Hewlett Packard Enterprise | VEEAM

Solution brief

Protect your data from malicious ransomware threats

This data availability best practice is designed to ensure that all businesses effectively prepare for and avoid potential data loss and downtime from ransomware attacks. By following industry best practices, IT managers can avoid paying ransom and create a rock-solid data availability solution for day-to-day operations by leveraging both HPE and Veeam® software.

"There's no one method or tool that will completely protect you or your organization from a ransomware attack. But contingency and remediation planning is crucial to business recovery and continuity—and these plans should be tested regularly."

– Former FBI Cyber Division Assistant Director, James Trainor.

This quote helps users understand that ransomware is only part of a threat landscape that will eventually penetrate their network. The best solution is to protect what they are after—their data. **fbi.gov/news/stories/incidents-of-ransomware-on-the-rise**

Rise in ransomware attacks

Ransomware attacks continue expanding to multiple verticals by exploiting regulatory and compliance demands, vulnerable networks, and poor backup best practices. As the threat escalates, more verticals and businesses of all breadths are being targeted and exploited. Even with strong cyber security solutions and practices, networks are consistently penetrated. According to the Institute for Critical Infrastructure Technology (ICIT), 2016 and 2017 are expected to be years in which ransomware wreaks havoc on companies. Ransomware threats are on the rise, with "almost 40% of businesses attacked."[1]

Business and IT risks of ransomware

Ransomware attacks are more than security risks. Businesses victimized by ransomware are faced with financial and technical problems—as well as damage to the company brand from which they might never recover.

Financial downfall

The cost of the ransom, the loss of valuable IT time, and the potential downtime to mission-critical applications can permanently damage a business.

IT setbacks

Hackers retain control and access to the victim's network for potential future attacks and charges. IT managers face recurring threats and dedicate more resources to prevent ransomware, siphoning time from crucial IT practices that are critical to the business.

Damaged company brand

Many businesses fail to report ransomware attacks to avoid a damaged reputation, client loss, and loss of market share. Yet businesses that pay ransoms or fail to back up their data eventually become victims of higher profile attacks that lead to severe damage to their brand identity and reputation in the market place.

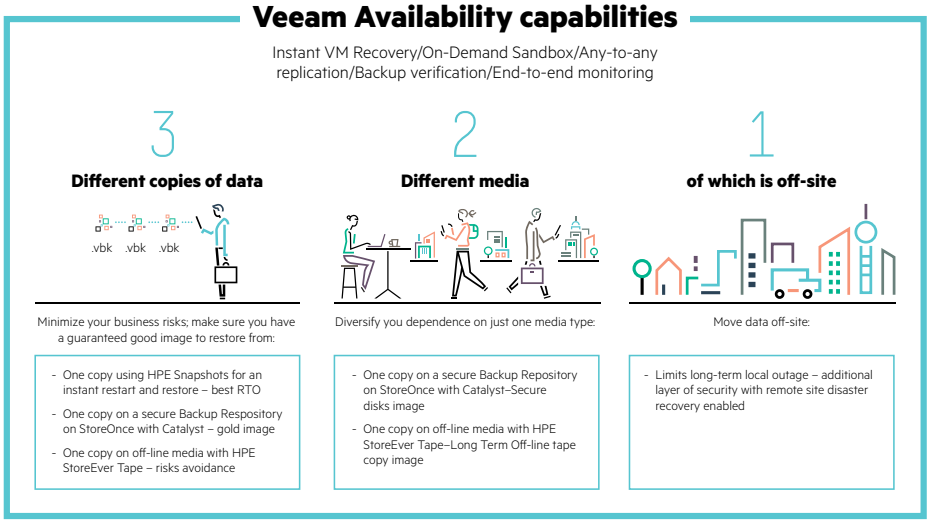
[1] "**Ransomware threat on the rise as 'almost 40% of businesses attacked'**," The Guardian, August 2016.

Veeam and HPE solutions overview
Veeam and HPE's industry-leading solutions are fully equipped for businesses of all sizes to combat malicious attacks and protect their data.

- **Rapid data restores and recovery**
  HPE Storage Snapshots enables fast virtual machine (VM) and granular recovery to override encrypted ransomware databases, applications, files, and operating systems (OS). Recover quickly and avoid application downtime with proven integration with HPE 3PAR StoreServ, Store Virtual, StoreOnce, and StoreOnce Catalyst.
- **Infrastructure lockdown**
  Ransomware can't infect what it doesn't see. HPE makes this possible through an integration with StoreOnce Catalyst, which makes backup images invisible to ransomware, thereby making restore possible. An additional layer of protection is added through offline tape and asynchronous remote replication copies.
- **Testing environment**
  Test and remove ransomware items quickly before restoring VMs to production with Veeam On-Demand Sandbox™ and Veeam SureBackup.
- **Built-in ease of use**
  Leverage the built-in backup assessment to ensure your critical VMs are protected with the Veeam ONE™ monitoring, reporting and capacity planning tool.

These capabilities are standard with the Veeam Availability Suite™ and HPE storage combined integration. This solution does not require any special scripts and leverages standard HPE and Veeam products.

Sign up for updates



Case study—Successful ransomware defense using Veeam

The Bedford School in England was the victim of a malicious ransomware attack through a CryptoLocker virus that infected a faculty member's computer and encrypted all files. The school lacked the resources to pay the hefty ransom and could not afford additional downtime to their networks.

The IT team at Bedford followed the 3-2-1 backup rule and avoided paying any ransom or losing network capabilities. Veeam helped them restore every encrypted file quickly.

The HPE and Veeam ransomware solution

This data availability solution by Veeam and HPE is designed to combat any ransomware attempts by hackers. By following Veeam's 3-2-1 backup best practices, businesses can ensure the integrity and availability of their data. The diagram above depicts the 3-2-1 rule along with industry-leading recommendations.

Leveraging the 3-2-1 backup rule for ransomware

The goal of the 3-2-1 rule is to provide customers with a data protection solution that maximizes application uptime and data availability. With the proper execution of the 3-2-1 backup best practices, IT managers can protect their data by following our 3-2-1 guidelines:

- Maintain three (3) copies of your data—the primary data and two copies— to avoid losing data to a faulty backup.
- Store backup copies on two (2) different media types—such as tape, disk, secondary storage, or cloud.
- Keep one (1) copy off-site—either on tape or in the cloud—in the event of local hazards or ransomware infections within the network.

Summary

The data availability solution is a fully integrated solution comprised of existing technology. It not only enables organizations to rapidly recover from ransomware attacks, but also provides an enterprise-class data availability solution for day-to-day operations. This best practice solution is both flexible and affordable, and can be quickly implemented by a Veeam certified partner.

Learn more about how to follow the 3-2-1 rule with Veeam Backup & Replication™ blog.

Hewlett Packard Enterprise | VEEAM

a00000445enw, January 2017