC) and least-privilege access features to minimize the access any particular user or service has. Rubrik's UI, CLI, SDKs, and other tools consume the same APIs and are held to the same security requirements. All communications within and between nodes is secured and mutually authenticated.

API endpoints that control the underlying behavior of the Rubrik system require an additional level of authorization that can only be supplied from a certified technical support engineer. This prevents a malicious actor from being able to alter the behavior of a Rubrik cluster. This design allows Rubrik to claim true immutability, allowing organizations to quickly recover from a ransomware attack by using a backup—and without paying the ransom.

Figure 4. Rubrik Solution Resiliency Overview

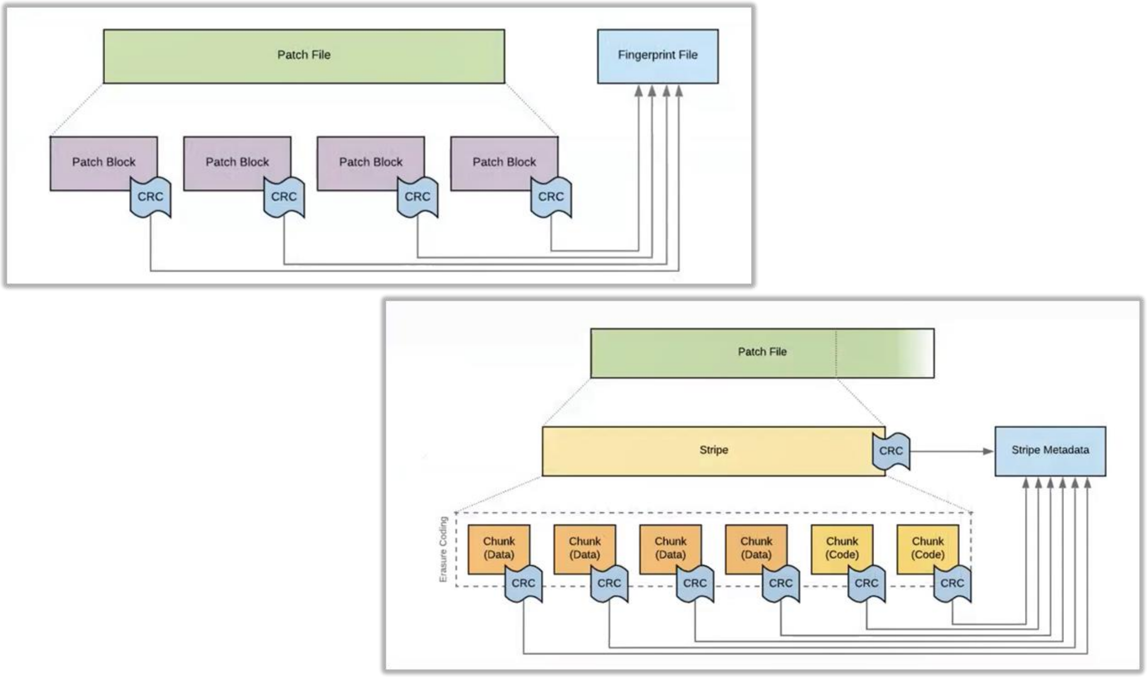


Source: Enterprise Strategy Group

Next, ESG took a deeper look into the Rubrik filesystem design, as shown in Figure 5. As backups are processed, all data is written into proprietary sparse files called *Patch Files*. Append-only files (AOFs) keep a record of data changes that occur by writing each change to the end of the file. This means that recovering the entire data set is performed by replaying the append-only log from the beginning to the end.

Cyclical redundancy check (CRC) checksums and fingerprints are then used to verify the integrity of a data transfer or a file. Checksums appear as long alphanumeric strings of characters that compare an original file to a copied version of that file to ensure they are the same.

Figure 5. Rubrik Filesystem Immutability Details



Source: Enterprise Strategy Group

Key resiliency features at the physical layer include:

- The AOF computes a stripe-level checksum, which it stores within each metadata stripe.
- Metadata is stored in a distributed metadata layer, protecting against potential data loss.
- A chunk checksum is computed and stored in the stripe metadata alongside the list of chunks.
- Replication and erasure coding[3]—a method of data protection where data is broken into fragments and stored with redundant data across a set of different locations or storage media—occur at the chunk level.
- If a data rebuild is needed, the resiliency provided by erasure coding is automatically leveraged in the background.

