Technical Review

Quickly and Efficiently Recover from a Ransomware Attack with the Rubrik Data Management Platform Immutable Architecture

Date: May 2020 **Author:** Vinny Choinski, Senior Validation Analyst; and Christophe Bertrand, Senior Analyst

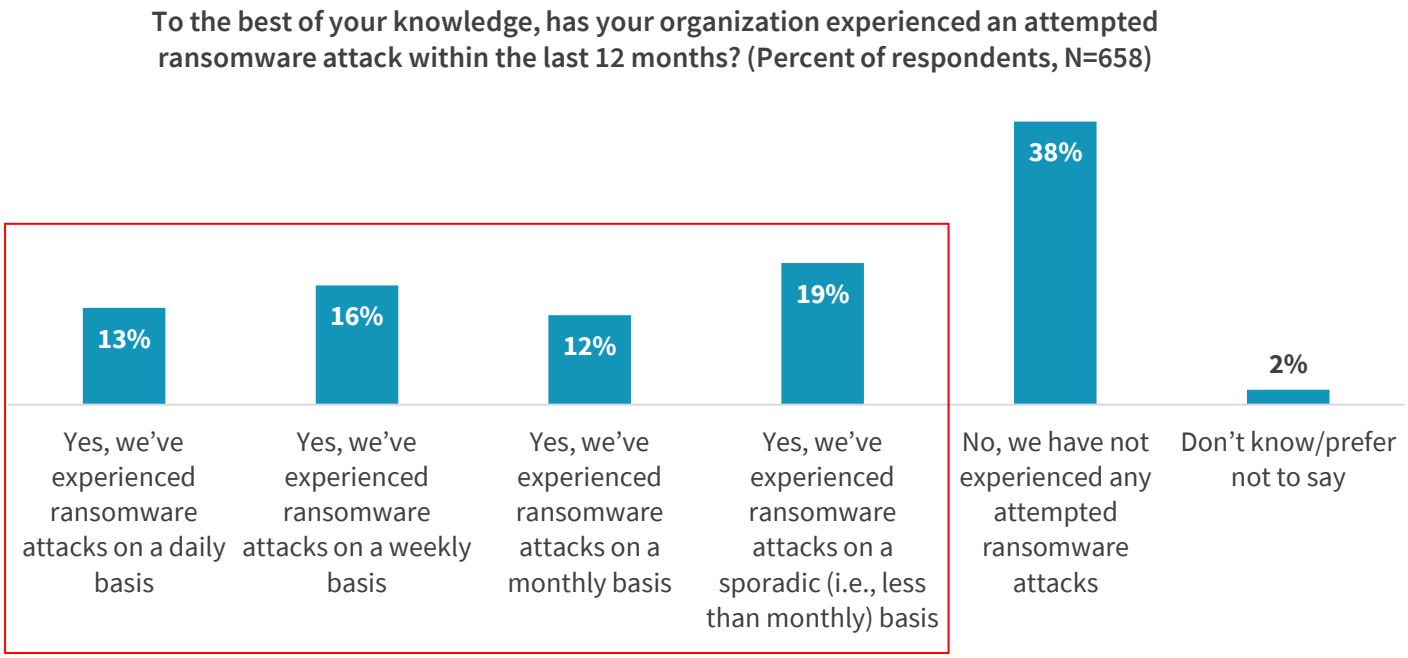
Abstract

This ESG Technical Review documents hands-on analysis and review of the Rubrik architecture. We examine how Rubrik protects data from ransomware attacks and accelerates the post-attack recovery process with its immutable architecture.

The Challenges

Ransomware is pervasive and represents a serious threat to organizations of every size. According to the FBI, organizations are paying more than $1 billion annually to ransomware criminals to retrieve their data. ESG recently completed its annual technology spending intentions research survey of 651 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 and Western Europe.[1] According to Figure 1, while 40% of organizations haven't suffered a ransomware attack (or prefer not to say), the majority of firms indicated that they dealt with ransomware in 2019. In fact, 60% reported experiencing a ransomware attack at some point over the 12-month period, with 29% reporting that attacks happened on a weekly basis (or even more frequently). Alarmingly, 13% faced ransomware threats daily! Organizations reporting a cybersecurity skills shortage were much more likely (67% versus 54%) to have been targeted by ransomware over the last 12 months. ESG's 2020 technology spending intentions research also indicates that 62% of organizations will increase cybersecurity spending in 2020, and it's safe to assume that, in many cases, ransomware concerns helped to at least influence these security investment positions.

