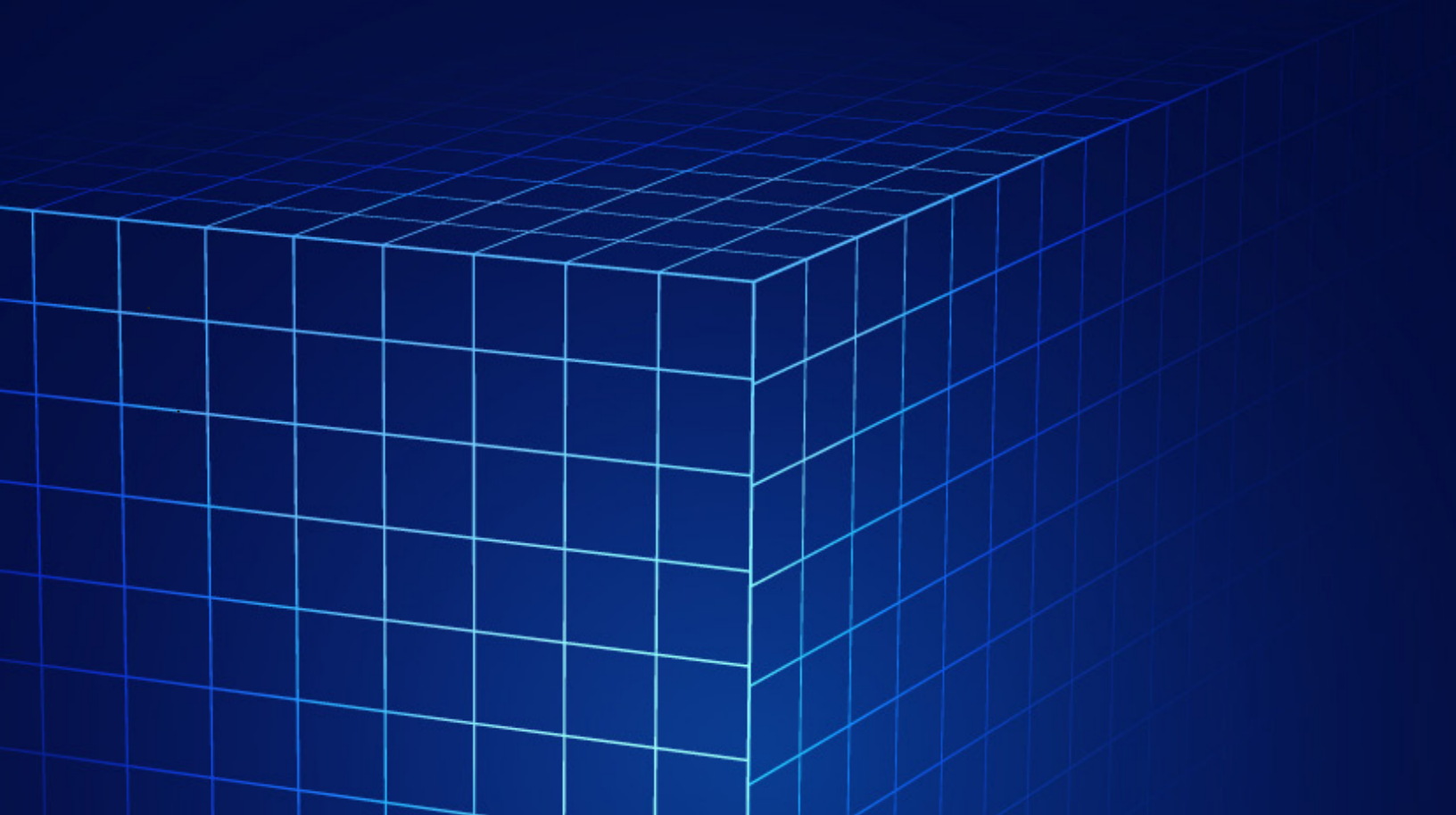
PLATFORM9 VEEAM

Migrate off VMware

Your Veeam protection moves with you

Private Cloud Director (PCD) integrates natively with Veeam Data Platform, delivering agentless, snapshot-based protection for migrated VMs through the Veeam workflows your team already operates.