Why This Matters

The shift from physically air-gapped tape to online digital backup has created an attack vector that ransomware attackers can use to target backup systems. In the tape world, protocols such as TAR were used to transfer data from servers and storage to physical and removable tape media. If a recovery was needed, physical tape would be used. Now, with the use of digital backups, protocols such as NFS and SMB are employed. In many cases, this has created a mutable process burdened with both physical and logical layer challenges, including any transport layer issues inherent to NFS and SMB.

In contrast, Rubrik Zero Trust Data Security is based on a zero trust design. By eliminating the use of protocols such as NFS and SMB, leveraging immutable storage, MFA, fine-grained RBAC, and SLA Retention Lock, the Rubrik system is resilient against ransomware attacks designed to prevent a recovery from backup files.

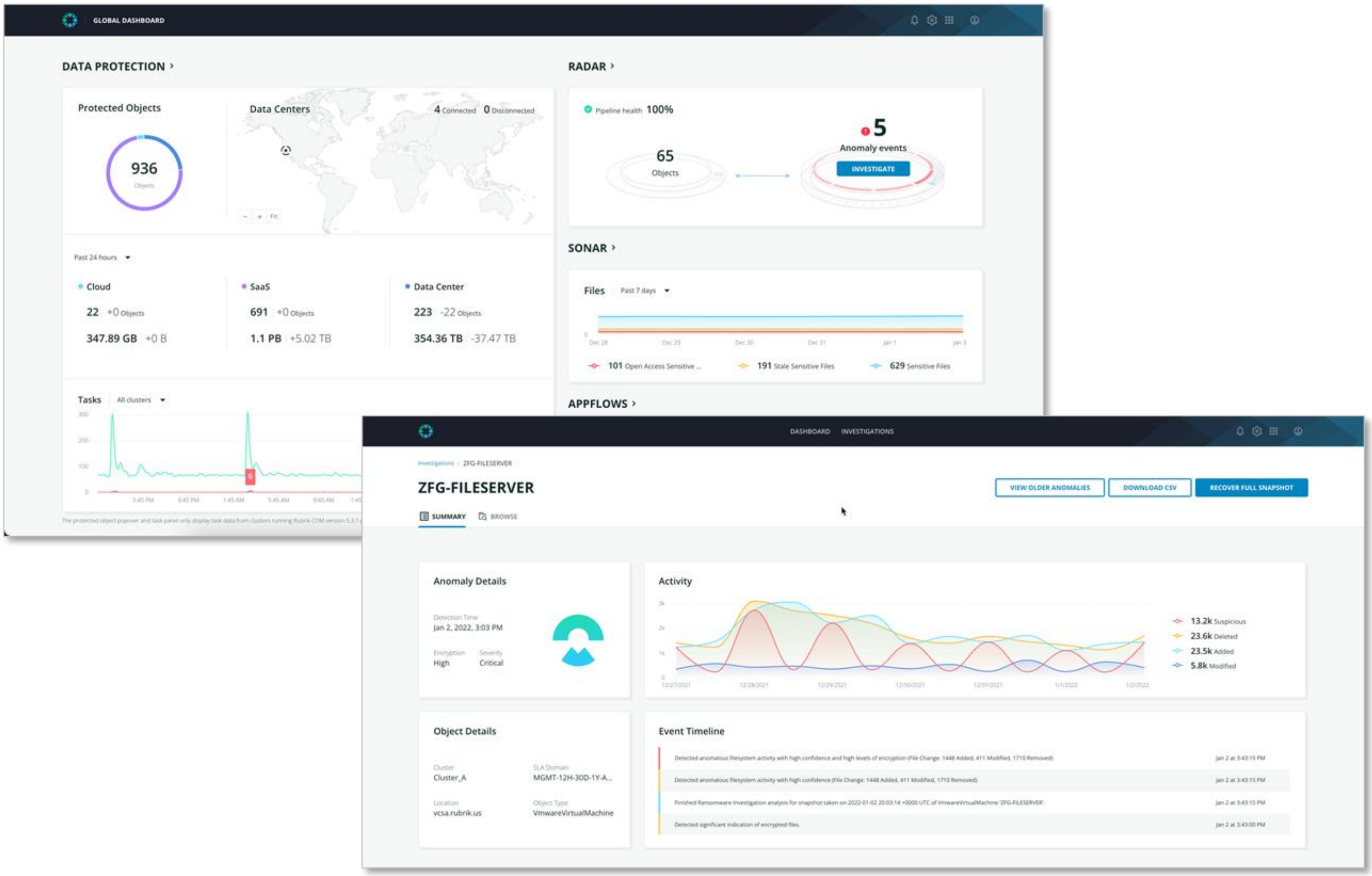
Ransomware Recovery Process

Recovering from a ransomware attack requires proactive data security and controls. In the previous sections, we focused on the importance of immutability to manage backups in preparation for an attack, and to initiate a fast recovery. In order to recover from an attack, it is also critical to have visibility into all of the organization's data and systems. An organization can utilize Rubrik, a SaaS platform that organizes business information and makes it discoverable and usable. Rubrik provides ML-driven insights with purpose-built services (Rubrik Ransomware Investigation, and Rubrik Sensitive Data Discovery) for data protection, governance, security, and mobility to ensure business continuity, accelerate time to value, and improve decision making.

