Pure Storage Ransomware Protection for FlashRecover

One of the most common ransomware attacks we see today is the destruction of backup data. The ability to recover quickly from this sort of destructive attack is a huge question mark for traditional backup systems or any purpose-built backup solution. Businesses cannot wait days or weeks to get their data back—they need to recover within hours from any sort of disaster to avoid incurring major downtime and the resulting loss of revenue.

With ransomware now targeting the backup ecosystem, your existing data protection solution may not be enough. Backing up data does safeguard against common disaster scenarios such as accidental deletion or natural disasters. But ransomware attacks can even further impact the backed-up data on the existing data protection infrastructure, and the ransomware threat is always looming. To address this challenge, Pure Storage and Cohesity have forged a strategic partnership and brought to market a first-of-its-kind solution.

What Is FlashRecover?

Pure Storage® FlashRecover//S™, Powered by Cohesity® is a true scale-out data platform that enables policy-based provisioning and management of data storage powered by FlashBlade®. This approach aims to disaggregate the storage and compute, gives the flexibility to scale the storage or compute independently, and lets you build a data center backup solution with lower costs. Pure Storage

FlashRecover//S offers a high-performance, simplified, and true scale-out data protection solution.

What's New in FlashRecover//S?

Pure Storage FlashRecover//S, Powered by Cohesity is an integrated modern all-flash data protection solution for rapid recovery at scale. This jointly developed solution is simple and fast and provides reliable backup and recovery for enterprise data—and much more. Pure Storage FlashRecover//S, Powered by Cohesity allows you to restore petabytes of data in *hours*, not days or weeks. It also provides an extra layer of data security that's game-changing in this era of ransomware attacks: With FlashBlade SafeMode™ turned on, all your backed-up data is protected with read-only mode snapshots that cannot be deleted or eradicated and are available for restore at any time.

Before diving deep into the FlashRecover//S implementation, I'd like to highlight one key business value proposition of this solution: With FlashRecover//S deployment in the data center, you can perform a complete disaster recovery of the cluster data and the backup data in just a few minutes. No other purpose-built backup appliance solution has the capabilities to perform a complete on-prem disaster recovery of the backup data in minutes—it's possible only with FlashRecover//S.

What Is SafeMode in FlashBlade?

SafeMode in FlashBlade provides rapid recovery from ransomware events. FlashBlade SafeMode for filesystems does two important things to protect against malicious attacks. It enables you to:

- Create on-demand, consistent point-in-time SafeMode snapshots for FlashRecover filesystems
- Create SafeMode snapshots for other filesystems, based on the snapshot schedule defined on FlashBlade

The SafeMode snapshot feature prevents the user from eradicating the snapshots from the system. In this way, SafeMode provides a path to rapid recovery at the time of ransomware attacks.

Now let's take a look at the architecture of FlashRecover//S, Powered by Cohesity.

