1. Use Cases and Scenarios

This service provides a secure, isolated, and immutable backup environment for Veeam workloads hosted in Azure, ensuring compliance, data protection, and ransomware resilience. Key use cases include:

- **Immutable Backup Repository**
  Store backups in Azure Blob with immutable storage (WORM) to prevent modification or deletion during the retention period.
- **Ransomware Recovery**
  Isolate backup storage in a secure vault with network segmentation and restricted access, ensuring recovery from cyber incidents.
- **Compliance and Regulatory Retention**
  Meet industry standards and legal retention requirements with immutable backup copies and audit logging.
- **Air-Gapped Backup Tier**
  Implement logical air-gapping by disconnecting the vault from production networks except during controlled backup/restore operations.
- **Disaster Recovery Readiness**
  Ensure offsite, tamper-proof backup copies are always available for recovery in case of on-premises or cloud incidents.

2. Architecture Overview

The architecture of Secure Vault for Veeam on Azure includes the following components:

- **Veeam Backup Server**
  Orchestrates backup jobs, manages repositories, and handles restore operations.
- **Azure Compute (Vault Access Gateway)**
  Dedicated, hardened virtual machines or appliances providing controlled access between Veeam infrastructure and the secure vault.
- **Azure Networking**
  Isolated virtual networks and subnets, NSGs, and firewall rules to restrict inbound/outbound traffic to authorized flows only.
- **Immutable Azure Blob Storage**
  Backup repository configured with Immutable Storage (WORM) and optional encryption keys managed by Azure Key Vault.
- **Monitoring & Logging**
  Integration with Azure Monitor and Veeam ONE for backup health monitoring, anomaly detection, and compliance reporting.

3. Supported Environments

Secure Vault for Veeam supports backup data from multiple source environments, including:

- **VMware vSphere Environments** (on-premises or hosted)
- **Azure VMware Solution (AVS)** workloads
- **Microsoft Hyper-V** clusters or standalone hosts
- **Physical Servers / Bare Metal** running supported OS (Windows Server, Linux)
- **Multi-cloud Deployments** (AWS, GCP) using Veeam Cloud Tier integration
- **Legacy Systems** backed up via Veeam Agents
- **Mainstream OS**: Windows Server (2012+), RHEL, Ubuntu, CentOS, SUSE

The only requirement is that Veeam can access the target vault over a secure IP connection, using VPN or private ExpressRoute for isolated transfer.