1 + 1 = 3
Pure Storage + Veeam
Better Together

Solution
Brief

Protect against ransomware with Pure & Veeam

Augment Veeam Software 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 as the threats become more frequent and complex. If you don't properly prepare, you may be forced to pay perpetrators to (maybe) unencrypt your data.

With millions of dollars spent annually to guard entry points to data and human error being the leading cause of malware attacks, many still underestimate the strategic value of a well-designed backup and recovery strategy.

The Veeam and Pure best practice solution for protecting against ransomware

Organizations can prepare themselves for a threat incident by adopting common best practices for data protection, including a 3-2-1 methodology and performing risk assessments. The 3-2-1 principle is to have **THREE** copies of your data on **TWO** different types of media with **ONE** copy being off site. In addition, the backup environment should be "air gapped," meaning it is offline or unwritable to prevent threats targeting the backup data sets. Performing regular risk assessments also should be part of your overall data protection strategy to proactively identify potential risks. As part of the risk assessment, you need to be able to verify that data is recoverable and that it can be restored quickly and easily.

Veeam ransomware best practice solution

While Veeam® doesn't prevent ransomware, the Veeam solution for ransomware following the 3-2-1 Rule of data protection, along with advanced features native to Veeam Availability Suite™, enables companies to quickly and effectively restore critical data infected by ransomware to a known good state:

Three copies of data: In addition to the primary or production data, there should be a backup copy of the data and also a copy of the backup data. Ideally, these would be stored on different physical devices.

Two types of media: It is imperative to use multiple forms of media to avoid drives in the same data center from being corrupted. Veeam natively supports backup to a variety of media types, including disk, tape, backup appliances and the cloud.

A recent report from cyber-security firm Malwarebytes found a 363% increase in ransomware detections against businesses from 2018 to 2019.

Researchers from CrowdStrike say there's been a rise in "big-game hunting," attacks that target large organizations that are "especially sensitive to downtime".

> "We chose Veeam for ease of use and reliable recovery. When the CryptoLocker virus hit, Veeam couldn't have been easier to use or more reliable… Veeam assures us our data will be available when we need it."
>
> Bob Eadie, IT System Manager,
> Bedford School

Read the case study

One off-site copy: Veeam's advanced backup and replication capabilities make it easy to have image-based replication and backup copies in a second location that is off site, on tape or in the cloud with Veeam Cloud Connect. Veeam offers WAN Acceleration and encryption to provide fast and secure replications and backup copies.

Risk assessment: Included in Veeam Availability Suite is Veeam ONE™, a powerful monitoring, reporting and capacity planning tool for the Veeam backup infrastructure. It comes with off-the-shelf reporting that performs a backup assessment to assure you are protected and has a built-in alert to warn of potential ransomware activity.

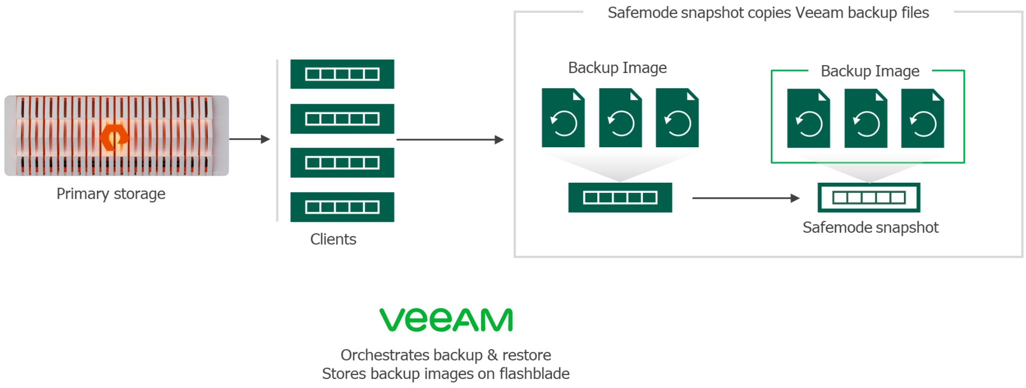
Your existing data protection may not be enough

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. First, if you're already struggling with meeting recovery SLAs, a ransomware attack can exacerbate the situation with additional downtime. Second, if you don't air gap your backup systems, the data can be compromised, which could require you to reinstall and reconfigure your backup solution before even contemplating data recovery.

Augment data protection with SafeMode snapshots

Creating an air gap for your backup environment can help safeguard against ransomware attacks on your backup data set. Pure Storage also offers an additional level of protection with a new approach to mitigating 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.
- **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 covers enhancements.


Safemode snapshot copies Veeam backup files
Backup Image
Backup Image
Primary storage
Clients
Safemode snapshot
Veeam
Orchestrates backup & restore
Stores backup images on flashblade

How Veeam & Pure can help you recover from ransomware

Rapid restores from ransomware attacks through fast VM and granular recovery override the encrypted ransomware database, applications, files and operating systems.

Rapid recovery and uninterrupted application performance with tight integration with Pure Storage All Flash arrays allow you to make frequent backups without impacting production systems. Further, with SafeSnap, you can create immutable backup data sets that cannot be modified or encrypted.

Test and discover recovery points to quickly and easily discover the last good restore point using Veeam DataLabs™.

Summary

Best practice solutions from Pure and Veeam enable organizations to rapidly recover from ransomware while providing an enterprise-class data availability solution for day-to-day operations.

Learn more

www.veeam.com/purestorage-flash-solutions.html

PURESTORAGE®