TECHNICAL BRIEF

Ransomware Remediation with FlashArray SafeMode

Utilize FlashArray™ SafeMode™ snapshots from Pure Storage® to safeguard your data.

Ransomware (when an intruder covertly encrypts your files and demands payment to decrypt or unlock them) can be disastrous for organizations. The loss of your data and monetary impact aren't the only concerns; in many cases, an attack results in a complete shutdown of the company's operations for days and being in the public spotlight for the wrong reasons. Your business reputation and brand value can be damaged as well. In a 2020 ransomware attack on Garmin, the downtime lasted nearly five days and though the ransom amount is not known, it is estimated to be around 10 million dollars.

What is Ransomware?

In the first half of 2020, the number of global ransomware reports increased by 715% year-over-year, according to the latest Threat Landscape Report 2020 by Bitdefender. With more people working remotely and a shifted business environment due to the global pandemic, cybercriminals have capitalized on the opportunity.

Ransomware affects all industries, from tech, insurance, oil, and gas to higher education. In 2019, over 500 schools were hit by ransomware. Ransomware software is big business, and the victims are increasingly larger, having to pay exorbitant sums to get back to business as usual.

What many people do not know is that ransomware attack software is as readily available as commercial software. It can be downloaded and purchased easily, often with a portion of any attack winnings going to the developer. Attackers don't have to be particularly knowledgeable or skilled. They can be disgruntled minimally skilled employees with access to critical infrastructure. With a quick download from the dark web, they can launch a ransomware attack before their employee accounts are locked down.

Safeguard

Protect your data from malicious ransomware attacks, reputation damage, and costly ransom demands.

Protection

No matter who attacks you, data can only be deleted in conjunction with Pure Support.

Simple

SafeMode takes only three simple steps to set up and is free to turn on.

How SafeMode Protects Critical Data

Let's look at two examples of a potential attack, assuming an attacker has gained admin rights to a FlashArray.

1. **The attacker encrypts volumes and eradicates the originals:** In this scenario, the original volumes are destroyed. When a volume is "destroyed" it sits in a special area of the FlashArray where it is removed from the volume inventory, but still exists in an eradication bucket. The eradication bucket defaults to a 24-hour timer where objects can be recovered or permanently eradicated. If the attacker has also eradicated the volumes then all volume data is gone, and you are now subject to the attackers' demands. To be clear, with SafeMode enabled, the attacker cannot remove the volume data from the eradication bucket, even with admin privileges. In our example here, the attacker can eradicate volumes because SafeMode is not enabled.
2. **The attacker encrypts volumes and eradicates all snapshots in addition to the volumes:** In this case, there are recovery points to go back to in the form of snapshots. However, the attacker has destroyed and eradicated them so there is nothing to restore from. This was possible because, as with Example 1, the attacker eradicated snapshots due to SafeMode not being enabled.

In either scenario, enabling SafeMode prevents the eradication of any volume or snapshot during the configured eradication timer length. If the eradication timer is set to 14 days, the recovery data you need to restore critical services will be completely protected for two weeks. Not only does SafeMode prevent even the most privileged of user accounts from eradicating volumes and snapshots, but FlashArray snapshots are immutable (unchangeable). Leveraging SafeMode with snapshots will always allow a guaranteed recovery point after an attack.

How to Recover from a Ransomware Attack

Revisiting our examples, if SafeMode was enabled in Example #1 you would be able to eradicate the attacker's encrypted volumes, and then restore your volumes—instantly—and be right back to a state before the volumes were encrypted.

In Example #2, the process is the same. You could eradicate the attacker's encrypted volumes but restore them from snapshots. Because the attacker could not eradicate the snapshots, they remained available for recovery. For both examples, it would be critically important to investigate the attack vector and take action to prevent a recurrence.

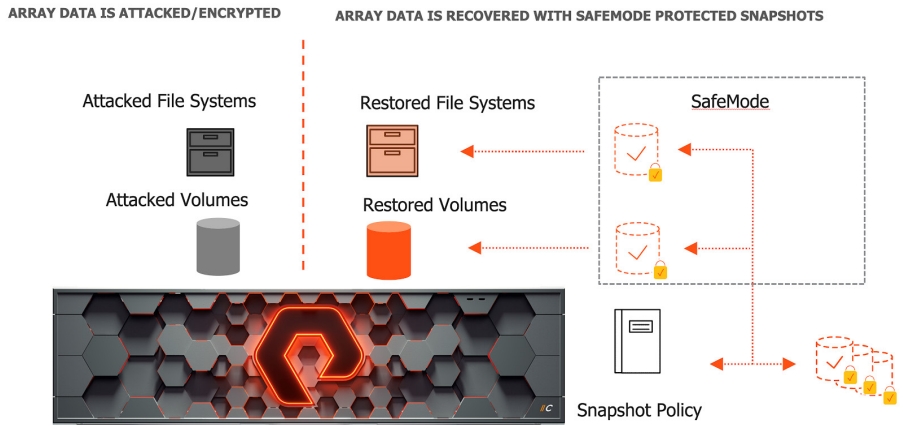

Figure 1. Attacked/encrypted volumes are easily replaced with snapshots from an earlier point in time.

SafeMode Configuration

SafeMode itself is easy to configure. Call Pure Support to request SafeMode be enabled and provide additional (up to five) contacts that are authorized to request SafeMode changes. Support will issue a six-digit PIN for each authorized user to be used for any future changes. SafeMode itself is either on or off; however, the eradication timer is configurable. Most of our customers settle on 14 days but the timer can be extended up to 30 days.

It is imperative to create a snapshot policy for SafeMode to protect your data. This is performed through FlashArray Protection Groups, where hosts, volumes, volume groups, files, and directories can all be automatically snapped on any regular basis. Snapshot retention and frequency are customizable. Even a third device, a "target," can be added for sending snapshots to another FlashArray, cloud service, or FlashBlade®.

If you need to recover FlashArray space, which can happen for example after data migrations to an array, you will need to conference call Pure Storage Support, with two authorized contacts and their assigned PINs to allow for permanent eradication of any items. However, this process is not necessary for the instant recovery of objects that are still pending eradication.

Conclusion

SafeMode is an easy, no-extra-cost feature that prevents permanent loss of data due to admin mistakes or malicious ransomware attacks. It works by simply preventing the eradication of objects for a configured time frame. In the event of an attack, instead of suffering painful and very public downtime only to wind up paying a ransom, you simply remove the attacker's encrypted data and instantly restore your data from a prior point in time.

To enable it all you need to do is call support, establish your contacts, and set the timer length. Those three steps will give you a simple, pro-active victory before potential disaster strikes.

PS2024-01 03/2021