



Solution Brief:


Countering ransomware with Veeam + Lenovo

The challenge

Ransomware attacks represent a serious threat to organizations across multiple industries worldwide. A new organization fell victim to ransomware every 14 seconds in 2019 and will fall victim every 11 seconds in 2021 according to Cyber Security Ventures. Ransomware cost has risen into the tens of billions of dollars per year, with prices continuing to grow for the foreseeable future. These costs include the cost to remediate attacks, cost of downtime and the actual ransom cost. While health care organizations have been the most publicized victims, this is a growing threat across all industries and governments.

Even though ransomware has been around since 1989, there's been a recent surge in attacks. The average cost of data breaches entered the hundreds of millions of dollars in 2020 according to Juniper Research. With damage related to cybercrime set to hit \$6 trillion by 2021, investing in security spending should be a priority for 2019 according to PhoenixNAP Global IT Services. Some common encryption ransomware programs include CryptoWall, Locky and TorrentLocker, which encrypt data on the attacked system and demand ransom in exchange for the key to unlock it. Some common lock screen ransomwares are FakeBsod and Brolo, which lock screens and demand payment to unlock them.

These threats are becoming more frequent and complex. So, organizations should ensure that they adopt common best practices for data protection, like the 3-2-1 Rule. This means having three copies of your data on two different types of media with one copy offsite. In addition, performing regular risk assessments should be part of your overall data protection strategy to proactively identify potential risks as well as verify that your data is recoverable and can be restored quickly and easily.

- 
- 24/7 operations
 - No patience for downtime and data loss
 - Growing amount of data

The solution

While Veeam® doesn't prevent ransomware, Veeam's solution for ransomware includes advanced features that are native to Veeam Availability Suite™. This enables companies to quickly and effectively restore critical data infected by ransomware to a known state.

In addition to primary or production data, you should have a backup copy of your data, and you should back up that backup of your data as well. Ideally, these would be stored on different physical devices. It is imperative to use multiple forms of media to prevent ransomware from corrupting multiple drives in the same datacenter. Veeam natively supports backup to a variety of media types including disk, tape, backup appliances and the cloud.

Every 14 seconds

a new organization falls victim to ransomware

Ransomware costs businesses more than **\$75B** a year

Businesses lose approx. **\$8,500/hour** due to ransomware-induced downtime

Ransomware has grown **56%** over the past year

Total cost of ransomware expected to hit **\$6T** by 2021

Source: comparitech.com/antivirus/ransomware-statistics/



One offsite copy: Veeam's advanced backup and replication capabilities make it easy to have offsite, image-based replication and backup copies sent to a second location whether that be on-premises or in the cloud with the help of Veeam Cloud Connect. This means Veeam Cloud Connect can store a backup copy offsite, to tape or in the cloud. Veeam also 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 that ensures you are protected, plus a built-in alert that warns users of potential ransomware activity.



Safeguard your backup infrastructure: Veeam allows you to carefully restrict access to backup repositories and provides you with the ability to keep backup data offline.

How Veeam and Lenovo can help you recover from ransomware

- **Data stays safe, ransomware stays out:** 100% of ransomware-proof backups with hardened Linux repository on Lenovo ThinkSystem DE Series storage systems.
- **Reducing complexity:** Veeam® reduces overall complexity to create powerful yet simple immutable data protection against ransomware and insider threats.
- **Rapid restores from ransomware attacks** through fast VM and granular recovery that overrides encrypted ransomware databases, applications, files and operating systems.
- **Rapid recovery and uninterrupted application performance** with tight integration with Lenovo ThinkSystem industry-leading storage, server and hyperconverged infrastructures.
- **Test and discovery recovery points** to efficiently find your most recent clean restore point with Veeam DataLabs™ and/or Veeam On-Demand Sandbox™

Diagram 1 shows how Veeam Availability Suite provides a turnkey solution that helps users recover from ransomware. There's no additional software to buy with the most modern storage, server and hyperconverged infrastructure from Lenovo ThinkSystem or ThinkAgile technology solutions.

