The Veeam Best Practice Solution for Countering Ransomware

24/7 operations

No patience for downtime and data loss

Growing amount of Data

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.

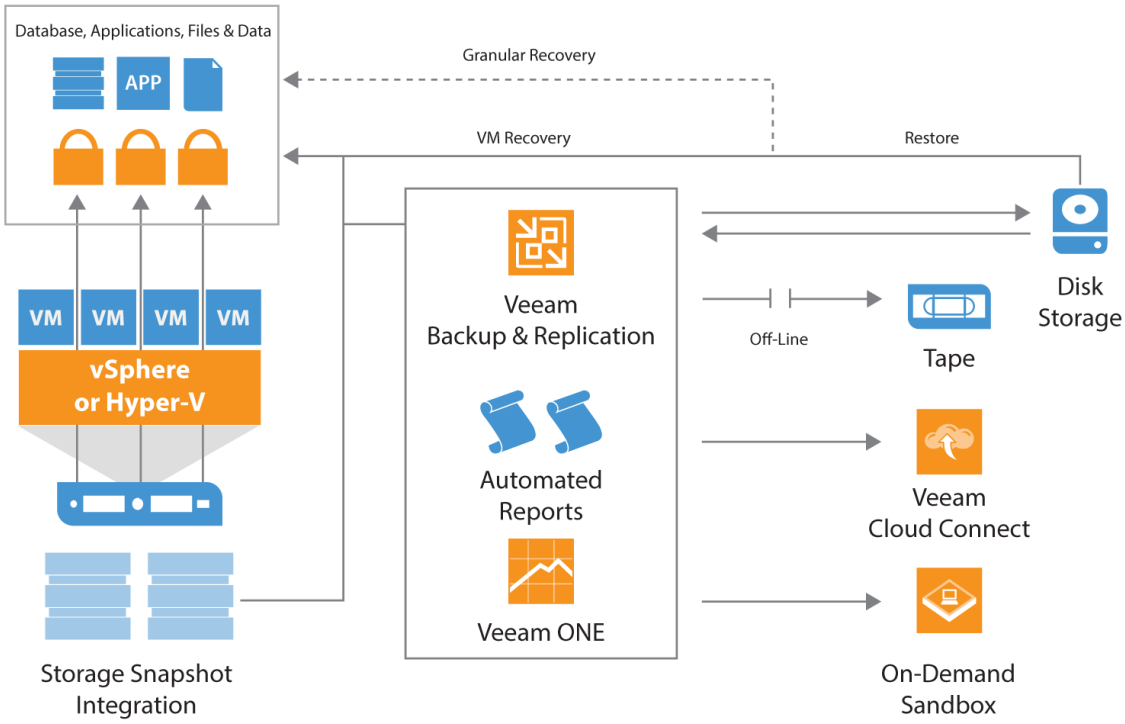

Diagram 1: Veeam operational diagram

Key Veeam Availability features

Veeam Features		Description
Full VM recovery	●	Recover an entire VM on the original host or on a different host. Includes quick rollback functionality to restore changed blocks only.
Instant VM Recovery™	●	Quickly restore service to users by starting a VM directly from a backup file on regular backup storage.
VM file and virtual disk recovery	●	Recover individual VM files (such as VMX) and virtual disks.
Instant File-Level Recovery	●	Recover files from 19 common file systems used by Windows, Linux, BSD, Mac OS, Novell, Solaris and Unix.[3]
Veeam Explorer™ for Storage Snapshots (HPE, NetApp, EMC and Nimble)[1]	●	Restore individual VMs, guest files and application items from EMC VNX, VNX2 and VNXe Snapshots, HPE 3PAR StoreServ, StoreVirtual and StoreVirtual VSA snapshots as well as from NetApp Data ONTAP based storage including FAS, FlexArray (V - Series), Data ONTAP Edge and IBM N series snapshots.-Series), Data ONTAP Edge, IBM N series and Nimble CS- and AF-series snapshots.
Veeam Explorer *for Microsoft Active Directory*	●	Search and restore for all Active Directory object types, such as users, groups, computer accounts, contacts, including user and computer password recovery.
Veeam Explorer *for Microsoft Exchange*	●	Get instant visibility into Microsoft Exchange 2010, 2013 & 2016 backups for item recovery of individual Exchange items (emails, appointments, notes, contacts, etc.), online archive mailboxes and hard-deleted items.
Veeam Explorer *for Microsoft SQL Server*	●	Restore individual SQL databases with ease, without needing an extensive SQL background or having to search for database and transaction log files.
End-to-end encryption	●	Secure backup data and network transfers with end-to-end AES 256-bit encryption without any negative impact on built-in compression and WAN acceleration data reduction ratios.
Native tape support	●	Back up and archive files and VM backups to standalone tapes, tape libraries and virtual tape libraries connected to any Microsoft Windows server in your environment.
Built-in WAN Acceleration	●	Get backups and replicas off site up to 50x faster and save bandwidth with agentless Backup Copy jobs.
Image-based VM replication	●	Replicate VMs on site for high availability or off site for disaster recovery.
Veeam Cloud Connect Replication	●	Ensure availability of your mission critical applications with fully integrated, fast and secure cloud-based disaster recovery through a Disaster Recovery-as-a-Service (DRaaS) provider of your choice.

Veeam Features		Description
Assisted failover and failback	●	Replica rollback and assisted failover and failback.
Replication from a backup	●	Create replicas directly from VM backup files without impacting production.
Planned Failover	●	Facilitate data center migrations with zero data loss.
1-Click Failover Orchestration	●	Built-in failover plan orchestration enabling easy 1-click site failover to minimize unplanned downtime.
SureBackup®	●	Automatically test and verify every backed up VM for recoverability by running the VM directly from the backup file (no full VM restore is required), including support for custom application test scripts.
SureReplica[1]	●	Automatically test and verify every replica VM for recoverability, including support for custom application test scripts.
On-Demand Sandbox™	●	Run one or more VMs directly from a backup in an isolated environment and the ability to troubleshoot, test and train on a working copy of the production environment without impacting business operations.
Centralized Management Web UI (Veeam Enterprise Manager)	●	Get a web-based, consolidated view of your distributed deployment in a single pane of glass without having to login to individual backup servers, including federation of multiple backup servers, centralized reporting and consolidated alerting. All editions include monitoring and reporting across multiple backup servers, as well as the ability to start and stop jobs. Enterprise and Enterprise *Plus* editions also include full job management functionality, and the ability to perform restores.

Summary

Best Practices Solution for ransomware enables organizations to rapidly recover from ransomware while providing an enterprise-class data Availability solution for day-to-day operations.

Learn More:

Veeam Backup & Replication Product Overview

Bedford School CryptoLocker Case Study

Global Alliance Partners: cisco Preferred Solution Partner · DELL EMC · Hewlett Packard Enterprise · Microsoft Partner Gold Application Development Gold Datacenter · NetApp Alliance Partner · vmware PARTNER TECHNOLOGY ALLIANCE