VEEAM PROPARTNER NETWORK

Product Scenario Card

Veeam Backup *for AWS*, *for Microsoft Azure* and *for Google Cloud*

Scenario overview

Corporate cloud-first mandates, and lack of available servers, have pushed organizations to transform FAST. Many quickly add AWS, Azure or Google Cloud Backup to their service subscriptions — but find it doesn't meet the needs of their business.

Here are just a few of the challenges and pain points organizations may experience:

- Cyber security attacks, disparate recovery across hybrid cloud
- Accidental deletion, cumbersome recovery in cloud
- Snapshot sprawl, compounding cloud costs
- Retention policy gaps across on premises and cloud workloads
- Complex systems, reducing staffing efficiencies

Elevator pitch

Veeam Backup for AWS, Azure, Google Cloud

delivers native, policy-based protection for reliable recovery from accidental deletion, ransomware and other data loss scenarios. It's an API-first approach, and immutable backups and full- and file-level restores ensure resilient protection that's easy and cost-optimized. This frees up time and resources for strategic IT priorities.

Trigger words / events

Words

- Public / Hybrid / Multi Cloud
- AWS Services (EC2, RDS, EFS, VPC, Outposts)
- Azure Services (Azure VMs, Managed Disks, Azure SQL, Azure Files, Azure Blob)
- Google Cloud Services (Compute Engine, Persistent Disks, Cloud SQL for MySQL and PostgreSQL, Cloud Storage)
- AWS Backup, Azure Backup, Google Cloud Backup

Events

- Lift & Shift of workloads from on premises to the cloud
- Cloud-first strategy for new workloads
- Ransomware or any cyber security attack
- Cloud overspend from retaining native snapshots
- Accidental deletion of cloud data
- Compliance mandates and audits compliance needs

Land and expand

Standardizing data protection across data center and cloud helps control threat surface and reduces budget and staffing inefficiencies.

- Veeam Universal License (VUL) makes entitling protection of cloud workloads easy
- Adding Veeam ONE™ supports monitoring of protection across the infrastructure
- Winning new accounts to Veeam can start with cloud, as Veeam's comprehensive protection offers competitive differentiation
- Lead with cloud in cloud-first sales opportunities, especially in white space (e.g. no backup, first-party backup)
- Expand to on premises for legacy competitive takeout

Key selling points

- **Relentless security** secured access and data management to help you overcome ransomware and other cyberthreats
- **Fast, reliable recovery** — powerful Recovery options that keep businesses productive with nearzero recovery time objectives (RTOs)
- **Zero compromise** — zero-fuss backup that meets service level agreements (SLAs) and budgetary requirements across the hybrid cloud

Menu of goals

Used as a strategy to help identify the customer's goal/problem/need

Business value (EDM)	Technical Goals (TDM)
"I need to control the costs associated with storing backups in line with our business and compliance goals".	"I want to stop spending hours each day manually managing point products across multi-cloud environments."
"I want a solution that is able to properly protect my workloads wherever they are, now and in the future."	"I need a solution that aligns to the well-architected security framework from AWS (Azure/Google Cloud)."
"My organization has zerotolerance for gaps in our cybersecurity strategy, including backup of our cloud workloads."	"I must be in control of my cloud backup spend so I stay under budget with my manager."

veeam PROPARTNER NETWORK

Product Scenario Card

Veeam Backup *for AWS*, *for Microsoft Azure* and *for Google Cloud*

Highlighting limitations of first-party backup

Why AWS Backup, Microsoft Azure Backup and Google Cloud Backup fall short:

- **Not secure:** Snapshots are not independent or isolated from the service or data they are protecting. If that service or data were to be compromised by a cyberthreat, then that snapshot would be compromised also leaving nothing to recover from.
- **Difficult to recover:** Recovering from snapshots is a manual and complex process, with the user having to create, connect, boot, mount and destroy services. This hinders recovery time objectives (RTOs) and increases the impact of downtime.
- **Expensive to retain:** Snapshots are often kept on disk which is significantly more expensive that object storage options, causing noncompliance with retention requirements or overspend.
- **Locked-in to a platform:** Snapshots are specific to that workload on that platform and are not portable across environments (e.g., one cloud to another, cloud to on-premises).
- **Complex in Hybrid / Multi Cloud:** Snapshotting and snapshot managers are specific to that platform only, which leads to complex and resource-intensive management of multiple point products that do not integrate.

Competitive differentiators

- **Operational consistency:** Centrally manage and monitor backup across hybrid- and multi-cloud environments
- **Portability:** Mobilize data, backups and licensing to, from and across clouds
- **Relentless security:** Secure data management and access
- **Fast, reliable recovery:** Recover full- and file-level data from any location
- **Zero compromise:** Cost control and automation/Day2

Objection handling

We already use AWS/Azure/Google Cloud Backup.

Even though AWS/Azure/Google Cloud Backup already have a backup solution, organizations find they don't meet all their requirements to have a secure, reliable environment. It is their data, and therefore their responsibility to protect it from data loss and cyberattacks.

I don't need to protect my cloud data — it is durable enough.

Veeam delivers native backup for AWS, Azure and Google Cloud that goes beyond the basic snapshotting of first party tools. With Veeam, organizations have access to full- and file-level restores to ensure resilient protection that's easy and costoptimized.

Questioning strategies

Helps you determine the customer's specific pain points and impacts so you can position the capabilities that would solve them

Credibility questions

Builds credibility to demonstrate knowledge of customer needs. Does that mean that you...:

Are you confident that you could recover from a ransomware attack on your cloud data?

What is your process for recovering individual files or folders of cloud data?

Could you move your data to another platform (i.e., cloud or data center)?

Environmental questions

Aims to understand the current state. How much? How many? How often?

Have you calculated your recovery point objectives (RPOs) for your most critical cloud workloads?

Have you calculated the real-time recovery time it takes you to recover cloud data?

Have you calculated your cost for storing snapshots long-term?

Broad questions

Gets them talking about goals/needs. Usually starts with "how?" or "what?"

What is your organization currently doing with the public cloud?

What is your process for backup of public cloud data?

How many products do you use to back your data up across your hybrid infrastructure?

Impact questions

Demonstrates the financial/personal impact of the existing state. Creates business justification for change.

What is the impact to your business if you don't have a clean backup to restore from if you were attacked by ransomware?

What is the impact to your personal productivity if you have to have to recover an individual file that was accidentally deleted?

What is the impact to your team's budget if you overspend on backup (i.e. compute and networking)? Does it take away from transformation initiatives?