Technical Review

Improved Ransomware Recoverability with SafeMode on FlashBlade from Pure Storage

Date: March 2020 **Author:** Vinny Choinski, Senior Validation Analyst; and Alex Arcilla, Validation Analyst

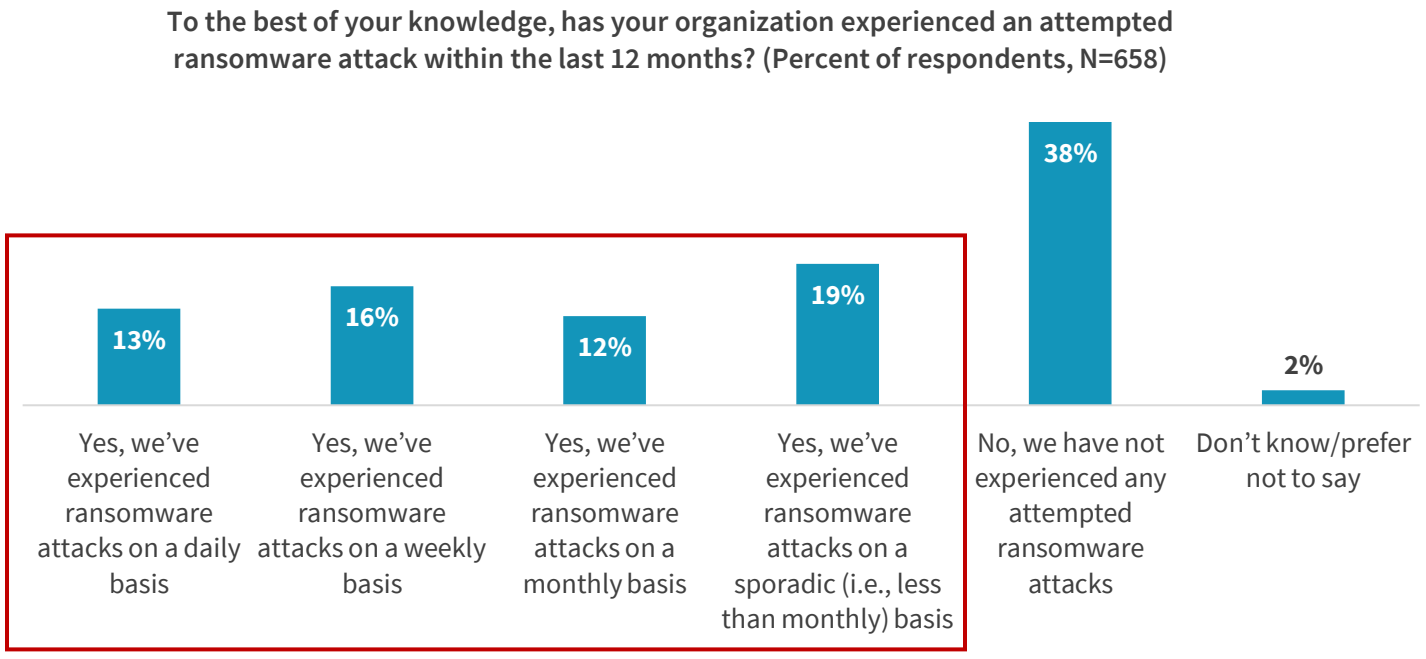
Abstract

This ESG Technical Review documents hands-on analysis and auditing of Pure Storage FlashBlade with SafeMode. We examine how SafeMode protects data from ransomware attacks or accidental deletion and integrates with current data protection solutions: Veeam, Veritas NetBackup, and Commvault.

The Challenges

Ransomware is pervasive and represents a serious concern for both business and IT leadership teams moving forward. 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 have dealt with ransomware in 2019. In fact, 60% reported experiencing a ransomware attack at some point over the twelve-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

