

SOLUTION BRIEF

# Combating Ransomware in the Public Sector

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

Ransomware attacks continue to be top of mind for public sector IT leaders. And for a good reason. They compromise access to your organization’s lifeblood—its 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.

## Ransomware Attacks Are Rising Across the Public Sector

Ransomware attacks have been rising across public sector organizations, and the level of sophistication is increasing. Government agencies, educational institutions, and healthcare systems have been hit hard with ransomware attacks and there’s no end in sight. With virtually no industry spared, the question isn’t if you’ll be compromised—it’s when. Proper education and preparation can help you combat the threat. It’s not easy, but it’s a battle you can win.

Government	Educational Institutions	Healthcare
<p><b>Risks:</b> National security, public safety, delivery of essential services, and data loss</p> <p><b>Potential Impact:</b> Inability to access critical information, exposure and loss of sensitive data, financial and productivity loss, diminished citizen trust, and reputation damage</p>	<p><b>Risks:</b> Exposure/loss of student, personnel, and operational data; disruption of remote learning and operations</p> <p><b>Potential Impact:</b> Inability to access data, interrupted or halted learning or research, reputation damage, and financial and productivity loss</p>	<p><b>Risks:</b> Exposure and loss of critical patient, clinical, research, and other data</p> <p><b>Potential Impact:</b> Disruption of essential services and processes, negative impact on research, exposure and loss of critical data, financial and productivity loss, and trust and reputation damage</p>



### Enhanced Protection

With SafeMode snapshots, ransomware can’t delete, modify, or encrypt.



### Backup Integration

Use the same snapshot process regardless of backup product or native data protection utility.



### Flexibility

Snapshot cadence and eradication scheduling are customizable.



### Rapid Restore

Leverage a massively parallel architecture and elastic performance that scale with data to speed backup and recovery.

## Your Existing Data Protection May Not Be Enough

Backups safeguard critical data against common scenarios such as natural or human-created disasters, data corruption, or accidental deletions. Ransomware attacks can stress existing data protection infrastructure built on legacy architectures, such as disk and tape, more than expected. First, if you're already struggling to meet recovery SLAs, a ransomware attack can exacerbate the situation with additional downtime. Second, an attack can compromise your backup systems and data, requiring you to reinstall and reconfigure your [backup solution](#), before even contemplating data recovery.

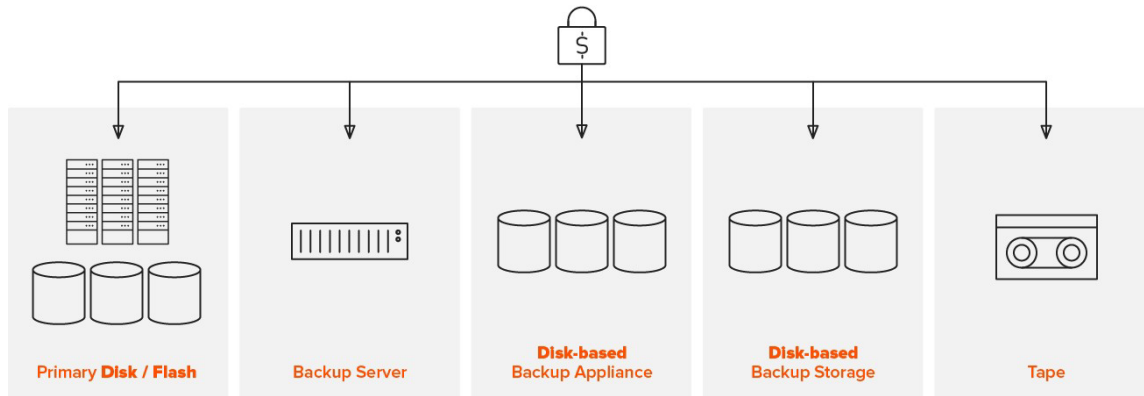


Figure 1. Ransomware attacks can compromise key elements of your data protection architecture.

## Augment Data Protection with SafeMode Snapshots

Pure has introduced an approach to mitigate against ransomware attacks when using Pure [FlashBlade®](#) or [FlashArray™](#) systems. SafeMode snapshots, a built-in feature of the Purity operating environment, enables you to create read-only snapshots of backup data and associated metadata catalogs after a full backup. Recover data directly from snapshots, helping guard against attacks by ransomware and even rogue admins. Pure all-flash storage solutions provide the following benefits:

- **Enhanced Protection:** Ransomware can't 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 the backup product or native utility used to manage data protection processes.
- **Flexibility:** Snapshot cadence and eradication scheduling are customizable.
- **Rapid Restore:** FlashBlade lets you leverage a massively parallel architecture and elastic performance that scales with data to speed backup and recovery at scale. Pure FlashBlade provides near-instant restore capabilities of 1PB+ per day.
- **Investment Protection:** FlashBlade includes SafeMode snapshots at no extra charge. Your Pure subscription or maintenance support contract cover enhancements.

## Combating Ransomware in the Public Sector

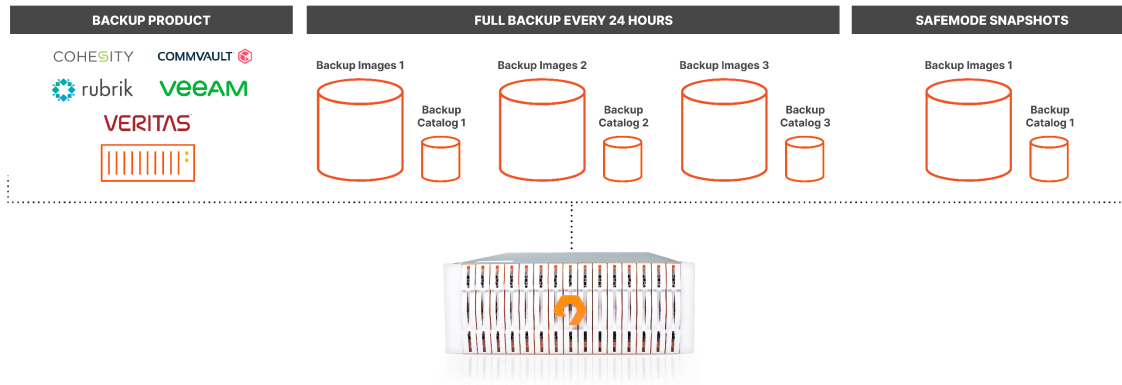


Figure 2. Day-to-day operations create read-only snapshots of backup images and metadata catalog.

### SafeMode Can Save the Day

When it comes to ransomware, don't assume that backup equals protection. Recovering successfully from a ransomware attack requires not only secure backups but a fast recovery platform. Every minute your applications aren't available costs your organization.

With SafeMode, data backup recovery is smart, fast, and easy. The "set it and forget it" policy automates snapshot creation and expiration. SafeMode enables rapid, high-capacity recovery with all-flash storage. And it's future-proofed. All features and enhancements are included at no charge. Stay safe with SafeMode and keep your data backups secure and your ransomware attacks at bay.

### Additional Resources

- Learn how to be [resilient](#) after a ransomware attack.
- Get the ransomware survival kit for [federal](#) and [state and local](#) governments and [education](#) institutions.
- Read the [Hacker's Guide](#) to Ransomware Mitigation and Recovery.
- Learn how to secure backups against ransomware with Pure Storage [SafeMode](#) Snapshots.

[purestorage.com](https://purestorage.com)

800.379.PURE

