VEEAM | PROPARTNER

Customer Scenario Card

Customer Scenario:

IT is unable to manage and recover unstructured data from large file shares and file servers

Persona

Technical Decision Maker

Feature/Product

Veeam® Backup & Replication™ — Enhanced NAS backup

Hurt

Broad questions: How do they do it now?

- How do you protect your unstructured data held in NAS?
- What is your process to recover a single file from a NAS file share?
- What is your process to recover from a broad ransomware attack on your NAS system?

Credibility questions:

- Do you have plans to purchase a NAS device in the future? What are you using now?
- Do your NAS file share and file server backups take longer than you would like?
- Do you struggle with recovering a single file from your NAS file share?

Scenario Overview

IT is unable to manage and recover unstructured data from large file shares and file servers

Most current and potential Veeam customers use network-attached storage (NAS). NAS devices provide the infrastructure to consolidate storage of unstructured data such as audio, video, websites, text files and Microsoft Office documents, all in one place. What draws customers to NAS is its ease of access, high capacity and fairly low cost.

The problem is that many customers are now protecting their unstructured data with tools and technologies that were designed decades ago and not built to handle the amount of data that customers have today.

To manage unstructured data through NAS, a few strategies commonly seen are:

- Larger companies may purchase specialized high-end NAS hardware that is effective and fully featured, but expensive and use proprietary protocols. Examples of this are from NetApp and Dell EMC.
- Medium and small companies may purchase a commodity NAS hardware solution which is more affordable and flexible but has limited capabilities and depends on NDMP to move data. This is a legacy approach that is slow and requires frequent full backups.
- Small-to-medium-sized businesses (SMBs), departments and remote offices may cobble together hardware using their own design that's more flexible but slow and potentially unreliable.

Plausible emergency

How would you feel if: You were unable to achieve your NAS recovery point objective SLAs due to your backup solution taking a long time to determine which files have changed and what needs backed up?

Emergency example: Customer gets infected with ransomware that encrypts all the data on their NAS. However, since their NAS backup solution takes too long to get incremental backups completed, files that have not yet been backed up have been encrypted and may be lost forever.

What if instead: Your NAS backup solution knew exactly which files and folders have changed, which dramatically decreased incremental backup performance to achieve your stated SLAs?

Trigger words/ events:

Trigger words:

- NAS
- Server message block (SMB) and/or common internet file system (CIFS) (NAS connection types is used interchangeably)
- Network file system (NFS)
- Unstructured data
- NDMP
- High-end NAS device vendor examples like Dell EMC Isilon and NetApp
- Commodity NAS device vendor examples like Synology and QNAP
- File share

Trigger events:

- A previous potential Veeam customer that did not purchase Veeam due to the lack of advanced NAS capabilities
- Can't meet backup windows for NAS
- Business changes that vastly increase the amount of unstructured data collected
- Issues in protecting large amounts of unstructured data with commodity or build-it-yourself hardware
- Changes to cloud strategy such as needing to restore to the cloud

Questioning strategy

Rescue

Usage scenario:

- If you could use any NAS hardware without sacrificing the ability to recover a single file anywhere with a few clicks, would it help you be more flexible in your hardware purchases?
- Would it help you meet service level agreements (SLAs) if you could protect your NAS file shares and file servers with advanced speed and recovery options, no matter what NAS hardware you purchase?
- Would you be more confident if you could rollback your NAS data to a specific point in time to quickly recover from any ransomware attack?

Competitive differentiators

- **The changed file tracking** feature enables faster incremental backups compared to the competitors that must scan each file to determine changes.
- **By not using NDMP**, Veeam enables customers to use any source NAS device alongside nearly any target backup device unlike legacy solutions that use NDMP and back up appliances that require their own hardware backup targets.

Key selling points

- **Leverage and extend current investments by increasing** the functionality (i.e., speed, restore options, flexibility) of commodity hardware or extending the functionality of high-end NAS devices, which increases ROI and flexibility.
- **Save time and effort** with innovative file change tracking that speeds up incremental NAS file server backups on any NAS filer, even for commodity NAS devices or build-it-yourself Linux or Microsoft Windows file shares.
- **Restore what you need when you need it** with flexible restore options, including entire share recovery that addresses complete hardware loss, point-in-time share rollback to help quickly recover from ransomware attacks and granular file-level recovery with global search features for day-to-day operational restores.

Sales and marketing resources

Short deck

Campaign-in-a-Box

Product overview