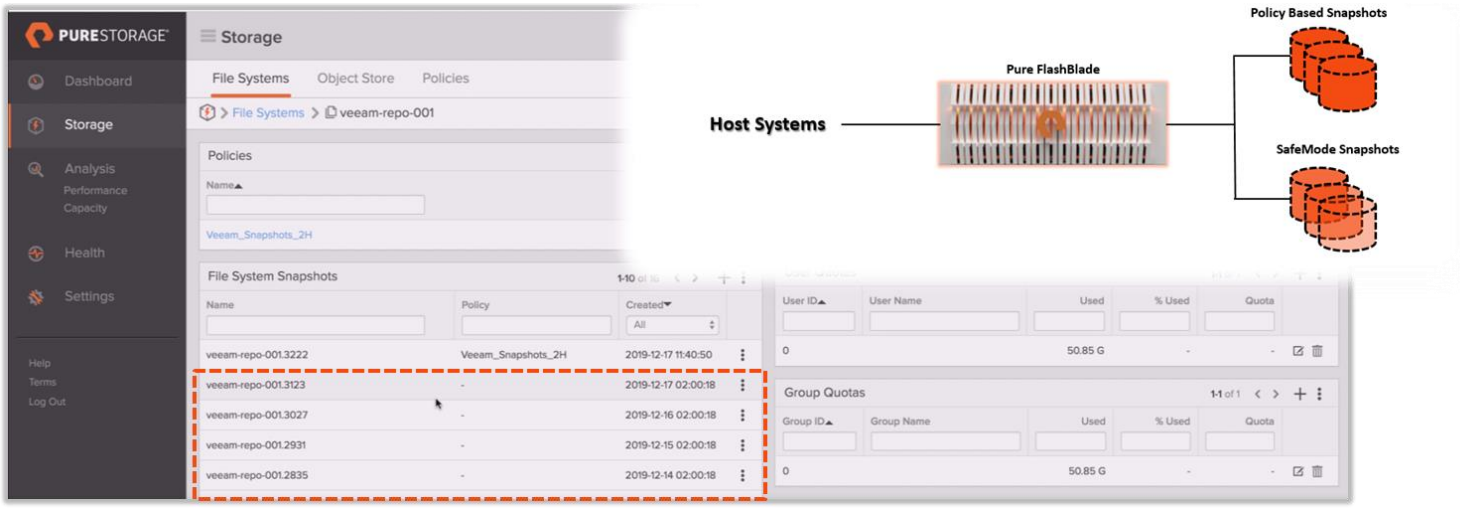
[1] Source: ESG Master Survey Results, *2020 Technology Spending Intentions Survey*, January 2020. All other ESG research references and charts in this technical review have been taken from this master survey results set, unless otherwise indicated.

The Solution: Pure Storage FlashBlade with SafeMode

The ever-increasing occurrence of ransomware attacks demands that organizations have a comprehensive approach to defend against such threats. This defense needs to include cybersecurity awareness and education for employees since many attacks launch through some kind of human interaction; collaboration between cybersecurity, systems, and data protections teams to harden infrastructures; and a response plan that is easy to execute from backups and that can be kept secure and validated if recovery is required.

Pure Storage FlashBlade is an advanced scale-out file and object storage platform designed to consolidate data silos like backup appliances and data lakes. Its high performance and broad feature set are the foundation for a data hub that can also deliver significant value for workloads beyond data protection, including analytics, AI, test/dev, and EDA. As shown in Figure 2, SafeMode snapshots are a built-in feature of FlashBlade that enable you to create read-only snapshots of backup data and associated metadata catalogs after you've performed backups. SafeMode snapshots are created and managed automatically, independent of administrator control. You can recover primary or backup data directly from these snapshots, helping guard against attacks by ransomware, activities of rogue administrators or employees, and even accidental deletion, where original copies are corrupted or no longer available to facilitate a restore.

Figure 2. FlashBlade with SafeMode Overview



Source: Enterprise Strategy Group

Key solution features include:

- **Enhanced Protection:** Ransomware can't eradicate (delete), modify, or encrypt SafeMode snapshots. In addition, only an authorized designee from an organization can work directly with Pure technical support to configure the feature, modify the policy, or manually eradicate snapshots.
- **Simplicity:** SafeMode setup is very simple and requires no daily operational overhead to maintain.
- **Backup Integration:** Organizations can utilize the same snapshot process regardless of the backup product or native utility used to manage data protection processes.
- **Flexibility:** Snapshot cadence and eradication scheduling are customizable.
- **Rapid Restore:** Ransomware uniquely challenges backup systems to potentially recover massive amounts of data. FlashBlade helps organizations to leverage a parallel architecture with elastic performance that scales with data to speed backup and moreover recovery.
- **Investment Protection:** FlashBlade includes SafeMode snapshots at no extra charge. A current Pure subscription or maintenance support contract covers enhancements.

ESG Validated

This ESG Technical Review documents hands-on review and auditing of Pure Storage SafeMode. We validated the solution by leveraging multiple Pure Storage hosted demo sessions, attending an architecture briefing and deep dive, and navigating the different storage and data protection interfaces used for integration and management.

