The Veeam Best Practice Solution for Countering Ransomware

Addressing ransomware attacks

Ransomware attacks represent a serious threat to organizations across a number of industries worldwide. According to the F.B.I., ransomware attacks collected $209 million in the first three months of 2016 and they are on pace to reach $1 billion in 2016. That doesn't include the costs to remediate attacks, nor does it include unreported attacks. While health care organizations have been the most publicized, this is a growing threat across all industries.

While ransomware has been around since 1989, there was a surge in ransomware attacks in 2013 with the Trojan CryptoLocker and its use of bitcoin which is a digital currency that facilitates anonymous payments. There are two basic types of ransomware, lock screen and encryption. 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.

The threats are becoming more frequent and complex. Organizations should assure that they adopt common best practices for data protection including adopting a 3-2-1 methodology and performing risk assessments. The 3-2-1 principle is; 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 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 the 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 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.

> "We chose Veeam for ease of use and reliable recovery. In 2014, the CryptoLocker virus hit, and 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

91% of those attacked had data encrypted and 95% were able to restore without paying*

* Veeam Customer Survey
Sept 2016

- **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 Can Help Recover from Ransomware:

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

- **Rapid recovery & uninterrupted application performance** with tight integration with industry leading storage vendors like Hewlett Packard Enterprise (HPE), Dell EMC, NetApp, Nimble, and soon, IBM.

- **Test and discover recovery points** to quickly and easily discover last good restore point using Veeam On-Demand Sandbox.

Diagram 1 shows how Veeam Availability Suite provides a turnkey solution to recover from ransomware. No additional software to buy, the chart includes the most modern storage devices and Veeam Backup & Replication™ software.

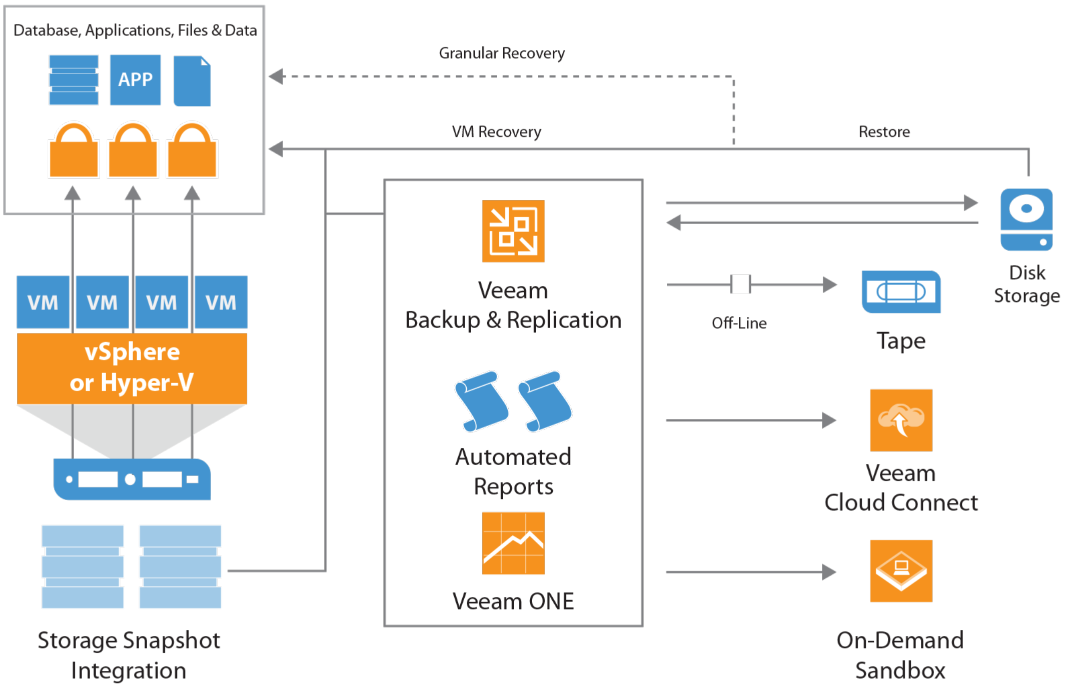

Diagram 1: Veeam operational diagram

Contact us today and become one step closer to achieving Availability for the Always-On Enterprise!

Company Name:

Phone:

Contact Person:

Email: