SUMMIT

Proxmox VE Backup, powered by Veeam

ENTERPRISE PROTECTION FOR KVM WORKLOADS.

Challenge

Proxmox Virtual Environment has moved from the lab into production. Organizations leaving VMware after the Broadcom licensing changes are standardizing on Proxmox VE for its open KVM foundation and predictable cost, and the workloads landing on it are the same SQL Servers, domain controllers, and line-of-business applications that used to live on vSphere.

What has not moved with them is the data protection operating model. Proxmox's built-in vzdump and Proxmox Backup Server are capable tools, but they are tools: someone has to run them, size them, verify them, keep copies off-site and immutable, and prove recovery to an auditor. They also recover only to Proxmox, which matters when the business wants the option to land a workload on another platform.

Summit's Proxmox VE Backup as a Service delivers fully managed, application-aware, image-level protection for Proxmox VE virtual machines, built on Veeam Backup & Replication, operated by Summit, and stored in immutable Summit repositories.

How We Do It

AGENTLESS, IMAGE-LEVEL BACKUP

Veeam worker appliances deployed into the Proxmox environment capture whole-VM images from Proxmox VE snapshots, with changed block tracking for fast incrementals. No agent is installed in the guest for backup unless application-aware processing is enabled, using the QEMU Guest Agent together with Veeam's non-persistent guest runtime.

RECOVERY TO WHEREVER THE BUSINESS NEEDS IT

Restore a file, an application item, or a whole VM back to Proxmox VE, bring a Proxmox backup up as a VMware vSphere, Hyper-V, or Nutanix AHV virtual machine with Instant Recovery, or restore it to Microsoft Azure, AWS, or Google Cloud. The same engine restores VMware and Hyper-V backups into Proxmox VE, which is how Summit supports customers mid-migration.

FULLY MANAGED OPERATIONS

Summit owns node onboarding, worker placement, policy configuration, monitoring, failure remediation, backup-window planning in coordination with customer needs, licensing reconciliation, and capacity management. Your team requests restores; ours performs them.

Deployment Models

Both models deliver the same underlying service. The difference is where the Proxmox VE environment lives and therefore where the Veeam workers run.

PROXMOX VE AT SUMMIT

The customer's Proxmox VE hosts run in a Summit data center. Workers, backup infrastructure, and repositories are on the same high-speed fabric, which keeps backup windows short and simplifies network design.

PROXMOX VE AT THE CUSTOMER SITE

The customer's Proxmox VE environment stays on-premises or in third-party colocation using cloud connect or via VPN to a backup repository. Summit deploys workers into that environment and backs up across a secured path to a Summit repository, with backup copy to a second site available.

Key capabilities

IMAGE-LEVEL VM BACKUP

Whole-VM capture of Proxmox VE QEMU/KVM virtual machines on Proxmox VE 8.2 through 9.2, including disks and VM configuration, through Veeam for Proxmox VE.

FILE-LEVEL RECOVERY

Mount a restore point and recover individual files and folders from Windows and Linux guests across the file systems Veeam supports.

APPLICATION-AWARE PROCESSING

Transactionally consistent backups with transaction-log handling for Microsoft SQL Server, Oracle, and PostgreSQL, and application-aware processing for other Veeam-supported applications in Windows and Linux guests.

CHANGED BLOCK TRACKING

Incremental backups read only changed blocks using QEMU dirty bitmaps, keeping daily runs short and repository growth proportional to change. QCOW2 disks retain tracking across VM power cycles; RAW and VMDK disks are re-read after a power-off.

APPLICATION-ITEM RECOVERY

Recover databases and application items through Veeam Explorers without restoring the whole VM.

INSTANT RECOVERY TO OTHER PLATFORMS

Start a Proxmox VE backup directly as a VMware vSphere, Microsoft Hyper-V, or Nutanix AHV virtual machine while data migrates in the background. Instant Recovery back into Proxmox VE is available with experimental support status from Veeam.

CROSS-PLATFORM RESTORE INTO PROXMOX

Restore VMware vSphere, Microsoft Hyper-V, Nutanix AHV, and Veeam Agent backups as Proxmox VE virtual machines, which turns the backup platform into a migration path for a VMware exit.

IMMUTABLE STORAGE

Backups written to Summit immutable repositories so retained copies cannot be altered or deleted inside the immutability window, including by a compromised administrator.

ENCRYPTED END TO END

Encryption in transit between workers, the backup server, and the repository, and encryption at rest on Summit repositories.

MALWARE DETECTION

Scheduled scanning of restore points with Veeam Threat Hunter or YARA rules, so a clean restore point can be identified before recovery.