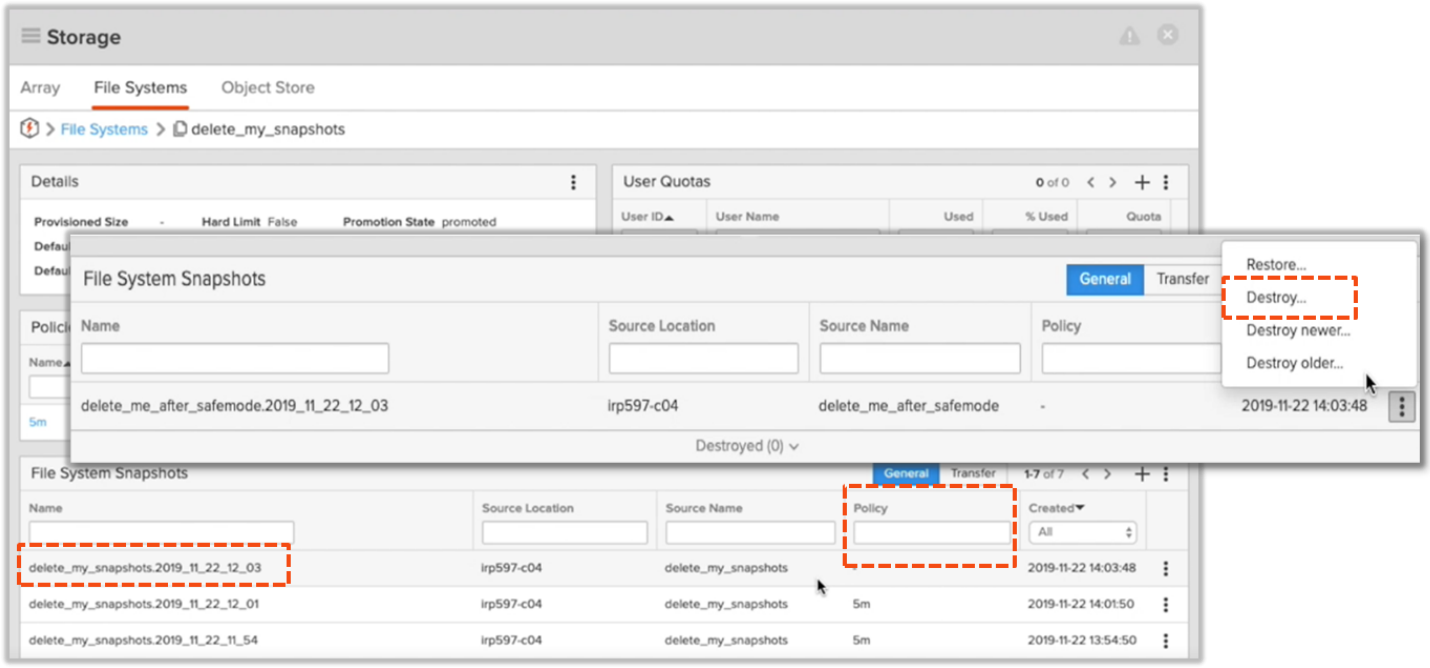
SafeMode Basics

Pure Storage SafeMode enables organizations to protect data backups of files or file systems from being compromised by ransomware attacks, accidental backup deletion, or rogue administrators. This prevents the manual and complete eradication (permanent deletion) of data backups from FlashBlade, enabling organizations to recover their FlashBlade systems after such events and return to production status quickly. SafeMode may only be activated by Pure Storage technical support.

ESG began its testing by reviewing how SafeMode protects against unintended removal of file or file system snapshots. Using the Pure Storage FlashBlade management interface, we navigated to the File Systems tab in the Storage menu to view the snapshots protected with SafeMode. Individual files or file systems protected by SafeMode are denoted by a blank entry under the Policy column. We used the snapshot named "delete_me_after_safemode.2019_11_22_12_03" (see Figure 3).

To completely remove the backup from FlashBlade, ESG first clicked on the stacked dots to the right of our SafeMode snapshot to reveal a pop-up menu and chose the Destroy option. This action moved the snapshot to the Destroyed Snapshots bucket.