Figure 1. Rate of Ransomware Attacks in 2019



Source: Enterprise Strategy Group

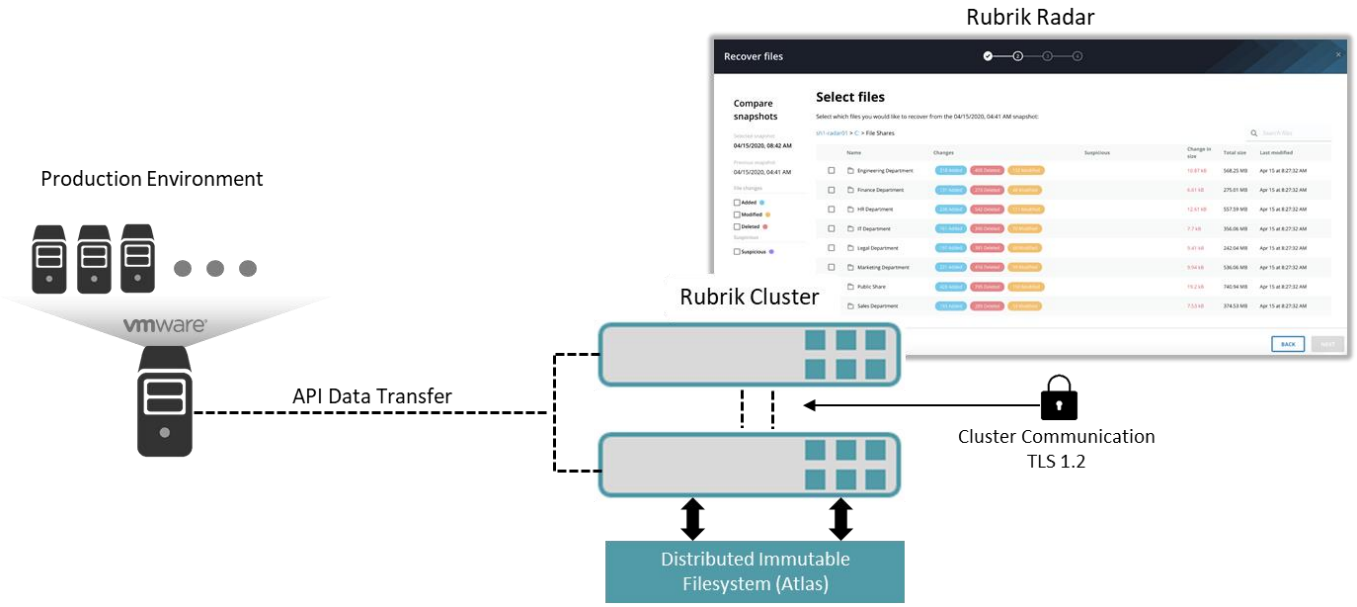
[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020. All other ESG research references and charts in this technical review have been taken from this master survey results set, unless otherwise indicated.

The Solution: Rubrik Ransomware Recovery

When people think about ransomware, they often wonder why people pay the ransom. Can't they recover from these attacks with their backups? The truth is that many solutions don't have the protection capabilities that organizations really need for malware protection and once in place, recovery scenarios quickly become limited. When data is compromised, most companies find themselves doing a quick cost-benefit analysis of their options. However, if the right data protection solution is not in place, it often leads to paying the ransom. A big part of the analysis includes the consideration that on average it takes at least seven days for an organization to recover its data, which is often enough time without business-critical systems to put a company out of business. Advanced ransomware is now targeting backups and thus encrypting/deleting them completely. This means recovering from offsite backups, such as tape, often takes too long, forcing organizations to pay the ransom in the end. Most organizations also don't have the visibility into their backups to know what they can recover without reintroducing the malware.

