SOLUTION BRIEF

Ransomware Mitigation from Pure Storage®

Mitigate ransomware attacks with SafeMode™ snapshots for Pure FlashBlade® and FlashArray™.

Ransomware attacks continue to be top of mind for business and IT leaders. And for good reason. They compromise access to your organization's lifeblood—your data. Consequences can be dire: Pay perpetrators to (maybe) unencrypt your data, stumble with decryption tools, or gamble on recovering from backups. With millions of dollars spent annually to guard entry points to data, many still underestimate the strategic value of augmenting data protection.

Your Existing Data Protection May Not Be Enough

Backups safeguard critical data against common scenarios such as recovering from natural or human-made disasters, data corruption, or accidental deletions. However, ransomware attacks can stress existing data protection infrastructures built on legacy architectures such as disk and tape more than expected.

If you're already struggling to meet recovery service-level agreements, a ransomware attack can compound the situation with additional downtime. Ransomware also compromises data and backup systems, which could require you to reinstall and reconfigure your backup solution before you can even contemplate data recovery.

Augment Data Protection with SafeMode Snapshots

With FlashBlade and FlashArray from Pure Storage, you can experience a new approach to mitigating and remediating ransomware attacks. SafeMode snapshots, a built-in feature of the Purity operating environment that powers FlashBlade and FlashArray, enables you to create read-only snapshots of backup data and associated metadata catalogs after you've performed a full backup with Commvault, Veeam, or Veritas data protection software.

Enterprise Threats

The number of organizations impacted by ransomware increased 102% between 2020 and 2021.[1]

Financial Exposure

All factors considered, the average ransomware recovery cost was $1.85 million in 2021, more than double the cost in 2020.[2]

Low Risk for Attackers

Anonymous cryptocurrency transactions enable extortion of huge ransoms as there's little chance of getting caught.[3]

SafeMode snapshots cannot be altered, encrypted, or deleted—whether it's unintentional, by a rogue employee, or through a hacker's programmatic approach. To manually access or eradicate snapshots, only authorized personnel in conjunction with Pure Support can delete or alter snapshots, providing a virtual air gap that is automated and simple to set up.

If your environment suffers an outage, whether from a ransomware attack or another type of disaster scenario, your authorized administrator will contact Pure Customer Support where access will be authenticated. Once verified, you can recover your SafeMode snapshots to get your data back online quickly and safely.

Pure Storage SafeMode Snapshot Benefits

You can recover data directly from snapshots, helping guard against attacks by ransomware, accidental deletions, or even rogue admins. SafeMode provides the following benefits:

- **Enhanced Protection:** Ransomware can't eradicate (delete), modify, or encrypt SafeMode snapshots.
- **Backup Integration:** 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 and easy to set up.
- **Rapid Restore:** Leverage a massively parallel architecture and elastic performance that scales with data to speed backup and recovery.
- **Investment Protection:** FlashBlade and FlashArray include SafeMode snapshots at no extra charge. Your Pure subscription or maintenance support contract covers enhancements.
- **Compatibility:** SafeMode seamlessly integrates with a variety of data protection solutions from Commvault, Rubrik, Veeam, and Veritas.

Additional Resources

- Learn more about SafeMode snapshots.
- Discover Pure Storage FlashBlade, FlashArray//C, and FlashArray//X.

[1] Check Point Research.

[2] "Ransomware Recovery Costs Near $2M," Dark Reading, April 2021.

[3] "How Bitcoin Has Fueled Ransomware Attacks," NPR, June 2021.

PS2100-01 07/2021