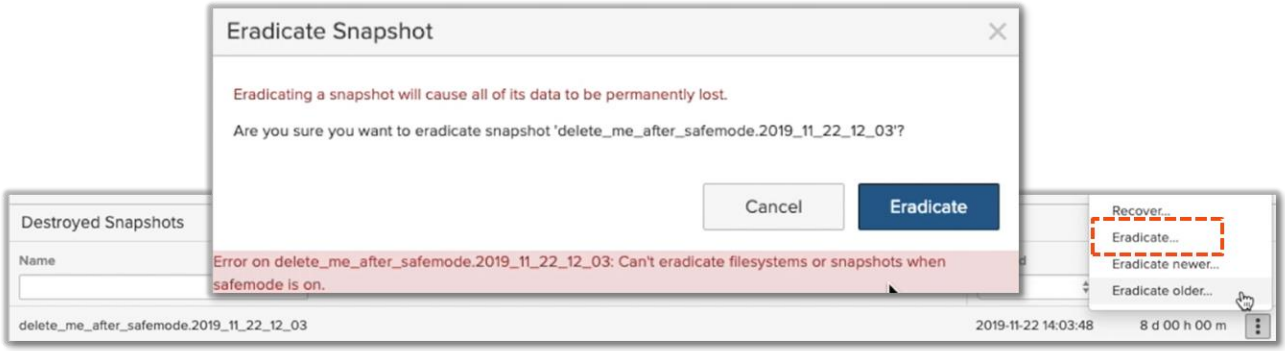
Figure 3. Snapshot Protected via SafeMode



Source: Enterprise Strategy Group

ESG then selected the same snapshot under the Destroyed Snapshots bucket, clicked on the stacked dots, and chose Eradicate from the menu. The interface flashed a warning message stating that the action will be permanent should we proceed. When we clicked on the Eradicate button, the error message in Figure 4 appeared, verifying that our chosen snapshot, protected by SafeMode, could not be permanently deleted. With SafeMode, an administrator can ensure that clean snapshots are still available to recover the FlashBlade system.

Figure 4. Attempting to Eradicate a Snapshot Protected by SafeMode

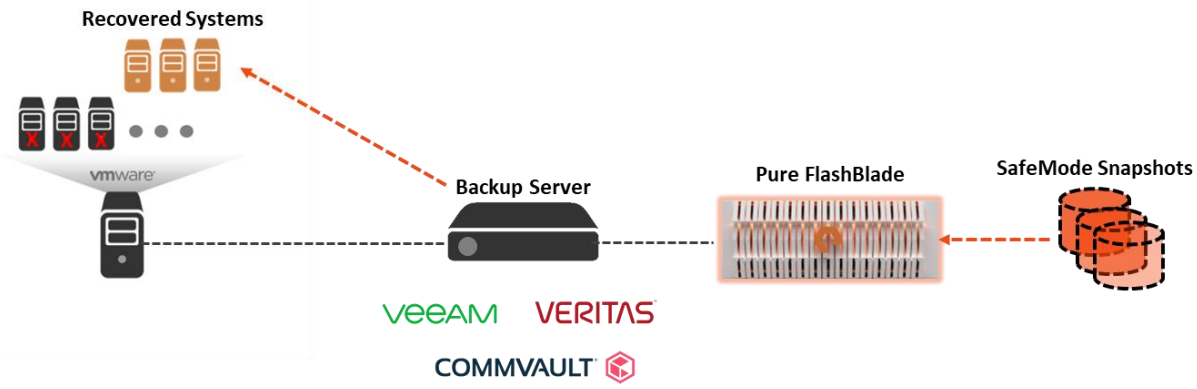


Source: Enterprise Strategy Group

SafeMode protects backups from ransomware by automatically creating read-only snapshots of data and associated metadata that cannot be deleted (see Figure 5). In other words, ransomware cannot write to the read-only SafeMode snapshots. Unlike policy-based snapshots managed by in-house administrators, SafeMode snapshots are dictated by policies enacted between a designated individual and Pure Storage technical support. SafeMode prevents designated backups from complete removal from FlashBlade, modification, or encryption, until preconfigured retention periods are met, and eradication may proceed.

Organizations can also leverage their existing data protection solutions with SafeMode, as illustrated in Figure 5, by directing the solution to use SafeMode snapshots for restoring data within FlashBlade.

Figure 5. Integration with Third-party Data Protection Solutions



Source: Enterprise Strategy Group

Why This Matters

Data backups compromised by ransomware, human error, or rogue administrators cost organizations lost time, revenue, and productivity. Having clean and available backups to recover and resume normal operations is critical when considering how to set both security and data recovery strategies.

