SOLUTION BRIEF

Ransomware Remediation for Pure FlashArray

Recover from malicious attacks faster with FlashArray™ SafeMode™.

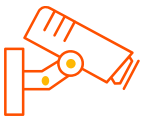
Ransomware attacks are reported in the news every day. These incidents affect industries worldwide. The risk to your business is growing at a phenomenal rate, with costs expected to reach $10.5 trillion globally by 2025[1]. The potential damage to your business extends beyond downtime and financial costs. Your reputation is at stake, even if an attack on your business doesn't make the news.

With FlashArray with SafeMode snapshots from Pure Storage®, lock down the critical data you need to recover from a cyberattack so that you can restart business services quickly, without succumbing to attacker demands.

Pure's approach to modern data protection isn't just an insurance policy. It's a vital component of the contemporary data center. Pure's solutions encompass multiple platforms and technologies, deliver efficient protection of critical data and applications with blazing fast restores, and let you derive real business value from your protected data. It's a continuum of protection technologies that span primary workload availability to snapshots and backup copies to long-term archives in the cloud.

Safeguard Recovery Data to Protect Your Business

Protecting against ransomware requires careful planning to outwit hackers, especially as attackers are increasingly moving toward targeted attacks. Ransomware attackers typically start by breaking into your systems up to weeks ahead of the attack to discover your vulnerabilities. Then, they launch an assault by encrypting your production data with their own key and demand payment for the key. At the same time, they encrypt or destroy any snapshots or backup data that you could use to restore your systems to their pre-attack, unencrypted state. SafeMode enables you to protect the critical snapshot and backup data you need to recover from such an attack in two ways. First, SafeMode prevents your recovery data from being corrupted or encrypted through an

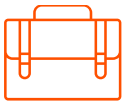


Enterprise Data Threats

Cyber criminals succeeded in encrypting data in 73% of ransomware attacks.[2]

Financial Exposure

IT services provider Cognizant anticipates a $50 million to $70 million loss after ransomware attack.[3]



Productivity Loss

A ransomware attack closed Baltimore County public schools for 115,000 students.[4]

always-on immutability capability. Second, it prevents recovery data from being entirely destroyed—even by someone with administrator privileges—through time-based eradication policies.

Speed Recovery with Immutable, Efficient Snapshots

Pure FlashArray offers an entire spectrum of business-continuity and disaster-recovery options—including snapshots, which provide fast recovery. A snapshot is a point-in-time image-level view of data that acts as a reference point for data protection and disaster recovery purposes. You can take snapshots of volume images, such as a database volume, for instant recovery. Or you can take snapshots of backup data and associated metadata catalogs to increase your level of data protection. All snapshots are immutable copies of data that a ransomware attacker cannot compromise, alter, or affect—even if your admin credentials become compromised.

Pure snapshots are available at no cost on all FlashArray devices and are simple to set up. Pure snapshots are:

- **Immutable to all:** Snapshots can't be modified or encrypted after they're created, not even by someone with admin access privileges.
- **Efficient:** Only the blocks that have changed since a previous snapshot are saved, speeding creation time and saving storage costs by not duplicating data.
- **Fully functional:** Snapshots are simply new volumes. You can mount, read, write, or snapshot them again, with the same performance as the original.
- **Flexible:** Recover any volume from any snapshot, instantly rolling forward or backward to restore business services.
- **Automatable:** Automate snapshot creation through end-to-end protection policies that give you the flexibility and confidence to operate worry-free.

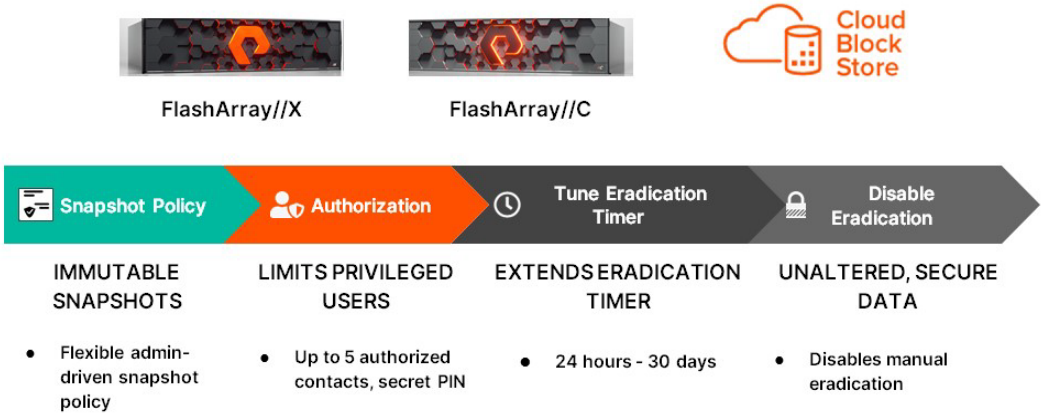


Figure 1. SafeMode protects your FlashArray snapshots from encryption and eradication during cyber-attacks.

Protect Snapshots from Eradication by Attackers

Attackers cannot encrypt or corrupt Pure's SafeMode snapshots, but they may attempt to eradicate (fully destroy) them from your system to prevent you from recovering data they've encrypted. To guard against this, FlashArray offers an eradication timer that will lock down data for a fixed period so that it can't be completely destroyed. The eradication timer disables eradication for everyone, including those with admin privileges.

The eradication timer is set to 24 hours by default. But with SafeMode enabled, you can increase it up to 30 days. This customizable timer gives you ample time to roll back your systems using immutable snapshots securely stored on your FlashArray, whether local or remote—and whether they're from a FlashArray//X, FlashArray//C, or Pure Cloud Block Store™.

Recover Quickly without Paying Ransom

As soon as you identify a ransomware attack and secure systems from unauthorized entry, you can begin recovery procedures. First, knowing that you have SafeMode-secured snapshots, you can eradicate any data the attacker encrypted or otherwise compromised. Then, you can instantly restore volumes from their SafeMode-secured snapshots. Your systems will be right back where they left off, without you needing to pay any ransom and with your organization's reputation intact.

Additional Resources

- Get more information about FlashArray data security and compliance.
- Learn about Ransomware protection for FlashBlade.

---

1 Cybercrime to Cost the World $10.5 Trillion Annually By 2025, Cybersecurity Ventures, November 2020

2 The State of Ransomware 2020, Sophos, May 2020

3 15 Malware and Virus Statistics, Trends and Facts, Safety Detectives

4 Ransomware Attack Closes Baltimore County Public Schools, New York Times, November 2020

PS2028-01 03/2021