Counter Ransomware with HPE and Veeam

Health Care Best Practice Solution

This data availability solution is a best-practice for Health Care developed by HPE, Veeam®, and Comport Healthcare Solutions in response to increasing threats of Ransomware and other malware attacks.

24x7

operations.

0

patience for downtime and data loss.

"We really appreciate Veeam's recovery capabilities when we're trying to restore a file or item during an HIPAA audit or for a critical business need."

– Roswell Park Cancer Institute

Addressing Health Care ransomware attacks

Meaningful Use and HIPAA legislation requires a regular risk assessment to identify and remediate risks to patient privacy and the overall protection of health information. These risk assessments should be dynamic and adjusted to address new threats and developments in the Health Care industry. The recent increase in 'ransomware' attacks, particularly targeting Health Care providers, should be explicitly addressed in your organization's next formal risk assessment.

"During the second quarter of 2016, an overwhelming 88 percent of all ransomware detections throughout U.S. industries—including Health Care, Retail, Education, Finance and Technology—occurred at Health Care organizations.[1]" These attacks on hospitals and health systems continue to expose gaps in processes and security tools that allow criminals to extricate ransom fees through untraceable Bitcoin.

The HPE and Veeam Ransomware Health Care Best Practice Solution

This data availability solution is a best-practice for Health Care developed by Hewlett Packard Enterprise (HPE), Veeam, and Comport Healthcare Solutions in response to increasing threats of ransomware and other malware attacks. This solution addresses Meaningful Use and HIPAA requirements, and when implemented as directed, will ensure that data is available to recover from any event that impacts PHI (Protected Health Information), including ransomware attacks. This is a part of the HPE and Veeam Ransomware Health Care Best Practice Solution for data availability and protection.

- **Complies with Meaningful Use and HIPAA regulations**
  - HIPAA Administrative Safeguard rule 164.308(a)(7)(ii)(A)
  - Disaster recovery plan 164.310(d)(2)(iv)
  - Reports for evidence of compliance 164.312(a)(2)(ii)
- **Beyond Meaningful Use and HIPAA regulations**
  - Rapid restores from ransomware attacks
  - Rapid recovery and uninterrupted application performance
  - Test and remove ransomware item
  - Verify and restore to normal operations

Diagram 1 on page two shows how HPE and the Veeam Availability Suite™ provide a turnkey solution to recover from Health Care ransomware. With no additional software to buy, all HIPAA and Meaningful Use functionality listed in the chart are included with standard HPE devices and Veeam Availability Suite software.

[1] According to Security Engineering Research Team Quarterly Threat Report for Q2 2016 from cybersecurity technology and services vendor NTTSecurity, formerly Solutionary.

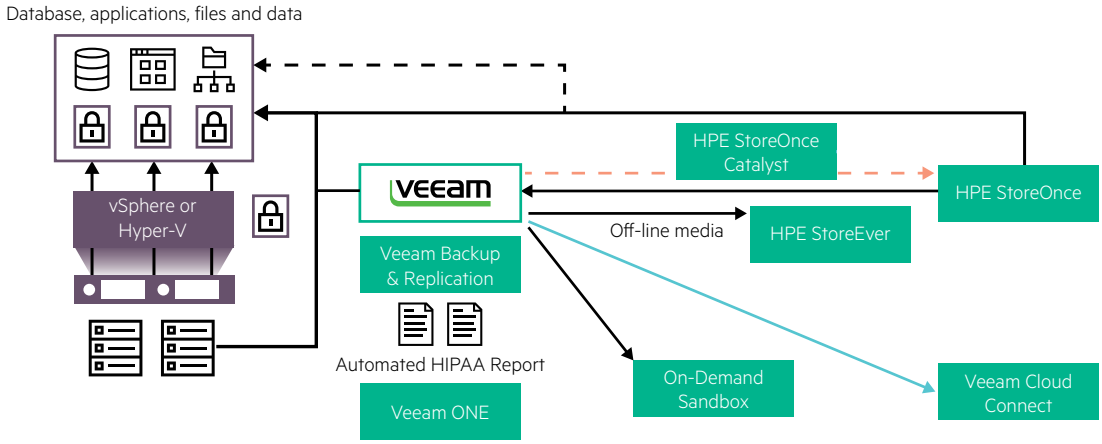

Diagram 1 - HPE and Veeam Ransomware Health Care Best Practice Solution Operational Diagram

Meaningful Use, HIPAA Legislation, and Ransomware Recovery	HPE and Veeam features included with Veeam Availability Suite	Description
HIPAA Administrative Safeguard 164.308(a)(7)(ii)(A)	Veeam Availability Suite software	Data availability solution, includes backup, recovery, and auditing
Disaster recovery plan 164.312(a)(2)(ii)	Veeam Availability Suite software	• Data availability solution, includes Veeam Cloud Connect for remote data recovery and offline media support for tape • Access to backup is controlled by HPE StoreOnce Catalyst, only active when used for backup and/or recovery purpose. Protects against ransomware attacks/scans of backup storage
Reports for evidence of compliance 164.312(a)(2)(ii)	Veeam ONE™	Monitoring, reporting, and capacity planning tool for the Veeam backup infrastructure
Rapid restores from ransomware attacks	Veeam Explorers™	Rapidly restore VMs, Guest OS, individual files, OS files, emails, applications MS SQL, MS Exchange, AD, MS Share Point and Oracle databases directly from your backups
	Instant VM Recovery™	Run any virtualized application on VMware vSphere or Microsoft Hyper-V directly from a snapshot
Integration with HPE Storage Snapshots, HPE StoreOnce, and HPE StoreOnce Catalyst	Backup from Storage HPE Storage Snapshots and HPE StoreOnce Catalyst protocol support	• Use HPE storage snapshots to quickly create copies of your environment, with no impact to production • StoreOnce for data encryption and deduplication • Catalyst for high speed backup, restore and security
Test and remove ransomware	On-Demand Sandbox™ for Storage Snapshots	Create a complete isolated copy of your production environment to remove the offending ransomware item before restoring to production

To learn more:

Contact Comport Healthcare Solutions at 201.236.0505 or info@comport.com.

Sign up for updates

Summary

The HPE and Veeam Ransomware Health Care Best Practice 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 Comport.

Learn more:

Veeam Product Overview
HPE and Veeam Availability solutions
Comport Healthcare Solutions – HPE Platinum Partner IT Service Provider, specializing in health care

4AA6-7848ENW, September 2016