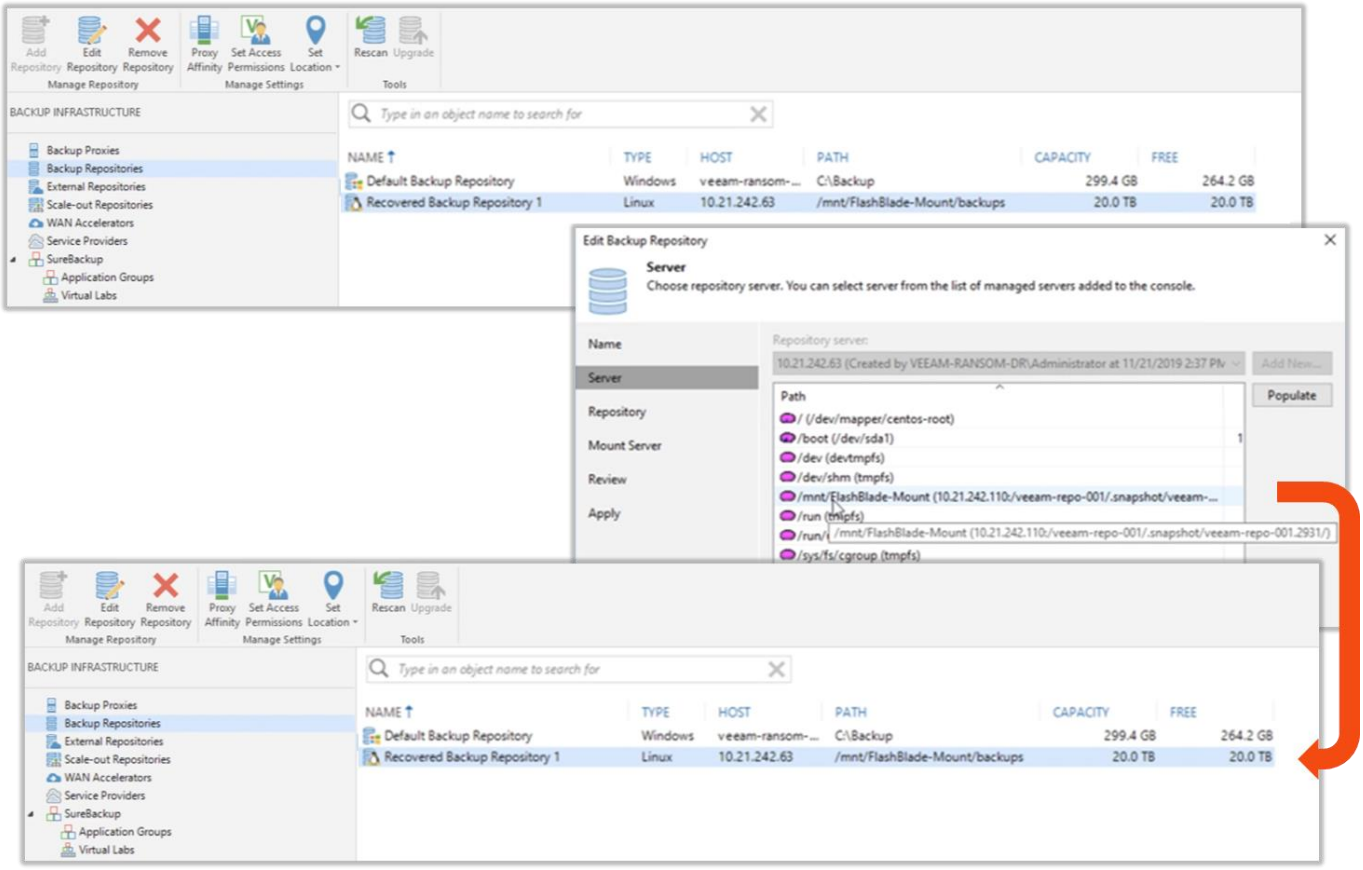
ESG verified that Pure Storage SafeMode on FlashBlade can prevent data backups from being modified, deleted, or encrypted by ransomware or other events. We observed how SafeMode provides an enhanced level of data protection by creating snapshots that cannot be changed or permanently deleted. Organizations can employ SafeMode to help ensure business continuity after events due to rogue activities or human error.

SafeMode Integration with Backup and Recovery

ESG conducted a more detailed review of how SafeMode on FlashBlade integrates with different data protection solutions. Here we looked at configuration options to help improve recoverability from a ransomware or other malicious attack with three different industry-recognized data protection solutions, including Veeam Backup & Replication, Veritas NetBackup, and Commvault Complete Backup & Recovery.

