VEEAM | PROPARTNER

Customer
Scenario Card

Customer Scenario:

IT is expected to keep data 100% safe from ransomware and other internal or external threats

Persona

Technical Decision Maker

Feature/Product

Veeam® Backup & Replication™: Ransomware protection with Veeam Cloud Tier

Trigger words/ events:

Trigger words:

- Ransomware
- Malware attacks
- Data security
- Cloud storage

Trigger events:

- Previous ransomware/ malware threat
- Change to data security requirements
- News of other companies'
  or peer data issues
- Moving from tape to cloud storage

Scenario Overview

IT is expected to keep data 100% safe from ransomware and other internal or external threats.

Have you heard anything about a company having to pay a ransom to get their data back? Being attacked by malware? Facing a data breach? Many of those stories end with the loss of customers, profit, reputation and often all three. Companies today must treat their data as the most important asset they have to protect, just like money in a bank or company secrets in a vault. To be protected from these attacks, historically, customers would put data on tape and send it secure offsite location that is disconnected from the network and safe from ransomware, malware or malicious actors.

With the growing popularity of cloud storage, customers are now moving from tape to cheaper cloud-based object storage for long term retention. Due to this shift, customers now need to create immutable backup copies when storing them in object storage. This means that data can't be locked or encrypted by ransomware, malware or malicious actors.

Key selling points

- **Data is kept safe against customer data breaches** due to ransomware and malware but is still recoverable, even outside the data center.
- **Immutable backup copies means that data is secure** and unable to be modified or deleted even against malware and malicious actors.
- **No additional data management is needed** to make backup copies secure from ransomware, malware or other malicious actors.

Questioning strategy

Hurt

Broad questions: How do they do it now?

- How do you keep your **primary data** safe from ransomware, malware or other threats?
- How do you keep your **backup copies** safe from ransomware, malware or other threats?
- What is your recovery procedure if you do get hit with ransomware? Can you recover?

Credibility questions:

- Is your management concerned with ransomware or other data threats?
- Are you dealing with a manual process to try to secure your backup data?
- Are you certain your data is still secure once it leaves your data center? Can you confirm its security?

Rescue

Usage scenario:

- If you knew your backup copy in object storage was immutable, would it help you feel more secure?
- If you could set up a policy that automates creating an immutable backup copy on your schedule, would it improve data security overall while reducing management time?

Plausible emergency

How would you feel if: Your primary backups were encrypted due to a ransomware or malware infection that spread to backup storage leaving you unable to recover from backups and forced to pay a ransom to criminals for access to your data?

What if instead: You followed the 3-2-1 Rule and had more than one copy of your backup data in the cloud with the added functionality of immutability that eliminates any possible infection of backup copies?

Competitive differentiators

While some competitors use proprietary means to provide immutable backup storage for ransomware protection and further lock customers into their own platforms, Veeam uses AWS' existing object-lock API, which reduces the complexity and potential security issues that come with proprietary mechanisms.

Sales and marketing resources

Short deck

Campaign-in-a-Box

Product overview