As shown in the upper left of Figure 6, Rubrik Ransomware Investigation identifies anomalous behavior, such as ransomware, and makes recovery from ransomware attacks faster and easier. Rubrik Ransomware Investigation is not required to recover from a ransomware attack, but it provides a higher level of visibility into the scope of the attack, which can dramatically speed up the ransomware investigation process. Rubrik Ransomware Investigation monitors the behavior of the data within the Rubrik backups and creates a baseline analysis of historical behaviors considering frequency, time, and volume of activity. It looks for deviations from the baseline to detect whether there is an anomaly, such as an increase in the number of files added, deleted, or modified, indicating changes in normal backup behaviors. Rubrik Ransomware Investigation detects anomalies using filesystem analysis and file content analysis, which is critical to increasing the confidence of the detection model. Organizations receiving anomaly alerts can leverage Rubrik Ransomware Investigation analytics to dig deeper into the content of the files and look for signs of malicious encryption. Rubrik can then compute an encryption probability using a statistical model. This allows the analysis pipeline to compute entropy characteristics to measure the level of encryption in the filesystem without the wastefulness of a "brute force" workflow. Since this analysis occurs on the backup data on the data protection platform, this doesn't require the performance, security, or management overhead of OS agents.

[3] Source: Rubrik blog, *Erasure Coding or: How Rubrik Doubled the Capacity of Your Cluster*, February 2017.

Figure 6. Rubrik Visibility



Detection Time
Jan 2, 2022, 3:03 PM

Encryption: High
Severity: Critical

Cluster: Cluster_A
SLA Domain: MGMT-12H-30D-1Y-A...
Location: vcsa.rubrik.us
Object Type: VmwareVirtualMachine

```
Detected anomalous filesystem activity with high confidence and high levels of encryption (File Change: 1448 Added, 411 Modified, 1710 Removed)    Jan 2 at 3:43:15 PM
Detected anomalous filesystem activity with high confidence (File Change: 1448 Added, 411 Modified, 1710 Removed)    Jan 2 at 3:43:15 PM
Finished Ransomware Investigation analysis for snapshot taken on 2022-01-02 20:03:14 +0000 UTC of VmwareVirtualMachine 'ZFG-FILESERVER'.    Jan 2 at 3:43:15 PM
Detected significant indication of encrypted files.    Jan 2 at 3:43:00 PM
```