As shown in Figure 6, we started our integration exploration by leveraging a Veeam environment with a backup repository configured on a Pure Storage FlashBlade file system. The top of the figure shows the backup repository highlighted in the blue shaded area before a simulated attack. In this view, we saw the repository name (FlashBlade SafeMode Backup Repository), the type (Linux), the host (10.21.242.63), and the path (/mnt/FlashBlade-Mount/backups). For this test scenario, we concluded that both the production and the data protection environment were compromised by the attack.

Figure 6. FlashBlade SafeMode with Veeam Backup & Replication



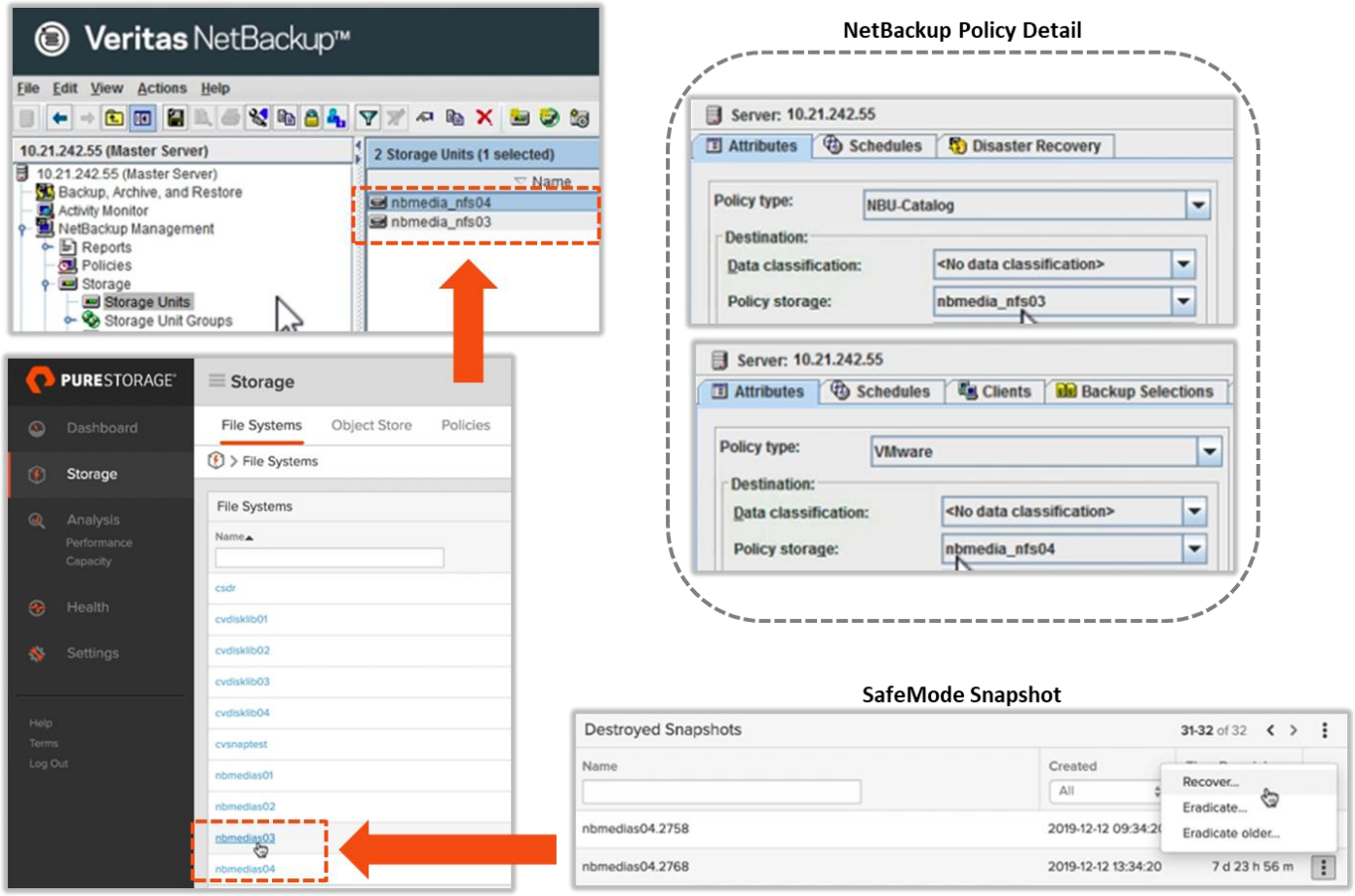
Source: Enterprise Strategy Group

To start the recovery process, a fresh install of the Veeam Backup & Replication application was conducted. It should be noted that this new instance of Veeam can be deployed on a physical server or virtual machine depending on resource availability at the time of the disaster. Then, as shown in the middle of Figure 6, we used the Veeam user interface to browse Linux host (10.21.242.110) for the read-only uncompromised SafeMode snapshot of the FlashBlade file system backup repository. As shown at the bottom of Figure 6, ESG simply created a new backup repository named Recovered Backup Repository 1. Then the new repository was scanned to import backup images and index the client information and history into the new Veeam instance. Once the scan was complete, we used the restore option in the Veeam UI to perform a full VM restore from the backup image in the SafeMode snapshot to recover the client backup data to a known good state.