Rubrik, by design, protects your backup data from ransomware. The solution ensures multi-layered data security by encrypting all data at rest and in transit. As shown in Figure 2, each Rubrik cluster transfers data to and from a protection client using strong randomized password authenticated APIs. It leverages the TLS 1.2 protocol for both data transfers and node-to-node communication certification. All backup data is stored in an immutable format, making the data unalterable, thus preventing ransomware from ever accessing and encrypting or deleting the backups. This is essential in any modern-day protection strategy. With just a few clicks, an organization can recover quickly from an attack to the most recent clean-state point in time by leveraging Rubrik's incremental-forever backup schema.

Figure 2. Rubrik Ransomware Recovery Overview



Source: Enterprise Strategy Group

Key solution features include:

- **Immutability:** Once written, data cannot be read, modified, or deleted. True immutability is critical for any true ransomware protection strategy. The Rubrik architecture is designed to fully safeguard backups.
- **Impact Visibility:** One key to a successful recovery is knowing the exact point-in-time copy that is deemed clean from all malware as the backup to restore. Fast, accurate visibility saves valuable time.
- **Instant Recovery:** Time is money and reputation after an attack. Recovery time objective (RTO) must be kept to a minimum. Rubrik accomplishes this through incremental-forever backups and point-in-time recovery options, making it quick and easy to restore.

ESG Validated

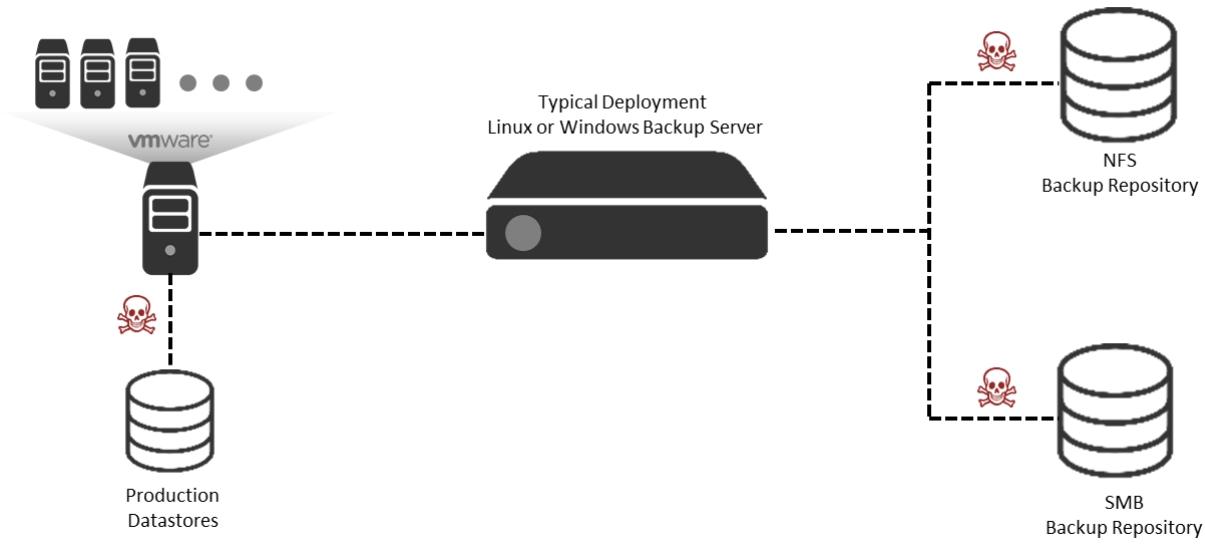
This ESG Technical Review documents hands-on analysis of the Rubrik for Ransomware solution. We validated the solution by leveraging multiple Rubrik hosted demo sessions, reviewing case studies, attending an architecture briefing, and navigating the different components of Rubrik, which, combined, form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

Data Protection Architecture Resiliency Basics

ESG began its testing by looking at the "traditional" backup and recovery architectures and understanding where the vulnerabilities exist, as seen in Figure 3. In essence, we want to better understand how a backup can get attacked and ransomware installed. Ransomware is a subcategory of malware, which is any malicious code or program that gives an attacker explicit control over your system. This includes viruses, bugs, worms, bots, rootkits, spyware, adware, and Trojans. It acts like an inside agent that installs malicious code on your computer or tricks you into loading a program either through malicious email attachments, web-based messaging, or a fake application update. As a result, the attacker gets hold of your system and the system won't respond to your commands anymore. Ransomware takes this one step further and encrypts your database and files. Once this happens, the attacker will demand payment to decrypt your files. There are three major categories of ransomware. Crypto ransomware attacks valuable files and prevents users from accessing them. Locker ransomware does not encrypt files, but rather locks the victim out and prevents them from accessing their system. Doxware is ransomware that extorts victims by threatening to release sensitive information if a ransom is not paid.

As shown in Figure 3, ESG explored the components of a common DIY data protection deployment using tools downloaded from vendor websites. In the middle, we see the Windows or Linux server where the backup application is deployed. Usually this is any available server in the data center connected to the same LAN as the backup clients. Like the clients it is intended to protect, it typically has some kind of access to the internet for patch management and remote administration. The server is where the backup application is installed, and it usually inherits the same credential schema the IT organization has standardized on. Because of this and because it often leverages filesystems (NFS and SMB) that ransomware knows and loves to store backup images, the backup application can be just as vulnerable as the systems it is intended to protect.

Figure 3. Traditional Backup Architecture



Source: Enterprise Strategy Group

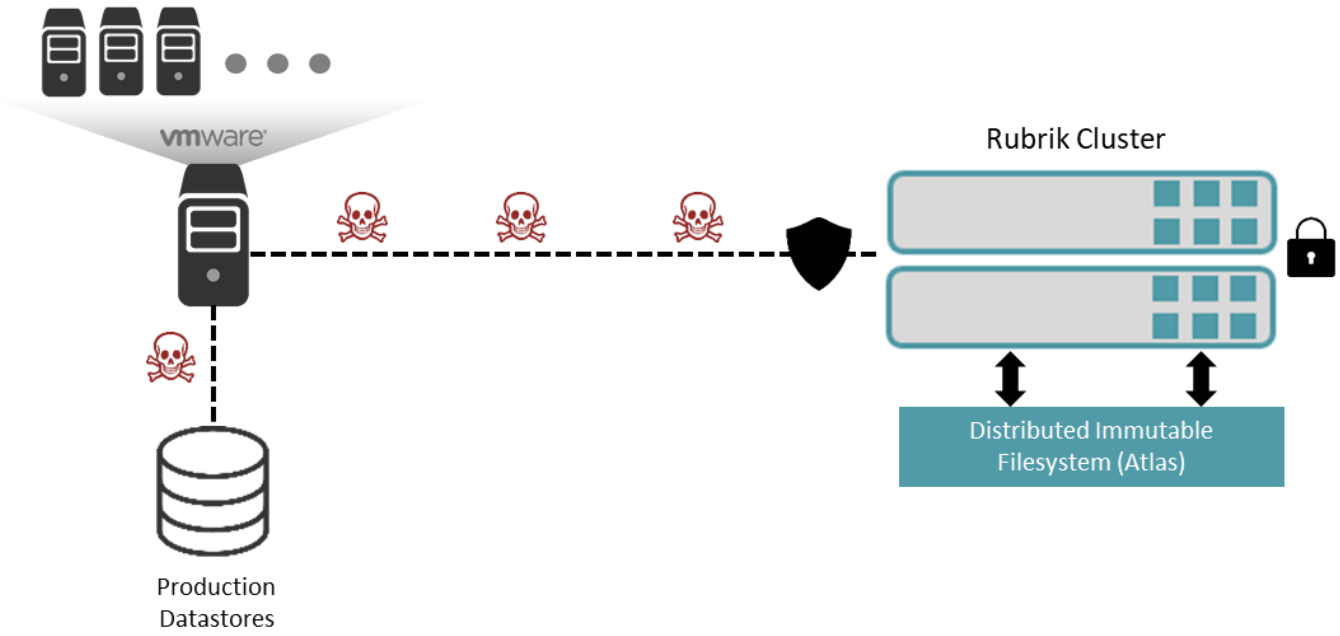
It's a challenge to prevent a ransomware attack from happening, and attackers are constantly looking for vulnerabilities. Equally important to prevention is recovery from your backups. The most secure way to ensure a successful recovery is through having an immutable backup solution. If a backup is immutable, once data is written, it cannot be read, modified, or