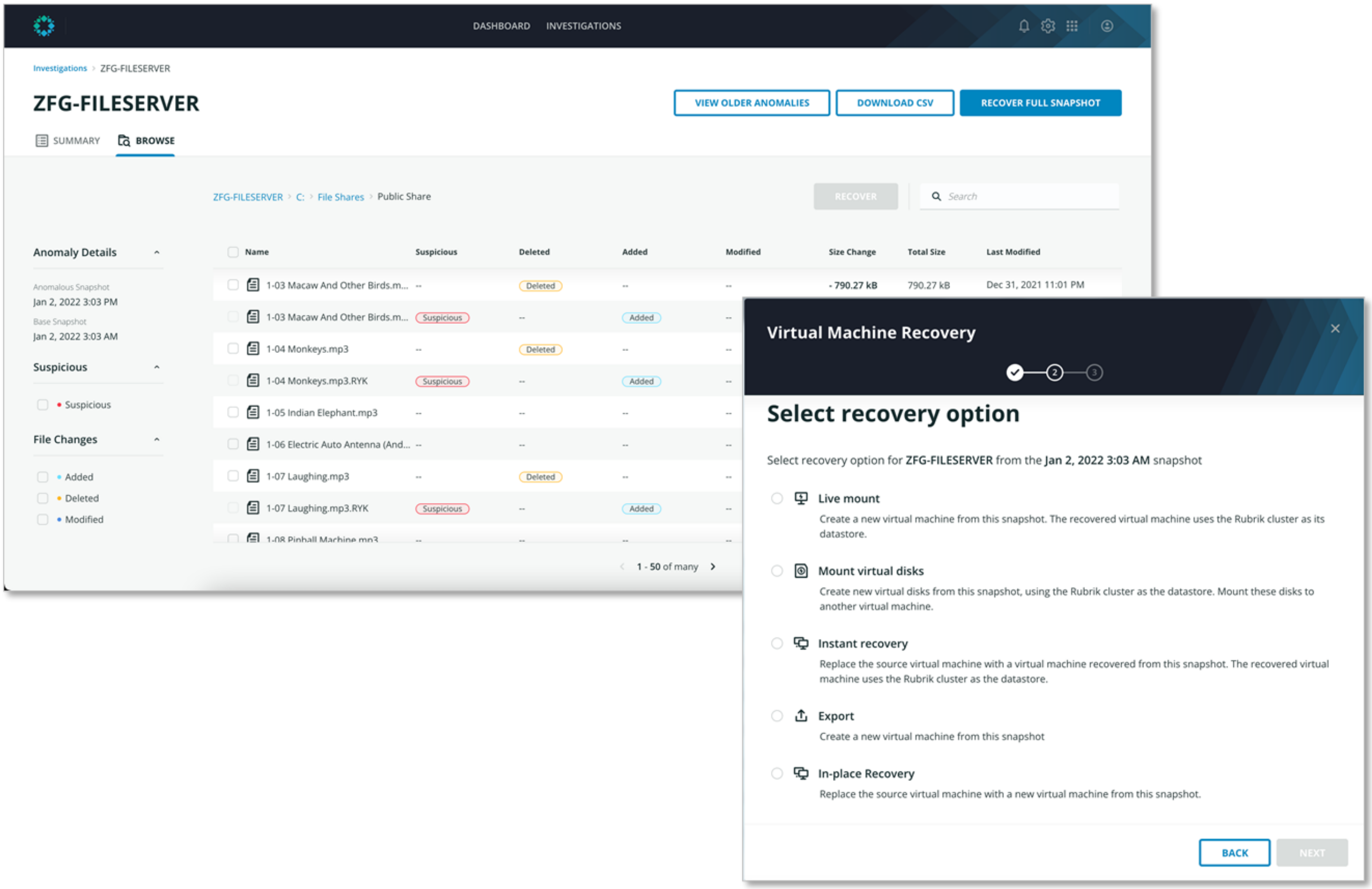
Source: Enterprise Strategy Group

After an attack on an organization's primary system, an administrator can access Rubrik Ransomware Investigation and begin the recovery process. As seen on the bottom right side of Figure 6, an administrator can quickly determine the timeline and best course of action to take for recovery. If an anomaly is detected, administrators can determine if this is due to normal or malicious activity.

As shown in the upper right of Figure 7, if volumes look suspicious, the administrator can drill down to the file level for deeper analysis. Suspicious files are flagged in red, blue identifies created files, and yellow identifies deleted files. The administrator can review these values and their histories to determine if behaviors have changed.

For administrators, there are several key questions to consider: Was there an attack? How and when did it happen? What is the right recovery point, and should the recovery model be at the file level, or a full snapshot? While recovering the full system state might be safest, it will inevitably take longer, and may risk the loss of data created since the ransomware encryption process began. As shown in the bottom right of Figure 7, administrators have many options for recovery: *Live mount*, *Mount virtual disks*, *Instant recovery, Export, and In-place Recovery*. Key capabilities include the ability to quickly Live Mount point-in-time copies of data into isolated networks for triage and root-cause analysis, which allows operations and security to work together, while Export provides the ability to completely reconstruct applications and services into different locations.

Figure 7. Rubrik Ransomware Recovery Process



Anomalous Snapshot
Jan 2, 2022 3:03 PM
Base Snapshot
Jan 2, 2022 3:03 AM

□ • Suspicious

□ • Added
□ • Deleted
□ • Modified

□ Name	Suspicious	Deleted	Added	Modified	Size Change	Total Size	Last Modified
□ 1-03 Macaw And Other Birds.m...	--	Deleted	--	--	- 790.27 kB	790.27 kB	Dec 31, 2021 11:01 PM
□ 1-03 Macaw And Other Birds.m...	Suspicious	--	Added	--			
□ 1-04 Monkeys.mp3	--	Deleted	--	--			
□ 1-04 Monkeys.mp3.RYK	Suspicious	--	Added	--			
□ 1-05 Indian Elephant.mp3	--	--	--	--			
□ 1-06 Electric Auto Antenna (And...	--	--	--	--			
□ 1-07 Laughing.mp3	--	Deleted	--	--			
□ 1-07 Laughing.mp3.RYK	Suspicious	--	Added	--			
□ 1-08 Pinball Machine.mp3	--	--	--	--			

Virtual Machine Recovery

✓ — 2 — 3

Select recovery option

Select recovery option for **ZFG-FILESERVER** from the **Jan 2, 2022 3:03 AM** snapshot

○ **Live mount**
Create a new virtual machine from this snapshot. The recovered virtual machine uses the Rubrik cluster as its datastore.

