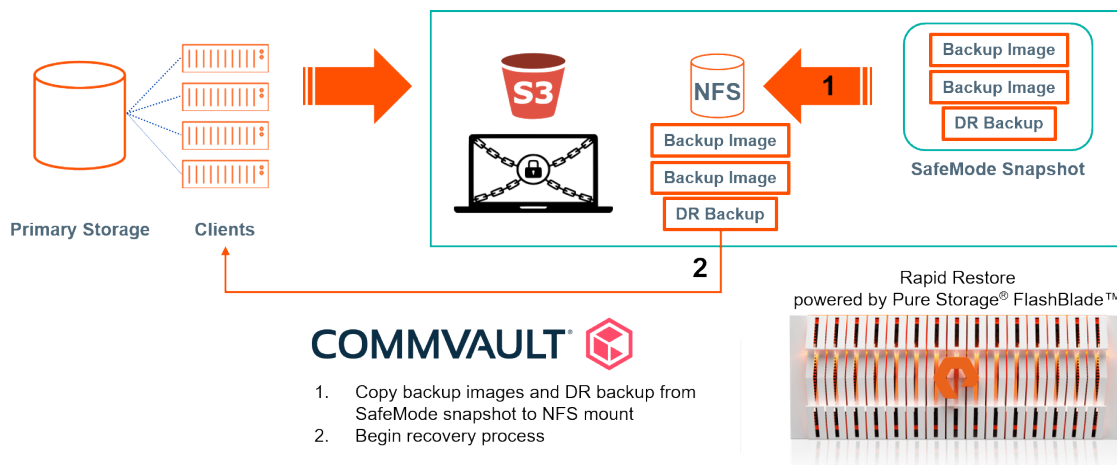# Achieve greater protection against ransomware with Commvault and Pure Storage

It seems that ransomware and cyber threats are at the top of everyone's minds. CTO's are wondering when their company will be hit by an attack and how much it will cost them when it does. Backup and storage administrators are worrying about their company data being compromised, their backup data being tampered with, and whether they'll be able – and how long it will take – to recover from an attack while still meeting their SLAs.

They, you, and everyone in between have good reason to be thinking about these things. According to IDC, security expenditures are expected to reach $151.2 billion worldwide annually by 2023.[1] And, despite the increase in awareness and spending, businesses like yours will still fall victim to ransomware attacks every 11 seconds in 2021.[2] These statistics reinforce the importance of data security as it relates to storage and recovery readiness. To address this, Commvault and Pure Storage have come together to monitor for, protect against, and rapidly recover from ransomware and other cyber attacks.

Commvault® Software includes several tools to protect and restore your data and applications, including **data isolation and air gapping**, **AAA Security Framework** for application hardening, and **environment monitoring** through anomaly detection and honeypot files. When used as the storage target for your Commvault backups, **Pure Storage® FlashBlade™** with SafeMode snapshots adds a layer of immutability and delivers fast recovery for your security strategy.

1. Copy backup images and DR backup from SafeMode snapshot to NFS mount
2. Begin recovery process

Rapid Restore powered by Pure Storage® FlashBlade™

Having a 3–2–1 backup strategy is a great starting point, where you have at least three copies of data, two of which are local but in different locations, and one copy offsite. Additional copies, layers, storage types, and diversification of the backup infrastructure alleviates having a single point of attack for "bad actors" to target.

Ransomware and cyber threats will never be 100% avoidable, but together, Commvault and Pure Storage make it more difficult for an attack to be successful.

1   New IDC Spending Guide Sees Solid Growth Ahead for Security Products and Services, October 2019
2   Global Ransomware Damage Costs Predicted to Reach $20 Billion (USD) By 2021, Cybersecurity Ventures, October 2019

Secure Snapshots from Pure Storage

Designating the Pure Storage FlashBlade with SafeMode as your backup target enables you to create immutable snapshots of Commvault backup data and associated metadata catalogs after you've performed a full backup. SafeMode offers the ability to prevent backups from being compromised by attackers by taking away the ability for the FlashBlade administrator to manage these snapshots. Even if a "bad actor" were to obtain the FlashBlade administrator credentials, they still could not delete, encrypt, manipulate, or reverse the immutability options applied to the backup data. This is because only an authorized designee from your organization would work directly with Pure Technical Support to configure the feature, modify the policy, or manually eradicate snapshots. This "separation of power" is the strength behind SafeMode and is what helps protect your data from not just ransomware attacks, but from compromised administrative accounts as well.

