10 FAQs for Pure Storage SafeMode for Epic

As your healthcare organization scales, so does your responsibility to protect your customers' clinical data from ransomware attackers. While there's a role technology can play, the human element has been left out of many offerings for ransomware mitigation—until now.

If you're currently using an Epic ecosystem, here are 10 things to know about leveraging Pure Storage® SafeMode™ and how it can play an important role in the protection of clinical data for Epic.

How SafeMode Solves the Human Element in Data

Protection

SafeMode is a data protection solution that is built into the Pure Storage Platform in FlashArray™ and FlashBlade® systems. The combination of immutable snapshots and SafeMode gives Epic customers using Pure Storage products a higher level of data protection from data destruction, ransomware attack, or user error. In these scenarios, SafeMode disables the default eradication policy built into the array's capacity reclamation process. This means that backups can't be deleted (accidentally or deliberately) by anyone unless they've been authorized by Pure.

How does SafeMode for Epic work?

By disabling the usual 24-hour window of time, storage volumes dropped in the "Destroyed" storage container cannot be removed or eradicated from the array. If there's an attempt to do a forced eradication, an alert in the Purity UI will indicate that eradication is not available.

Changes to SafeMode are only possible when at least two authorized contacts from your organization conference with the Pure Storage Support team. You can authorize up to five contacts, each of whom will get a unique six-digit PIN. To request this, simply call Pure Support and they'll set up a conference call with you and your account team.

10 Common Questions for SafeMode with Epic

1. Does Epic recommend the use of SafeMode for Pure Epic customers? Does SafeMode work with Epic storage volumes?

Yes and yes. Pure has briefed Epic's technical support team on the use of SafeMode with a positive response from Epic related to protecting Epic customers

as part of an overall malicious attack mitigation strategy.

Pure FlashArray and/or FlashBlade volumes do not recognize if the data is related to Epic or any other application. SafeMode protects all storage volumes using the same approach. Volumes used to offer databases the ability to read and write data have no awareness of the database engine the volumes are designated for. That said, Intersystems IRIS, Oracle, SQL Server, Mongo, Splunk, and many others can benefit from the protection provided by Pure and SafeMode.

2. Does SafeMode work with Epic-approved host operating systems and databases?

Yes. Epic currently supports both IBM AIX and Linux RHEL operating systems for the operational database (ODB) servers and Windows Server for the services and presentation tiers of Epic. Since SafeMode is an array-based feature, host operating systems are not impacted using SafeMode. Contact your local Pure SE and your Epic Server System liaison for the latest OS supportability matrix.

3. Is there a cost to use SafeMode? How do I enable SafeMode for my Epic environment?

There is no cost for Pure customers with active support contracts, just like all the other features available to Pure customers running Epic.

To enable SafeMode, work with your local AE/SE team and Pure Support to begin the registration process. They'll help you generate a unique six-digit PIN for each trusted individual—as few as two, or as many as five. Support will also make the necessary changes to the array's Purity settings to enable SafeMode. Once it's enabled, the entire array is protected by SafeMode.

Selecting trusted users should be done carefully. You may want to consider having authorized users outside of the storage administration team, such as organizational leadership or a security/compliance officer.

Important: If a SafeMode authorized contact changes roles or leaves the

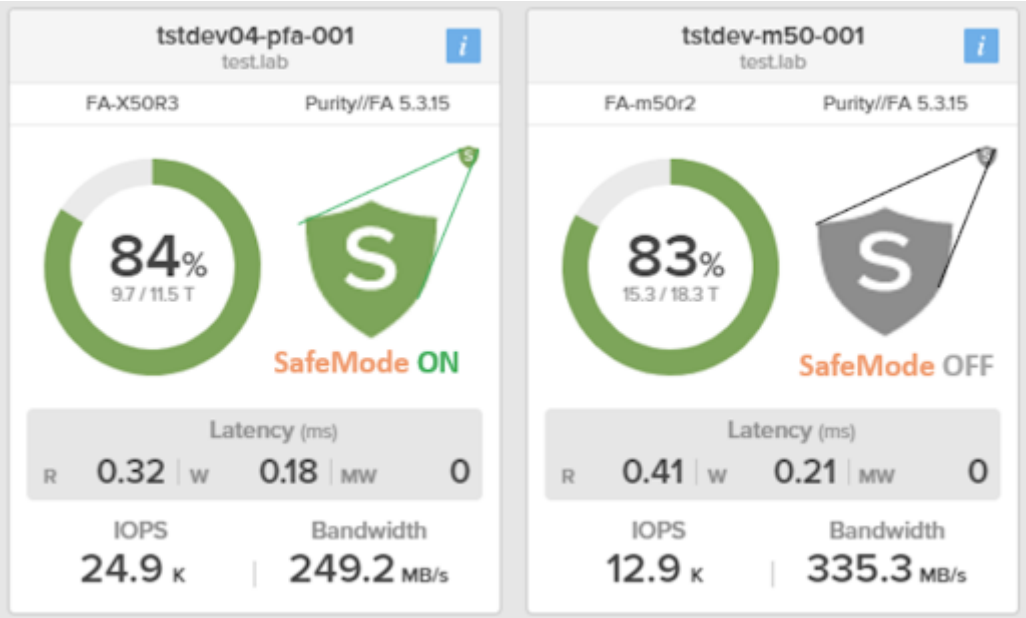
organization, be sure to contact Pure Support right away to update your SafeMode authorized contacts.

4. How does the use of SafeMode impact Epic's freeze and thaw operations for backups and/or refresh processes?

If you use scripts that call Epic's delivered instfreeze and instthaw scripts as part of either backup snapshots or environment refresh scripting, SafeMode itself does not change the workflow in any way. If you're using the "purepgroup eradicate" CLI call in the event, you'll need to physically remove a utility volume(s) of data, and SafeMode will return a result that states "Eradication is DISABLED." If you're using this, contact your local team as well as the Pure Professional Services team to understand how to account for this change in how volumes are managed under programmatically controlled scripts or REST API interaction.

5. How can I identify if my array has SafeMode enabled or disabled?

The Pure1 management portal for your fleet of arrays has a new identifier that is now part of the array's Appliances view. You'll see a new icon below the Purity version indicator that appears as a shield with an "S" in the middle. When SafeMode is enabled, this new icon will be green to indicate that SafeMode is on. When an array is not running SafeMode, the icon will be gray to indicate that SafeMode is off. Below is an example of how this looks in the Pure1 portal.



6. Is it possible to allow the array to eradicate certain utility volumes automatically with SafeMode enabled? How?

During the initial activation of SafeMode with Pure Support, you can define an eradication window greater than the default 24-hour policy. The eradication window you select should provide enough time so that if a ransomware event is suspected, the array will protect the volumes(s) while you and the Pure Support team investigate the incident to determine what actions are needed. A good rule of thumb is seven days, but it can be as many as 30 days.

Important: This setting has an impact on arrays where available space may be limited due to consumption. Because of this, it's important to consider how long space can be consumed while awaiting the SafeMode eradication policy to expire. For Epic customers, both Epic and Pure feel that seven days should be adequate, but it's important to discuss this with your storage and DBA teams to identify the proper number. If an array is 80% full or more, it's critical to discuss a capacity upgrade before turning on SafeMode.

7. Pure works with the industry's leading backup and recovery partners to deliver best-in-class data protection. How does SafeMode interact with their software?

In most cases, the third-party backup tool provider will leverage the Purity REST API to interact with SafeMode. That said, every third-party backup independent software vendor (ISV) may interact differently with SafeMode. For this reason, it's important to reach out to the Pure Support team to determine which ISVs are collaborating with SafeMode and how it's being done.

Learn more about Pure's backup and recovery partners >>

8. With SafeMode enabled, can I still use Pure protection groups as a logical container for all volumes related to an Epic instance?

Yes. Protection Groups allow all the Epic-specific volumes to be managed as a single logical container versus volume-by-volume. It's critical to include Journals along with the database volumes. The InterSystems IRIS database journals or WIJ volumes should be included along with any app volumes. This is a key item to ensure in a situation of recovery so all the data volumes related to a specific instance are returned to the state in which the snapshot was taken. This is a general requirement by Epic and a Pure best practice.

9. If I believe I'm the victim of a ransomware attack or an accidental erasure, what are my next steps?

Immediately report the situation to your internal trusted SafeMode contacts, Pure Support, and your Epic Server Systems team liaison. Your local Pure account team

should also be notified to ensure there's full transparency of the event at all levels.

Once that process has started, Pure and Epic can collaborate on the best way to recover the data back to an operational state. Epic may request time to do some data integrity forensics to determine if any records were lost or if the database is in an unhealthy state of operations. This could take some time based on the severity of the situation. You may also consider mobilizing certain key application stakeholders that represent certain clinical application functions. An application that's the scale of Epic requires the actions of a team of application liaisons who are acquainted with the various clinical and business units to make sure full functionality is assessed and confirmed.

Learn more about how Pure can help you before, during, and after a ransomware attack or data loss scenario >>

10 Are there any services that can be used to assess readiness for implementing SafeMode?

Yes. The Pure Professional Services team has a SafeMode Advisory Workshop that can help you find answers to the key questions and data points to ensure your SafeMode configuration meets your needs. This is a paid engagement that ensures all the necessary capabilities and workflow questions are addressed. To learn more, read the SafeMode Advisory Workshop Service Brief.

Related links:

See how to enable SafeMode and SafeMode best practices (Pure1 login required)

Pure SafeMode Advisory Workshop blog post

Read more about SafeMode