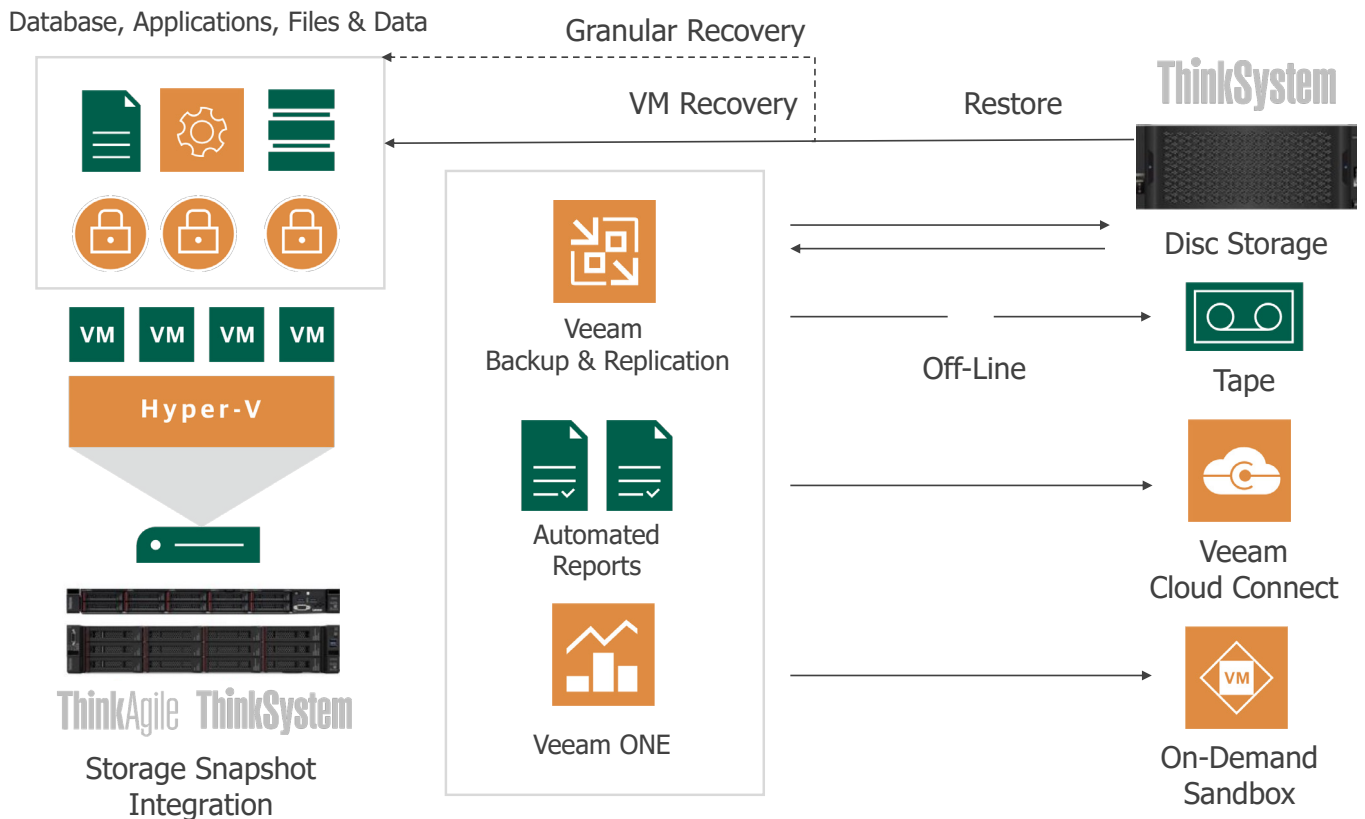


Diagram 1: Veeam operational diagram with Lenovo infrastructure integration



Learn more
vee.am/lenovo



Download free trial
vee.am/availabilitysuite