Next, as shown in Figure 7, we reviewed the process of configuring Veritas NetBackup with SafeMode on FlashBlade. Veritas NetBackup uses the concept of storage units as a location to store both client backup images and backups of the NetBackup catalog. The NetBackup catalog contains application configuration settings and information about the client backup images that are also saved in storage units.

As shown in the top left side of Figure 7 in the orange callout box, the test environment was configured with two storage units (nbmedia_nfs03, and nbmedia_nfs04). These storage units were hosted on a Pure Storage FlashBlade with SafeMode snapshots configured. The NetBackup policy detail section of Figure 7 shows that the catalog is being backed up to storage unit ***nbmedia_nfs03***, and that backup policy ***VMware*** is leveraging storage unit ***nbmedia_nfs04*** to back up virtual machines in the environment.

Figure 7. FlashBlade SafeMode with Veritas NetBackup



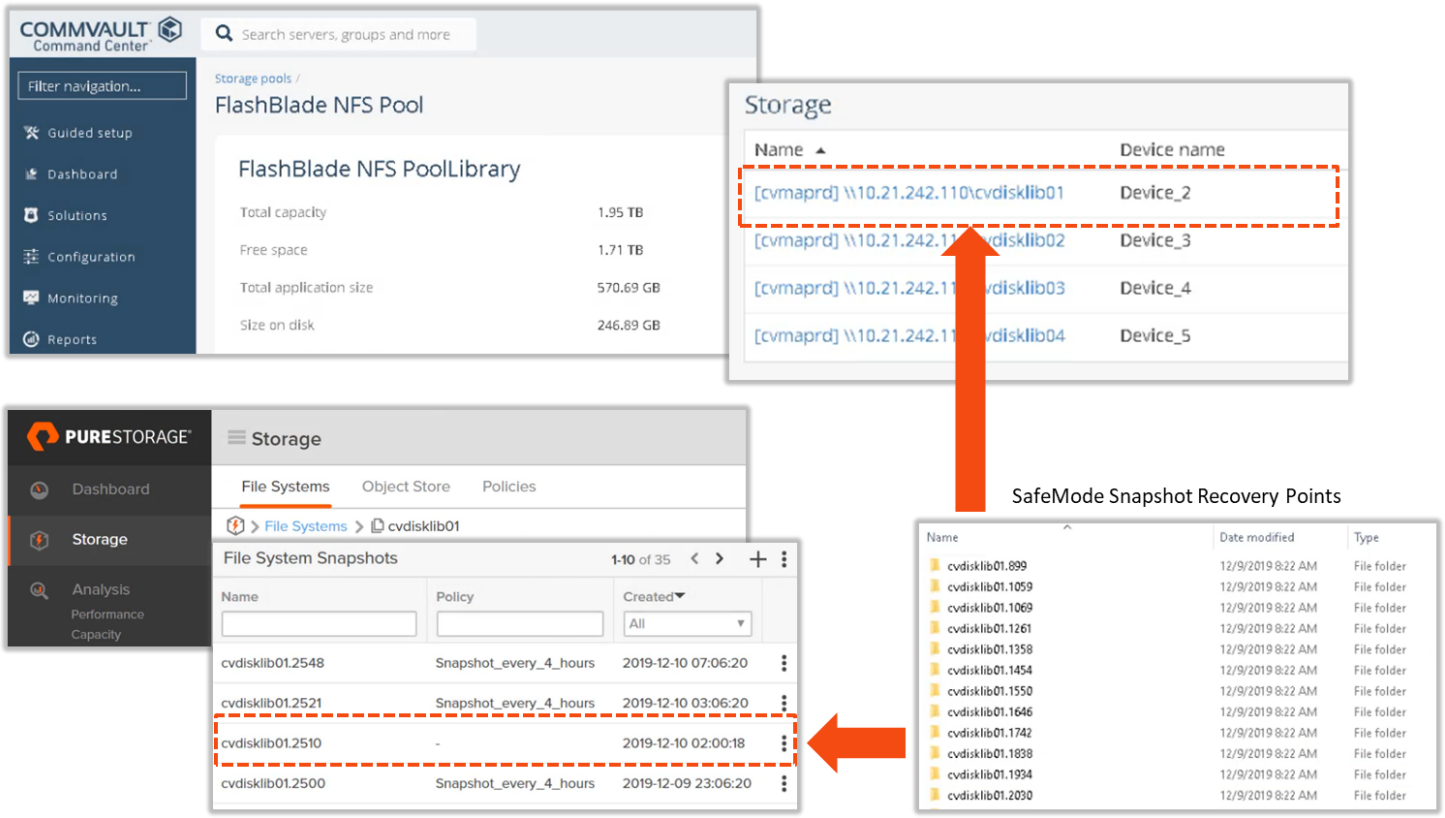
Source: Enterprise Strategy Group

We used the same test scenario with NetBackup as we did with Veeam. That scenario describes a situation in which the production systems as well as the data protection environment are compromised by ransomware. In this test, we actually deleted the FlashBlade file systems and standard snapshots and initiated a restore request which was subsequently unsuccessful. Then, as shown at the bottom of Figure 7, we used the FlashBlade UI to restore file systems ***nbmedia03*** and ***nbmedia04*** from a SafeMode snapshot and, with the file systems recovered, we restarted NetBackup services and used its UI to restore production systems to a known good state.

Finally, as shown in Figure 8, ESG reviewed the process of configuring Commvault Complete Backup & Recovery with SafeMode on FlashBlade. Commvault data protection uses the concepts of a CommServe and MediaAgents. The CommServe provides administrative control of the solution and the MediaAgents move and store backup images from

clients and recover data from backup images. Even though both components of the solution were protected during testing, Figure 8 focuses on recovering ***Storage Device_2*** from a point-in-time (pre-ransomware) SafeMode snapshot. As shown by the SafeMode snapshot recovery points section on the bottom right side of Figure 8, we used a SafeMode snapshot from December 9th to do a successful (pre-ransomware) recovery of the Commvault Storage Device_2.

Figure 8. FlashBlade SafeMode with Commvault Complete Backup & Recovery



Source: Enterprise Strategy Group

Why This Matters

You know it's going to be a bad day when you get to the office and find out you have been hit with ransomware. It only gets worse when you find out your backups have also been compromised. Today's cyber criminals are targeting not only end-user primary data, but also NAS files systems and object stores that many data protection solutions rely on to store backups.