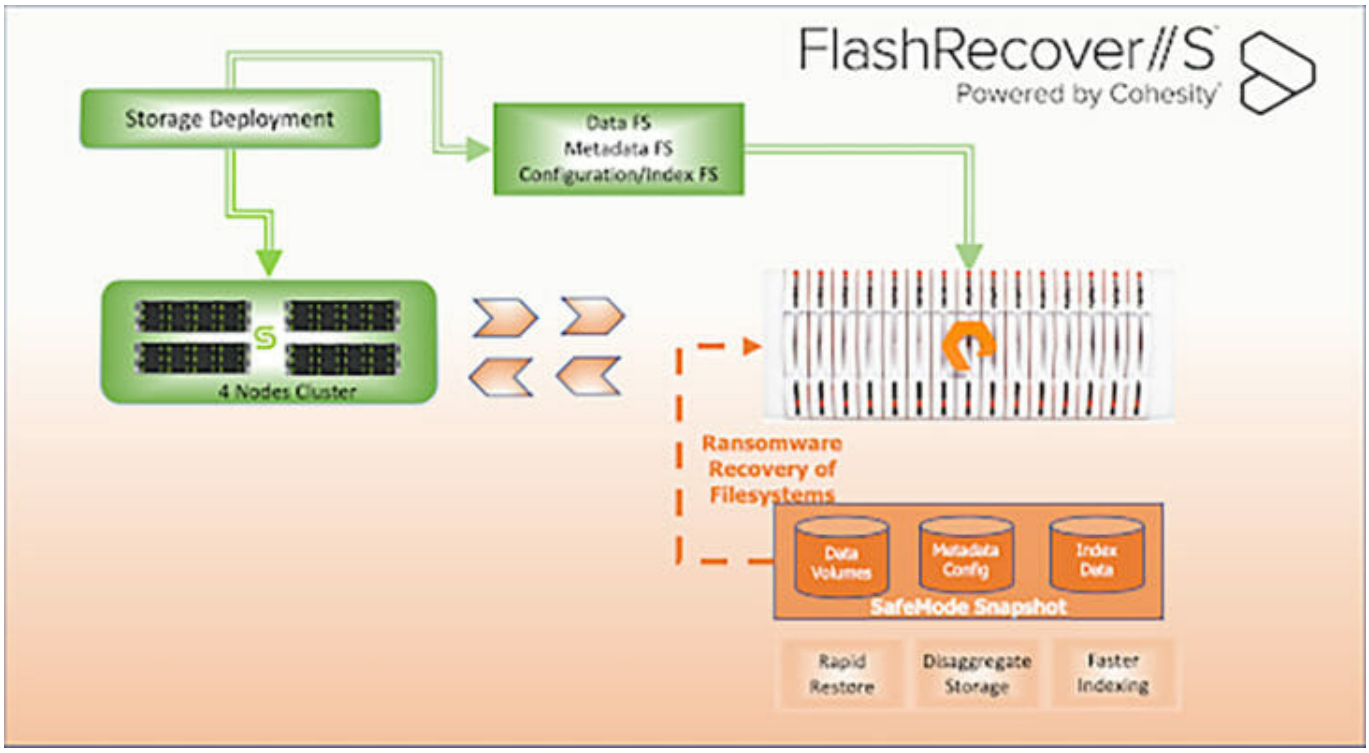

Figure 1: FlashRecover//S architecture overview.

The FlashRecover//S solution is made up of three main parts:

- **Cohesity DataProtect Software**
  - Cohesity DataProtect is simple, comprehensive, enterprise-grade backup and recovery software for traditional and modern data sources.
- **Cohesity-certified Compute Nodes**
  - Cohesity DataProtect runs on Cohesity-certified compute nodes for Pure FlashRecover//S with no local drives.
- **Pure Storage FlashBlade**
  - Pure FlashBlade is the backend storage where the filesystems are created and mounted to compute nodes via NFS v3 protocol.
  - SafeMode is enabled on the FlashBlade system.

A FlashRecover//S deployment doesn't just create backup data filesystems for data on FlashBlade, it also creates the filesystems for metadata and configuration data on the FlashBlade filesystem. FlashRecover//S comes with the snapshot feature enabled by default, which means you can perform on-demand SafeMode snapshots of backup data, cluster data, and metadata on FlashBlade and later use them for recovery purposes.

Wondering How You Can Perform Consistent Snapshots on FlashRecover Filesystems?

To create a useful and consistent SafeMode snapshot of the backup copies, metadata, and configuration data, it's important to quiesce the services on the Cohesity cluster. Currently, manual intervention is required to perform the SafeMode snapshot. You can create the SafeMode snapshot of your FlashRecover//S via ssh logging into one of the FlashRecover cluster nodes. An **iris_cli cluster create-snapshot** command is used to create the snapshots. During this process, all of the cluster services will be

stopped and all of the current running jobs and schedule on the cluster will be terminated. During this process, an internal backup of the node local data to the appropriate FlashBlade filesystem is performed. Once the process completes all the prereqs for creating the snapshot, the cluster will create the snapshot of all the FlashRecover filesystems on the FlashBlade automatically. This is how simple it is to take consistent point-in-time SafeMode snapshots on FlashBlade, which can be later used to perform the recovery after a ransomware attack.

Note: The initial release of this feature requires manual intervention to perform consistent snapshots, because in the present implementation, automatic SafeMode snapshot creation via a FlashBlade schedule would not guarantee consistent snapshots of all FlashRecover filesystems. A later release of FlashRecover will have improved integration that may be able to cover the operational gaps in the process.

For a complete guide to disaster recovery of backup data with FlashRecover and SafeMode snapshots, please refer to this whitepaper and demo video of the solutions.

What's Next

I strongly recommend leveraging the integrated snapshot feature of FlashRecover and SafeMode snapshot on FlashBlade to get another layer of protection to protect yourself from any ransomware or malicious attacks on backup data.

Please refer to the following white papers and guides to learn more about FlashRecover:

- Restore virtual machines at the speed of 1PB/day (Pure1® login required)
- Demo video on backup and restore virtual machines at scale (Pure1 login required)
- Simplified Oracle protection with FlashRecover (Pure1® login required)
- Back up EPIC with FlashRecover (Pure1® login required)