BACKUP COPY AND 3-2-1-1-0

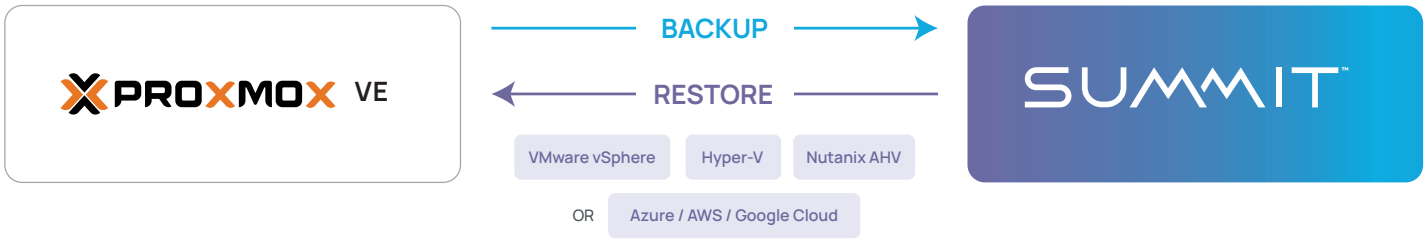
Optional second copy to another Summit site, object storage, or a Summit Veeam Cloud Connect repository for off-site, immutable retention.

MONITORING AND REPORTING

Continuous job-health monitoring by Summit operations, with success and capacity reporting, plus a quarterly health review covering job trends, restore tests, capacity, and licensing.

Your Business Data

DATA PROTECTION AND MANAGEMENT SOLUTIONS



WHAT GETS PROTECTED:

- Virtual machine disks and configuration
- Windows and Linux guests
- SQL Server, Exchange, Active Directory, SharePoint
- Oracle and PostgreSQL databases
- Files and folders
- Application items

Benefits

MANAGED PROTECTION THAT MOVES WITH YOUR HYPERVISOR STRATEGY

PROTECT PROXMOX LIKE PRODUCTION	Application-consistent, immutable, off-site backups with tested recovery, rather than a snapshot script and a hope.
KEEP YOUR PLATFORM OPTIONS OPEN	Recover a Proxmox workload on VMware, Hyper-V, or AHV, or bring a VMware workload into Proxmox, from the same backup set. The backup platform is not what locks you in.
REMOVE THE OPERATIONAL BURDEN	Worker placement, backup windows, change-rate surprises, licensing reconciliation, and failure remediation shift to Summit, with no additional headcount and no second backup product to learn.

Service Details

PROTECTED WORKLOADS:

Proxmox VE 8.2 through 9.2 virtual machines (QEMU/KVM) on x86-64 hosts installed from the official Proxmox ISO, standalone or clustered.

DEPLOYMENT MODELS:

Proxmox VE hosted at Summit, or Proxmox VE at the customer site with Summit-deployed workers. Same underlying service in both.

NOT IN SCOPE:

LXC containers, VM templates, linked clones, VMs sharing a BIOS UUID, iSCSI-attached and passthrough disks, VMs on BTRFS or custom storage, and Proxmox VE permissions, users, and API tokens. These are limitations of Veeam for Proxmox VE and are read to the customer at scoping.

Service Details

STORAGE:
Summit immutable repositories (hardened repository or S3-compatible object storage with object lock). Optional backup copy to a second Summit site, object storage, or Veeam Cloud Connect. Backup copies of Proxmox VMs held on Cloud Connect support file-level restore only.

REPORTING:
Continuous job-health monitoring by Summit operations, with success and capacity reporting. Quarterly health review covering job-success trends, restore tests performed, capacity trends, licensing reconciliation, and ticket history.

LICENSING:
Per protected virtual machine through Veeam Universal License instances, plus repository storage consumed. A VM is licensed while it has a restore point in the last 31 days.

SUPPORT MODEL:
24x7x365 incident response through the Summit NOC for priority incidents. Change requests, scope adjustments, and non-urgent configuration changes are handled during business hours. Escalation runs through Summit support and engineering, with Summit opening Veeam cases on the customer's behalf where required.

BACKUP FREQUENCY AND RPO:
Daily by default, tunable to the customer's requirement; transaction-log backup intervals for supported databases.

RETENTION:
Policy-driven, with GFS weekly, monthly, and yearly tiers for compliance or regulatory hold.

ENCRYPTION:
Encrypted in transit, and at rest on request.

ONBOARDING:
Approximately two to three business weeks from order to first completed full backup, including node onboarding, worker deployment, and initial backup. The customer provides a root-equivalent account on each Proxmox VE node as well as the Proxmox platform itself (password-based SSH, by requirement), file-level storage for workers, network paths, and the QEMU Guest Agent in guests needing application-aware processing.

COMPLIANCE:
SOC 2 Type II across Summit data centers and processes. HIPAA BAA available on request.

Related Summit Services

PROXMOX VE DRAAS	VEEAM CLOUD CONNECT	MANAGED BACKUP AND DRAAS
Replicate Proxmox VE virtual machines to a Summit recovery site for minutes-level RPO and Summit-run failover from a tested runbook, built on the same Veeam platform.	Send backup copies from your own Veeam deployment to a Summit cloud repository for off-site, immutable retention.	Extend a single data protection strategy across Proxmox VE, VMware, Hyper-V, physical, and SaaS workloads.