deleted. ESG found that in a traditional backup and recovery architecture where backup software is not decoupled from the typical storage system, a vulnerability may exist to allow the ransomware in. Most backup solutions use an NFS storage as their backup target. If the ransomware is targeting the NFS filesystem, backups become vulnerable. Once in place, it can then encrypt the backup and prevent access. This can be a common problem with some leading backup vendors, but with Rubrik, storage is tightly integrated into the backup appliance and its security schema, which does not expose this vulnerability to ransomware attackers.

Figure 4 shows an overview of the Rubrik solution resiliency features. Under normal operations, without true immutability, disk-based backup solutions run the risk of becoming infected with ransomware. This can include backups currently being written as well as existing backups. With Rubrik's API-based architecture, access to the protection storage is hidden from the client network—unlike some traditional designs that use standard storage protocols for connectivity. Rubrik has an API-first design as part of the architecture, which requires authentication to all endpoints that are used to operate the solution. Authentication can be handled via credentials or secure token. This includes environments using role-based access control (RBAC) or multi-tenancy features to logically divide the roles, features, and resources that are under management. Rubrik's CLI, SDKs, and other tools consume the APIs and are held to the same security requirements.

API endpoints that control the underlying behavior of the 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 eliminates vulnerabilities and allows Rubrik to claim true immutability, with the ability to quickly recover from a ransomware attack from a backup without paying the ransom.

