SOLUTION BRIEF

Protect against Ransomware with Pure

Increase data protection with Pure Storage® FlashBlade™ and SafeMode snapshots.

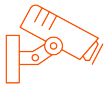
Ransomware attacks continue to be top of mind for business and IT leaders. And for good reason. They compromise access to your organization's lifeblood—data. Consequences can be dire: Pay perpetrators to (maybe) unencrypt your data, stumble with decryption tools, or gamble on recovering from backups. 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 man-made disasters, data corruption, or accidental deletions. However, ransomware attacks can stress existing data-protection infrastructure that may be built on legacy architectures, such as disk and tape, more than expected.

First, if you're already struggling with meeting recovery SLAs, a ransomware attack can exacerbate the situation with additional downtime. Second, your backup systems and data can be compromised, which could require you to reinstall and reconfigure your backup solution, before even contemplating data recovery.

You may think ransomware is "Windows-specific," with your backups impervious to attacks while hosted on Linux servers. But in 2019, a new family of ransomware called Lilocked (or Lilu) emerged and started targeting Linux servers and respective data.[4]

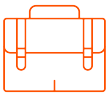


Enterprise Threats

Though overall attacks declined in 2018, enterprise attacks increased by 12%.[1]

Financial Exposure

NotPetya-related costs contributed to a $264 million quarterly loss at Maersk. [2]



Productivity Loss

Costs of downtime are 23 times greater than average ransom requested in 2018.[3]

[1] "Internet Security Threat Report, Volume 24," Symantec Corporation, February 2019.
[2] "NotPetya Ransomware Attack Cost Shipping Giant Maersk Over $200 Million," Forbes, August 2017.
[3] "A Look at Ransomware in 2019," Datto, October 2019.
[4] "Lilocked Ransomware Infects Thousands of Linux Servers to Encrypt Files," SecurityIntelligence, September 2019.

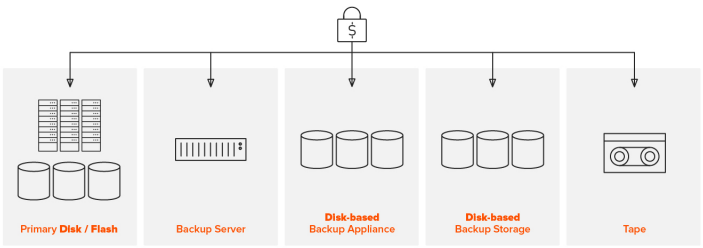


Figure 1: Ransomware attacks can compromise key elements of your data protection architecture.

Augment Data Protection with SafeMode Snapshots

At Pure Storage®, we acknowledge and share the concerns around ransomware. We're pleased to introduce a new approach to mitigating against these attacks when using Pure FlashBlade™ systems. SafeMode snapshots, a built-in FlashBlade feature, enable you to create read-only snapshots of backup data and associated metadata catalogs after you've performed a full backup. You can recover data directly from these snapshots, helping guard against attacks by ransomware and even rogue admins. FlashBlade provides the following benefits:

- **Enhanced protection:** Ransomware can't eradicate (delete), modify, or encrypt SafeMode snapshots. In addition, only an authorized designee from your organization can work directly with Pure Technical Support to configure the feature, modify policy, or manually eradicate snapshots.
- **Backup integration:** Utilize the same snapshot process regardless of backup product or native utility used to manage data protection processes.
- **Flexibility**: Snapshot cadence and eradication scheduling are customizable.
- **Rapid restore**: Leverage a massively parallel architecture and elastic performance that scales with data to speed backup and moreover recovery.
- **Investment protection:** FlashBlade includes SafeMode snapshots at no extra charge. Your Pure subscription or maintenance support contract cover enhancements.

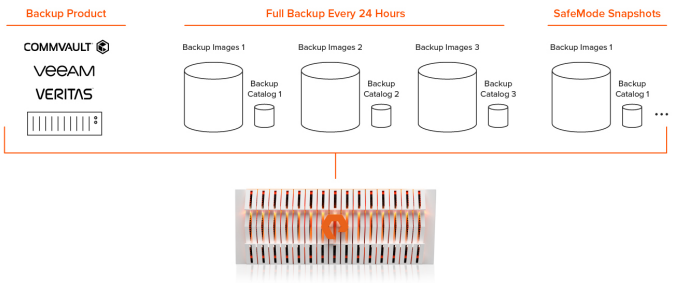


Figure 2: Day-to-day operations create read-only snapshots of backup images and metadata catalog.

Additional Resources

Learn more about SafeMode snapshots.

PS1030-01 11/2019