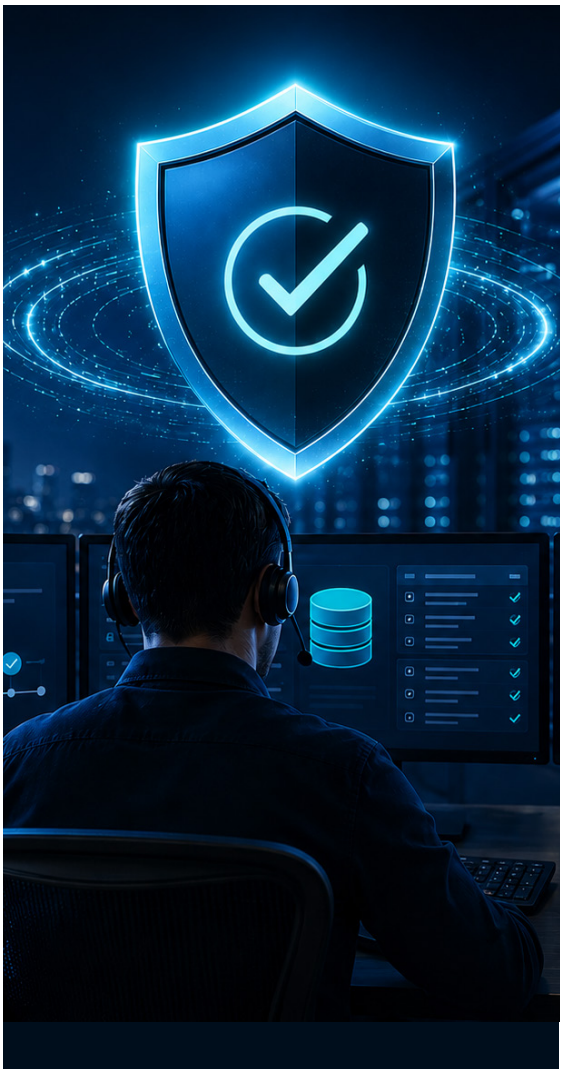


What the renewal quote actually says

Broadcom's post-acquisition pricing pushed VMware renewal quotes up 5× to 10× for enterprises. For service providers in Broadcom's VMware Cloud Service Provider (VCSP) program, the problem runs deeper than price. Most can no longer renew directly at any price. Their options narrowed to buying through a shrinking set of authorized partners, rehosting customer workloads on public cloud, or replacing the virtualization stack outright. The dollar delta for a mid-size service provider runs into the seven figures a year, with no corresponding gain in capability. For most VCSP providers, the exit is no longer hypothetical. It is a deadline. The live question is what survives the move.

The path off VMware with vJailbreak

Private Cloud Director (PCD) is where your estate lands. It is a VMware alternative that runs on the hardware you already own and delivers the HA, live migration, and multi-tenancy your team expects. vJailbreak is how you get there. It is Platform9's free, open-source migration tool that moves VMs from VMware to PCD, with no separate migration tooling to license.



The migration into PCD runs as one pipeline. vJailbreak connects to vCenter and discovers the source VMs. It copies each one using changed-block tracking, so the final cutover moves only the changed blocks. It then converts each VM to run on PCD, injecting VirtIO drivers, remapping networks and storage, and running a health check. In the common path, your ESXi hosts stay untouched, and each VM is only briefly shut down at cutover. When you want to reuse the same hardware, vJailbreak can also reprovision the freed ESXi hosts as PCD nodes, one host at a time.

VirtIO drivers show why the pipeline matters. They are the step older tools left for you to do by hand, and because vJailbreak handles them on the way in, every VM lands on PCD ready to run and ready to back up.

Your backup and restore keep working

Veeam is the market leader in data protection. Service providers standardize on it for a simple reason. They sell uptime, while Veeam Data Platform is the solution behind that promise. When a tenant database becomes corrupt at 3 a.m., or a storage rack goes offline mid-close,

