Lenovo VEEAM

1+1=3 Lenovo + Veeam Better Together

Solution Brief

Countering Ransomware with Veeam and Lenovo

24/7 operations

No patience for downtime and data loss

Growing amount of data

The Challenge

Ransomware attacks represent a serious threat to organizations across a number of industries worldwide. A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021 according to Cyber Security Ventures. Ransomware's costs has risen into the tens of billions of dollars a year, with it continuing to grow for the foreseeable future. These costs include the costs to remediate attacks, the cost of downtime to an organization, and the actual ransom cost. While attacks on health care organizations have been the most frequently publicized, this is a growing threat across all industries and governments. The threats are becoming more frequent and complex. Recent news reports on attacks on local government offices in the USA highlight the proliferation of these attacks.

While ransomware has been around since 1989, there was a surge in ransomware attacks. The average costs of data breaches will reach into the hundreds of millions of dollars by 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 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 ransomware are FakeBsod & Brolo which lock screens demanding payment to unlock them.

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: https://www.comparitech.com/antivirus/ransomware-statistics/

Countering the Ransomware threat:

Organizations should assure that they adopt common best practices for data protection. For example, have three copies of your data on two different types of media with one copy being 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 data is recoverable and that it can be restored quickly and easily.

In addition to the primary or production data, there should be a backup copy of the data and a copy of the backup data. Ideally, these would be stored on different physical devices. It is imperative to use multiple forms of media to prevent ransomware 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.

One off-site copy: Veeam's advanced backup and replication capabilities make it easy to have off-site, image-based replication and backup copies to a second location being offsite, tape or the cloud with Veeam Cloud connect. With Veeam Cloud Connect it can

store a backup copy off site, to tape or in the cloud. Veeam offers WAN acceleration and encryption to provide fast and secure replications and backup copies.

Risk assessment: Included in the 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.

Safeguard the Backup Infrastructure: Veeam allows you to carefully restrict access to the backup repository and provides the ability to keep the backup data offline.

How Veeam and Lenovo Can Help Recover from Ransomware

While Veeam® doesn't prevent ransomware; the Veeam solution for ransomware with advanced features native to the Veeam Availability Suite™ integrated with Lenovo ThinkSystem servers and storage enables companies to quickly and effectively restore critical data infected by ransomware to a known good state.

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

Rapid recovery and uninterrupted application performance with tight integration with Lenovo ThinkSystem industry-leading storage, server, and hyperconverged infrastructure.

Test and discovery recovery points to quickly and easily discover the last clean restore point using Veeam DataLabs/ On-Demand Sandbox

Diagram 1 *shows how Veeam Availability Suite provides a turnkey solution to recover from ransomware. No additional software to buy, with the most modern storage and server, and hyperconverged infrastructure from Lenovo ThinkSystem or ThinkAgile technology solutions.*

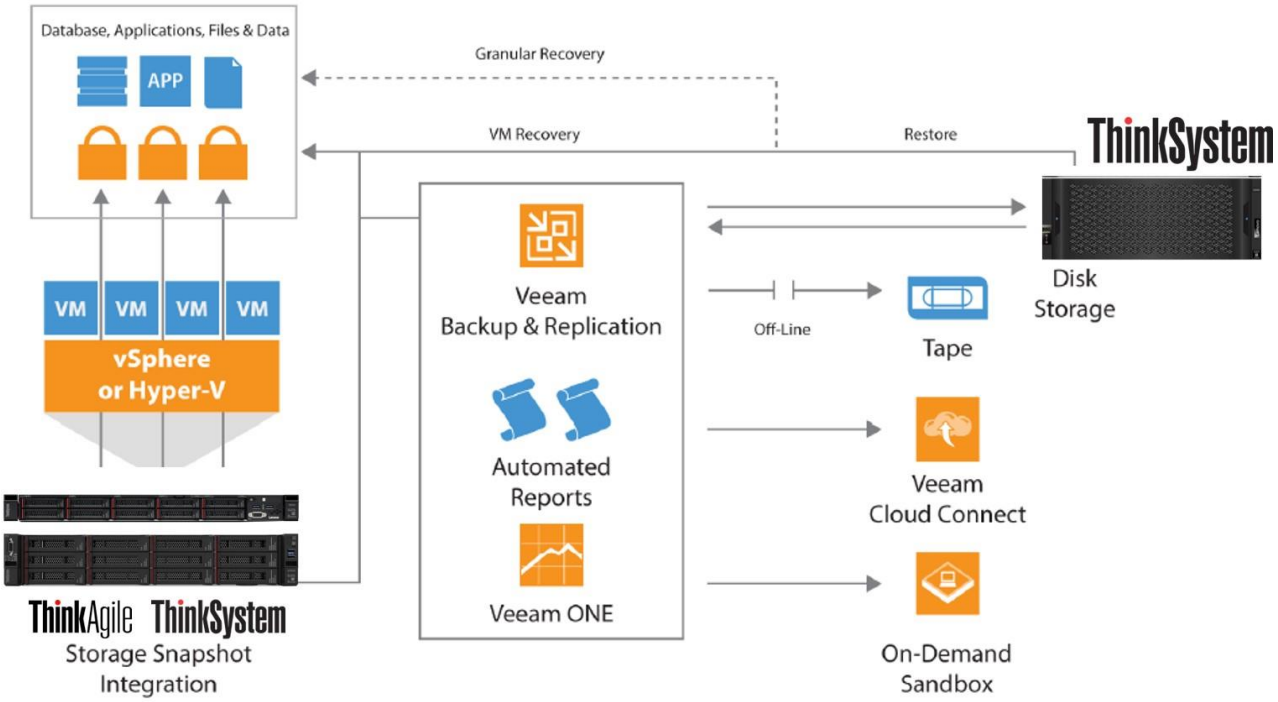

Diagram 1: Veeam operational diagram w/ Lenovo infrastructure integration

About Veeam

With the growth and sprawl of today's data, traditional data management is not enough. As the leader in Availability across cloud environments, Veeam® is uniquely positioned to help customers along their journey to Intelligent Data Management. Veeam is the global leader in Intelligent Data Management. Veeam Availability Platform is the most complete solution to help customers on the journey to automating data management and ensuring the availability of data. We have more than 330,000 customers worldwide, including 75 percent of the Fortune 500 and 58 percent of the Global 2000. For more information, go to: https://www.veeam.com/lenovo-storage-solution.html

About Lenovo

Lenovo (HKSE: 992) (ADR: LNVGY) is a US$45 billion Fortune Global 500 company and a global technology leader in driving Intelligent Transformation through smart devices and infrastructure that create the best user experience. Visit our website at http://www.lenovo.com/.