Wouldn't it be great to have an extra level of protection with the right performance so that you knew your backup data was going to be good to go and able to meet or exceed your recovery SLAs when you need it the most?

ESG confirmed that FlashBlade with SafeMode can help add that extra level of preparedness to your data protection environment. Using it in conjunction with your data protection application can help ensure the data in your backup images is as you expect it to be—in other words, ready to use in the event of a disaster when you need it the most.

The Bigger Truth

It is not uncommon to hear yet another news story about ransomware attacks carried out against organizations of all sizes, from state government agencies to healthcare, media, and more. These attacks are not mere inconveniences, as businesses lose valuable time and revenue to recover from these events. Although it is ideal to prevent all attacks, organizations must have strategies in place to get the business up and running again should an attack occur. Backing up data via data protection solutions is a start, yet more can be done to keep clean and unadulterated backups available for faster recovery.

Pure Storage SafeMode on FlashBlade enables organizations to protect data backups against ransomware attacks, as well as accidental deletion or rogue storage administrator activities. Snapshots that are protected via SafeMode cannot be modified or permanently deleted from FlashBlade, making it easier for organizations to recover data quickly. SafeMode is a feature that can only be enabled by Pure Storage technical support at the customer's request and with an authorized representative working directly with Pure technical support. Organizations can also use SafeMode snapshots with third-party data protection solutions to enhance data protection and recovery processes.

ESG verified that Pure Storage SafeMode on FlashBlade can prevent data backups protected by a SafeMode snapshot from being modified, deleted, or encrypted by ransomware or other events. We also reviewed the integration of the solution with three industry-recognized data protection solutions and found it was quite easy to configure with all three protection schemas because it simply presents itself as a disk backup target, but with the benefit of SafeMode protection capabilities.

If you are currently looking to harden your data protection infrastructure and you want to add deeper protection against threats like ransomware or even attacks by rogue administrators or employees, ESG believes FlashBlade with SafeMode from Pure Storage is worth serious consideration.