Figure 4. Rubrik Solution Resiliency Overview

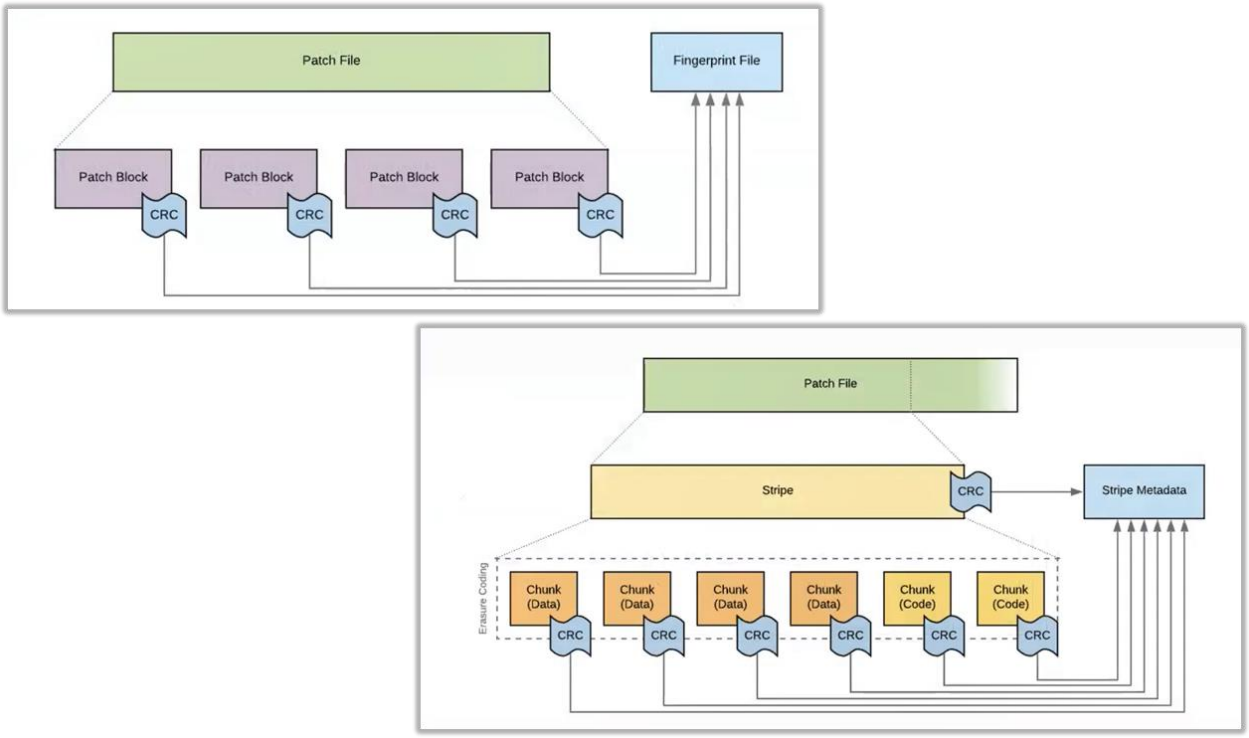


Source: Enterprise Strategy Group

Next, as shown in Figure 5, ESG took a deeper look into the Rubrik filesystem design. When a backup is run, Rubrik takes the following steps at the logical layer. All customer 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. In doing this, anyone could recover the entire data set by replaying the append-only log from the beginning to the end.

Cyclical redundancy check (CRC) checksum 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 act as digital fingerprints and compare an original file to a copied version of that file in order 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.
- A chunk checksum is computed and stored in the stripe metadata alongside the list of chunks.