Better together

Commvault and Pure Storage have cooperatively tested the industry-leading security controls in Commvault Complete™ Backup & Recovery with the immutable storage integration of Pure Storage FlashBlade with SafeMode so you can rest assured we know how to protect and recover your data from a ransomware attack.
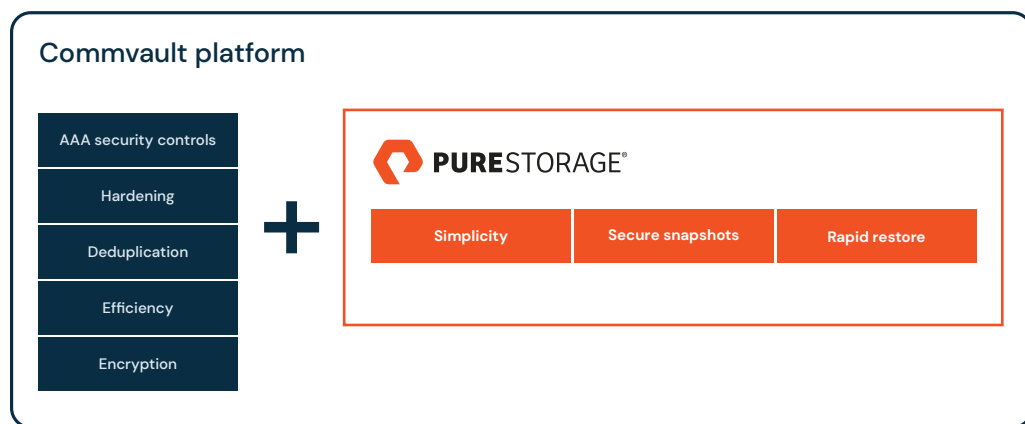
Commvault security controls and hardening

If a "bad actor" attempts to gain access to Commvault, the built-in AAA security controls and hardening capabilities act as a first line of defense, blocking the culprit from gaining access and deleting or encrypting data.

Deduplication

Commvault software deduplication begins where the source data resides. When FlashBlade is used for the target backup data, only changed blocks are transferred to the device, drastically reducing the amount of bandwidth required for copy operations. This also allows more backup cycles (Full, and Incremental backups) to be protected, while reducing the storage footprint. Ultimately, Commvault's deduplication allows backup copies to quickly be stored, reducing recovery point objectives, and increasing recovery readiness.

Efficiency

By using FlashBlade and Commvault Software together, organizations can leverage Commvault's storage accelerator capability. This allows large data volumes to be sent directly to FlashBlade, thus avoiding additional load on MediaAgents and speeding up the backup.

Encryption and key management

Storage encryption protects data at rest from being useful if stolen. However, this does not handle source-side encryption needs. Commvault's FIPS 140-2 certified encryption module handles encryption at the source, prior to sending data to the Pure Storage FlashBlade. This encrypts and secures every block of data transmitted to the storage device. For deeper levels of security, encryption keys can be offloaded to external key management servers.

Simplicity

The Pure Storage FlashBlade array scales non-disruptively, with multiple chassis forming a single backup domain. This eliminates the need to manage where data is placed and, more importantly, where to find it during a restore. The device serves as a backup target for Commvault, as well as for application-native backup processes.

Secure

As mentioned earlier, Pure Storage FlashBlade with SafeMode offers the ability to prevent backups stored on the device from being compromised by attackers, thus acting as a force multiplier on FlashBlade's existing simplicity and Rapid Restore capability. When SafeMode is activated, you can rapidly recover primary or backup data directly from these snapshots, helping guard data from 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. For further piece of mind, leverage **Commvault Activate™** to proactively scan your files and ensure your most critical data is protected and ready for recovery.

Rapid Restore

Ransomware attacks uniquely challenge backup systems to recover massive amounts of data in a very short amount of time. Rapid Restore powered by Pure Storage FlashBlade systems dramatically reduces the time spent restoring your Commvault-protected data, allowing you to still meet your recovery SLAs. A recent customer Proof of Concept (POC) test showed that FlashBlade was, on average, 61% faster than a competitive NAS-based device.[3]

Conclusion

While cyber threats are increasing, your organization can keep pace and mitigate risk. The combination of Commvault Complete Backup & Recovery and Pure Storage FlashBlade with SafeMode immutability reduces risk by providing an additional layer of protection. You can rest assured that your critical data will not be deleted, modified, or accessed by malicious cyber or internal threats, and that you are recovery ready.

---

3   Pure Storage POC done in April 2020, details available on request

---

Meet your data protection needs now and in the future with enterprise backup software. **Learn >**

commvault.com | 888.746.3849
get-info@commvault.com