Product Spotlight

How Rubrik Handles Ransomware Recovery

Storage Switzerland, LLC

George Crump | Lead Analyst

A ransomware attack puts IT in a battle against the malware author. To the victor goes the data. Every organization needs a prevention strategy. It also must realize that at some point the virus will get through, and at that point it will need a recovery strategy. Rapid recovery from a ransomware attack requires unique capabilities that not all data protection solutions have.

Requirements for Ransomware Recovery

Ransomware is a different type of disaster. First, it can strike at anytime. And once a night backup is not enough. Multiple protection copies have to be made throughout the day.

Second, depending on when the attack is identified, the malware will encrypt thousands if not hundreds of thousands of files. But the virus will not encrypt ALL files. Recovery requires identifying the correct files and restoring only those files.

The third challenge is that no other potential disaster specifically targets the protection architecture like ransomware. There are strains that not only go after popular snapshot solutions but also target backup software databases.

The final challenge is to perform the recovery quickly. With many legacy backup solutions it takes time to identify and select the impacted files needing recovery. And for most backup solutions the most time consuming recovery is copying back thousands of files one at a time.

Prevention is, of course, always the first step in Ransomware protection. Organizations need to do what they can to make sure that its servers are up to date, eliminate the use of older protocols like SMB 1.0 and ensuring that users get training to be aware of suspicious emails.

Rubrik's Ransomware Answer

Organizations also need to prepare for the inevitable; if a malware makes its way into the organization, a recovery will be required. The first step in that preparation is to make sure that data is frequently protected. Unfortunately, most backup solutions are difficult to architect to ensure the performance required for frequent backups.

The Rubrik Cloud Data Management platform includes a converged data protection solution. Meaning it provides both the protection hardware and the protection software in a single platform. Performance is built in via technologies such as change block tracking, parallel ingest, flash landing space and smart scheduling.

It handles the administrative complexity of frequent backups with ease. First, instead of creating jobs, protected objects are assigned to policies. Policies also define how many versions of data Rubrik should maintain, if it should replicate data, how long it should retain data and if it should be archived.

A major challenge to performing more frequent backups is how much data traverses the network from source storage to backup storage. Rubrik interfaces with the appropriate hypervisor or application to make sure only changed data is transferred and that applications including databases are in a backup mode prior to transfer.

Not all backup solutions can be considered a reliable fix for Ransomware. As stated earlier, some snapshots or backups are vulnerable to the same encryption attacks as source data. Rubrik architecture was designed to ensure that backup copies are immutable, or not writable once created.

Rubrik Restoration

If a ransomware malware makes it through the organization defenses, and the organization is prepared for it, IT must now identify the infected files and find the last known good copy of those files in the backup storage system. Identification is particularly hard if the malware made its way into a virtual machine and encrypted files within that VM. Many data protection solutions provide only limited search within the VM. The only option for IT is to mount a separate copy of the VM and manually extract files.

Rubrik, as part of its snapshot process, will launch a separate task to index files within the VM. It creates metadata for granular search and restore of those files. The search metadata is also global, searching across the on-premises store as well as an archive copy of the data in the cloud or on object storage. For Rubrik, finding the recovery copies for files infected by a ransomware attack is easy.

But even with the speed of Rubrik's index, manually searching for ten thousand or more infected files will still be a chore. Fortunately, Rubrik wraps all of its converged backup functionality around a REST API interface. Even the user interface uses the API to connect to back-end functions. Anything done through the user interface can alternatively be scripted via the API for maximum flexibility.

The REST API functionality works particularly in a Ransomware recovery situation. The list of impacted files can be pulled from the software that identified the corruption and then fed directly into Rubrik via that API, creating a fully automated recovery process.

In the worst case scenario, where an entire volume is corrupted, Rubrik has a live mount feature. This capability mounts a read-write version of a snapshot as a volume which the original VM can access. The result is almost instant access to data enabling users to get back to work quickly.

What makes Rubrik unique in its response to Ransomware is how simple it makes the preparation phase. First, one purchase delivers both hardware and software, modernizing the backup architecture in one step. Second, the software will automatically discover the virtual machines to protect. Third, assigning those virtual machines to service level agreements instead of backup jobs is much more user friendly. Finally, its recovery capabilities both in finding files as well as in restoring them is fast and painless.

More than Ransomware

While the threat of ransomware might motivate organizations to upgrade their data protection architecture, protection and recovery from ransomware should just be one aspect of it. A modern data protection architecture should protect against day-to-day mistakes as well as full scale disasters. Rubrik is a complete data protection solution, but unlike most data protection vendors, they provide both parts of the architecture; hardware and software.

The Rubrik Hardware

The Rubrik hardware is a scale-out shared nothing cluster built on commodity servers. The cluster is built via “Briks”, a 2U appliance with 12 HDDs and 4 SSDs. Each Brik has 4 hardware nodes per appliance. Each node has two processors and is assigned 3 HDDs and 1 SSD. The advantage of this configuration is that Rubrik provides a cluster in a box, enabling a customer to get started without having to buy 4 separate nodes and cable them up.

The Rubrik File System

At the heart of the Rubrik solution is its Atlas file system. It is a web-scale file system designed specifically to store and track multiple versions of data. It is also a master-less shared nothing architecture, eliminating bottlenecks and single points of failure.

The file system intelligently stripes data across disks and provides global deduplication and compression. It leverages the available flash storage to aide in data ingest performance and when using instant recovery. It is accessed via NFS and delivers a respectable 30K IOPS per Brik. If primary storage fails, Rubrik is a more than acceptable stand-in for the majority of workloads.

The Rubrik Software

The converged data protection functions include expected capabilities like backup, recovery, search, replication and archival. But unlike most data protection solutions these functions are all integrated into the system and not separate stand alone products. Rubrik provides application consistent snapshots for Microsoft Exchange, Sharepoint, SQL Server, Active Directory and Oracle RDBMS.

Rubrik also fully embraces the cloud, with their cloud connect functionality. They support Amazon S3 as well as other object stores. Rubrik uses this connectivity to archive old data copies to either of these destinations. There is also a cloud version of Rubrik, to protect cloud-based applications and enable cloud to cloud data movement.

Rubrik also recently improved its analytics and reporting capabilities. The system can now help organizations to plan for growth as well as reporting on SLA achievement on a daily or weekly basis. The Analytics feature can also monitor remote sites, to make sure they are ready in the case of a disaster.

StorageSwiss Take

Ransomware is an evolving threat. Its developers continue to get more creative over time. Combating this threat requires a modern data protection solution that can protect itself from attack, protect organizational data more frequently than once per night and make it easy to find data when a recovery is required. But that solution should do far more than protect against ransomware.

Organizations should use the ransomware threat as an opportunity to upgrade their entire data protection architecture to better protect the organization's data and improve data recovery. Rubrik makes that architecture upgrade a one-stop shop, introducing simplicity to a typically very complicated process.

Sponsored by Rubrik

About Rubrik

Rubrik is the market leader in Cloud Data Management, the world's first platform to orchestrate data for hybrid cloud enterprises anytime, anywhere. They blend future-proof architecture with consumer-grade simplicity to pioneer a fresh approach to an old problem. Rubrik's mission is to simplify how businesses around the world keep and use their data. Visit https://www.rubrik.com/ for more information.

About Storage Switzerland

Storage Switzerland is an analyst firm focused on the virtualization and storage marketplace. For more information please visit our website **storageswiss.com**