- Replication and erasure coding 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 air-gapped tape to digital backup has created a vulnerability for ransomware attackers 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 digital backups, protocols such as NFS and SMB are used. In many cases, this has created a non-immutable process with both physical and logical layer challenges, including any transport layer issues inherent with NFS and SMB.

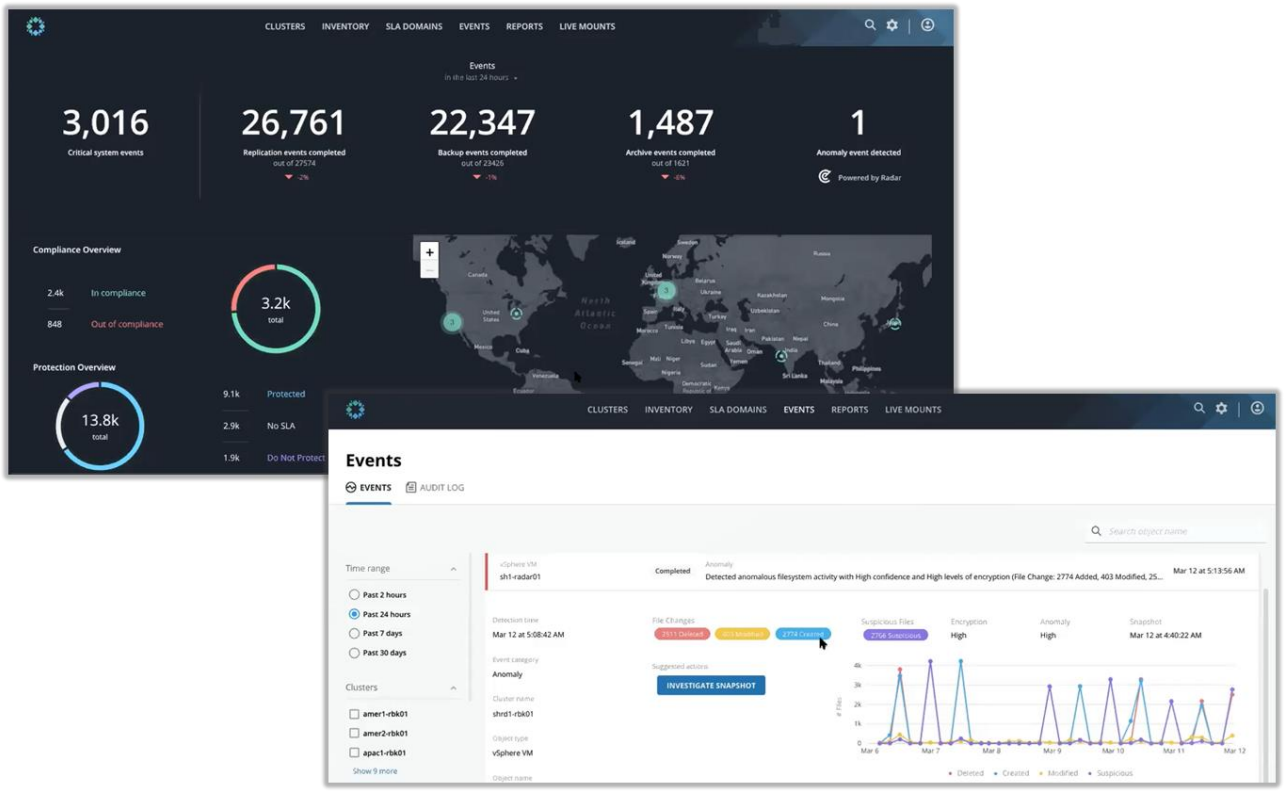
In contrast, Rubrik is an API-first design, which has eliminated the use of protocols such as NFS and SMB. By leveraging APIs, an interconnected system is created between production servers, storage, databases, applications, and VMs. Backups are initiated and processed with APIs, making the Rubrik system naturally immutable and resilient to ransomware attacks designed to prevent a recovery from backup files. This is also coupled with a strong logical and physical layer checksum and fingerprint process to ensure data integrity.