○ **Mount virtual disks**
Create new virtual disks from this snapshot, using the Rubrik cluster as the datastore. Mount these disks to another virtual machine.

○ **Instant recovery**
Replace the source virtual machine with a virtual machine recovered from this snapshot. The recovered virtual machine uses the Rubrik cluster as the datastore.

○ **Export**
Create a new virtual machine from this snapshot

○ **In-place Recovery**
Replace the source virtual machine with a new virtual machine from this snapshot.

Source: Enterprise Strategy Group

Restoring the earliest known clean snapshot can be the safest approach, but options exist to use a newer snapshot after reviewing where anomalies or concerns exist, and then recovering individual files that are suspect from a more recent point in time. This helps organizations achieve the best recovery time and recovery point objectives (RTO and RPO).

Why This Matters

Organizations rely heavily on their data protection vendors to ensure recoverability and reduce the time it takes for a restore when a data integrity event takes place. Modern malware attacks not only target production data but now extend into backup data sets to prevent victims from recovering without paying a ransom. Rubrik Zero Trust Data Security enables organizations to protect data backups from malware and ransomware attacks.

ESG validated that Rubrik Zero Trust Data Security—with immutable backups and visibility through Ransomware Investigation, and Rubrik Sensitive Data Discovery —allows an organization to quickly and easily recover from a malicious ransomware attack. Granular visibility into what was impacted allows for high precision in recovery to minimize data loss associated with the attack. If ransomware only affected a portion of the environment, organizations are able to recover that portion. RTO also becomes critical during these times, and proactive management of backup data with Rubrik Zero Trust Data Security can prepare an organization to recover quickly while limiting damage.

The Bigger Truth

Dealing with a ransomware attack is one of the most challenging events a data-driven organization can experience. It disrupts the organization at all levels. The costs of recovery and damage to an organization’s reputation can be immense. Unfortunately, it is not always possible to avoid a ransomware attack, and it feels like organizations are constantly struggling to stay one step ahead of attackers. If attackers do find their way in, organizations need to be able to rely on their data protection processes to quickly and confidently recover.

ESG verified that, unlike many other vendors that depend on third-party hardware and software products or tape solutions to achieve ransomware protection, the Rubik Zero Trust Data Security platform demonstrates robust ransomware capabilities. In ESG testing, Rubrik’s SLA policy engine, immutable backup storage, strong authentication—including multi-factor (MFA), fine-grained RBAC with least-privilege access, and SLA Retention Lock—demonstrated simple and secure protection of an organizations’ data.

Rubrik Ransomware Investigation and Rubrik Sensitive Data Discovery have created a holistic ransomware response strategy designed to protect any size organization. Our analysis was further validated with real-world case studies from customers who were able to instantly recover from ransomware attacks as well as others who hadn’t yet adopted a Rubrik strategy and had to pay dearly to recover from an attack.

Alarmingly, we found that some organizations still believe that paying the ransom could be a viable strategy. However, this only encourages more attacks. And just because attackers are paid doesn’t mean they won’t ask for more money—or even worse—they’ll just take the ransom and never unlock or return the data.

A serious ransomware protection plan needs to include a proven data security vendor that understands the multitude of challenges, and has built a solution that incorporates zero trust principles into technology that delivers clean, fast recovery for both on-premises and cloud-native workloads, file sets, databases, virtual machines, and instances. If your organization is looking for a solution that enables fast, seamless, confident recovery from a ransomware attack, ESG believes Rubrik Zero Trust Data Security is worth serious consideration.

The goal of ESG Validation reports is to educate IT professionals about information technology solutions for companies of all types and sizes. ESG Validation reports are not meant to replace the evaluation process that should be conducted before making purchasing decisions, but rather to provide insight into these emerging technologies. Our objectives are to explore some of the more valuable features and functions of IT solutions, show how they can be used to solve real customer problems, and identify any areas needing improvement. The ESG Validation Team’s expert third-party perspective is based on our own hands-on testing as well as on interviews with customers who use these products in production environments.