Ransomware Recovery Process

Recovering from a ransomware attack requires proactive data management 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. With Rubrik, an organization can utilize Polaris, a SaaS platform that organizes business information and makes it discoverable and usable. Rubrik Polaris provides ML-driven insights with purpose-built SaaS applications 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, Radar is Rubrik's application delivered via its Polaris platform to identify anomalous behavior, such as ransomware, and make recovery from ransomware attacks faster and easier. It should be noted that the Radar application is not required to recover from a ransomware attack, but it does provide a higher level of visibility into recovery options. Radar monitors the behavior of all the clusters and creates a baseline. Baselines are an analysis of historical behaviors and considers frequencies, time, and volumes. It then 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—basically, changes in normal backup behaviors. There are two ways Rubrik detects anomalies: filesystem analysis and file content analysis, which is critical to increasing the confidence of the detection model. If an anomaly alert is generated, organizations can leverage Radar analytics to dig deeper into the content of the files and look for signs of malicious encryption. The solution 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.

Figure 6. Rubrik Visibility

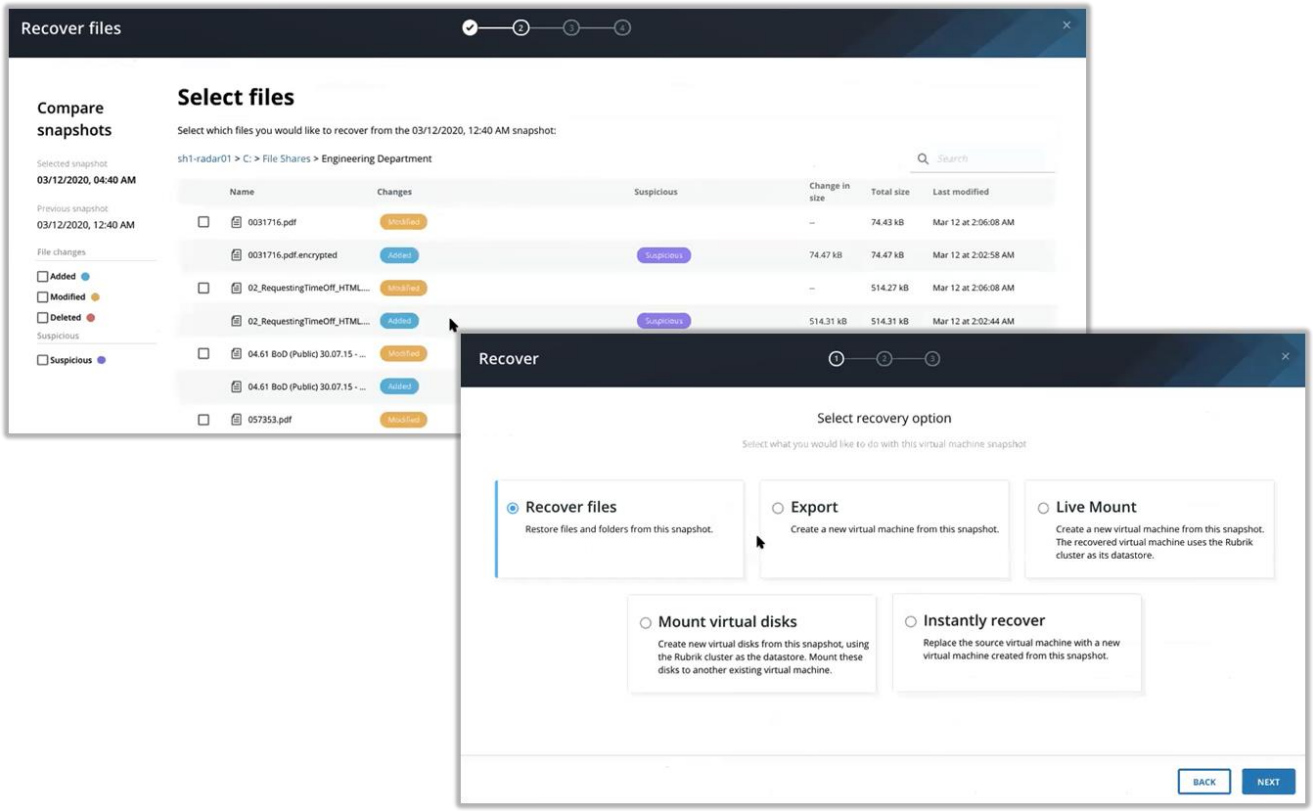


Source: Enterprise Strategy Group

After an attack on an organization's primary system, an administrator can access Radar and begin the recovery process. As seen on the bottom right side of Figure 6, an administrator can leverage the events page to quickly determine the best backups and course of action to take for recovery. In the center of the events page, three color-coded identifiers are present. Red identifies deleted files, blue identifies created files, and yellow identifies modified files. The administrator can

review these values and the history to determine if the behavior has changed. Radar flags suspicious activity in purple if an anomaly is detected, and the administrator can determine if this is due to normal activity or a malicious activity. As shown in the upper right side of Figure 7, if volumes look suspicious, the administrator can drill down to the file level for deeper analysis. For administrators, key questions to consider are: Was there an attack? How and when did it happen? What is the right recovery point, and should it be a file recovery or full snapshot? As shown in the bottom right side of Figure 7, administrators have many options for recovery, including Recover files, Export, Live Mount, Mount virtual disks, and Instant recovery. Going back to 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 different timestamp to help achieve the best RPO.

Figure 7. Rubrik Ransomware Recovery Process



Source: Enterprise Strategy Group

Why This Matters

Organizations rely heavily on their data protection vendors to ensure recoverability and reduce the time it takes for restore should a data integrity event take place. To prevent a victim from recovering without paying the ransom, new malware attacks not only target production data but now extend into the backup data sets. Rubrik enables organizations to protect data backups from malware and ransomware attacks.

ESG confirmed that Rubrik, with immutable backups, and visualization through Polaris and Radar, allows an organization to recover from a malicious ransomware attack quickly and easily. Granular visibility into what was impacted allows for surgical-level precision in recovery to minimize data loss associated with the attack. If ransomware only affects a portion of the environment, organizations can recover that portion. RTO also becomes critical during these times and proactive management of backup data with Rubrik can prepare an organization to limit the damage.

The Bigger Truth

Dealing with a ransomware attack is one of the most stressful events a data-driven organization can go through. It disrupts the organization at all levels and, if not prepared, the costs of recovery can be enormous and damage to an organization's reputation immeasurable. It is not always possible to avoid a ransomware attack and it feels like we are only staying one step ahead of the would-be attackers. If attackers do find their way in, organizations need to be able to quickly rely on their backup and recovery process.

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 data management platform, because of its design elements, inherits robust ransomware capabilities. The strong use of APIs, immutable backups, and Polaris Radar visualization has 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.

We found that some organizations even believe that paying the ransom could be a viable strategy. However, everyone should remember that this only encourages more attacks, and just because you pay an attacker doesn't mean they won't ask for more money, or even worse, just take your money and never unlock your files. Your only real contingency plan needs to be with a proven backup and recovery vendor that understands the challenges and has built technology that delivers the results you need. If you are looking to prepare for a fast, seamless recovery from a ransomware attack, ESG believes Rubrik is worth serious consideration.