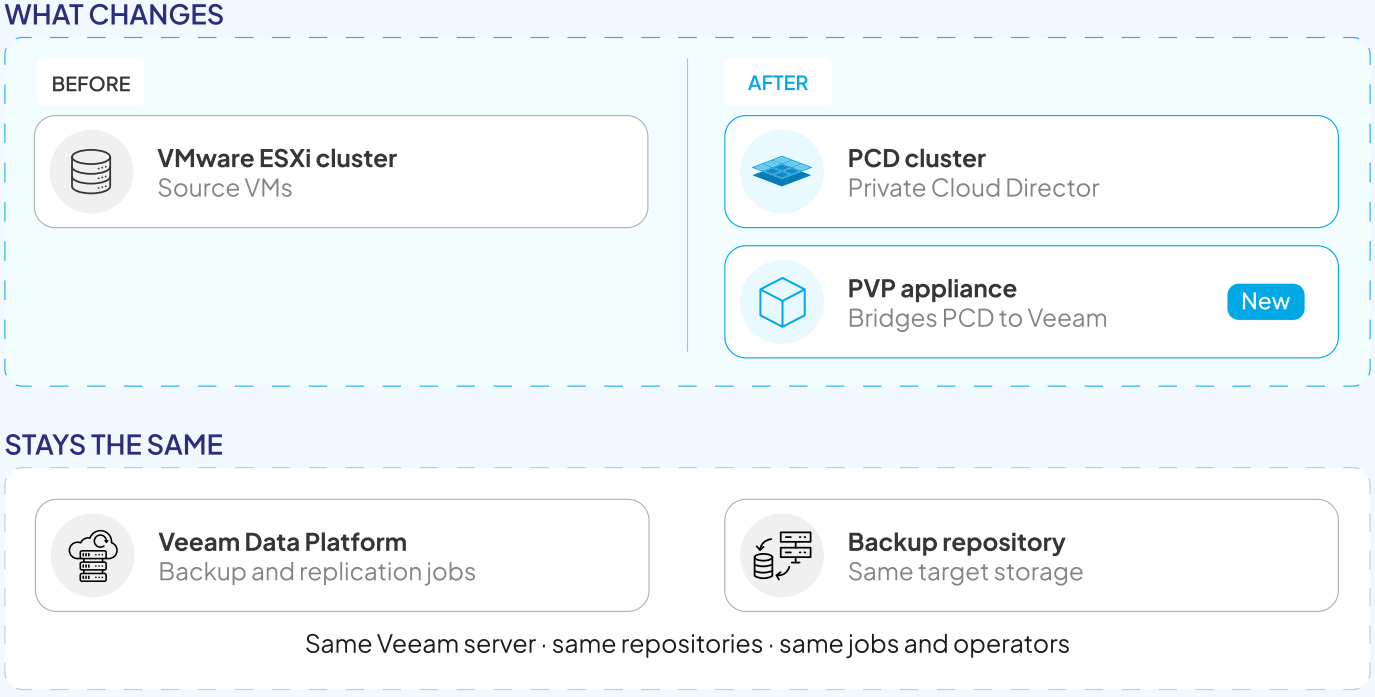
the operator restores to a known good point within the SLA. That reliable procedure was built on Veeam over the years, across the runbooks, dashboards, and on-call playbooks. With the Platform9 and Veeam integration, the hypervisor changes, while your backup doesn't. Your team keeps running the same Veeam deployment and meeting the same SLA.

How the integration actually works

PCD delivers a VMware-alternative virtualization layer on the servers and storage you already run, with HA, live migration, and multi-tenancy. Veeam Data Platform drives protection through native integration, with no custom scripts, no third-party proxies, and no in-guest agents. The integration is co-engineered by Platform9 and Veeam and validated through Veeam's Universal Hypervisor API program. The PCD Veeam Proxy (PVP) appliance presents PCD to Veeam as a supported hypervisor through Veeam's Universal Hypervisor APIs. Veeam's oVirt KVM plug-in service connects to the PVP, and a Veeam Worker moves the disk data to your repository. Backups are agentless and use snapshots taken through PCD's storage layer. Workload VMs run undisturbed while jobs execute. Job creation in the Veeam console is identical to that of any other supported hypervisor. Same wizard, same scheduling, same restore points.

MIGRATION IMPACT

Same backup stack, new hypervisor



Only the hypervisor changes. The backup topology, repositories, and operator workflow stay intact.

What it looks like at scale

Picture a service provider protecting dozens of tenant organizations on PCD. Each tenant runs a dedicated PVP appliance, so tenant data never crosses the proxy boundary. Cross-tenant restores are performed by explicitly targeting the destination tenant‘s PVP, ensuring each restore remains scoped to that tenant‘s proxy and credentials.

What you get, mapped to what you sell

Capability	Platform9 PCD	Veeam	Outcome
Agentless backup	PCD-managed volume snapshots	Veeam Data Platform coordinates jobs; Workers move data	Zero in-guest agent overhead during backup windows
Full VM restore	Restore to an alternate location	Cluster, storage, name, and network are all selectable	Known-good recovery on demand, under SLA
Per-tenant isolation	Dedicated PVP per tenant	Tenant-scoped credentials	Tenant data stays inside its boundary on shared infrastructure
Cross-tenant restore	Target destination tenant’s PVP	Cross-tenant restore	Workload relocation without credential proliferation
Migration continuity	Receives VMs from any source hypervisor via oVirt KVM restore	Restores VMware-era backups onto PCD	VMs and their backup history survive the move off VMware*

* VMs restored from older Veeam backups, rather than migrated through vJailbreak, require VirtIO driver injection after restore, a documented one-time step per legacy VM. VMs migrated via vJailbreak have their drivers injected during conversion, which is the recommended path.

The integration tax, itemized

Footprint

One PVP appliance per PCD tenant, an m1.xlarge VM (8 vCPU, 16 GB RAM, 50 GB volume), supporting up to 10 concurrent backup or restore operations. Scale it by adding 1 vCPU and 1 GB of RAM for every 2 additional concurrent operations.

No per-VM licensing

The PVP appliance is part of the integration. You size it in compute, not license count, and there is no per-VM backup license for the proxy.

Effort

Standing up the proxy and running a first non-production tenant is a contained exercise, not a project.

Storage

Uses your storage array's existing snapshot capability, a Cinder backend with snapshot support, and targets your existing Veeam backup repository. Only Cinder-volume VMs are supported; image-backed VMs are not.

Network

Veeam Data Platform to repository pathing is unchanged. The PVP appliance and workers need reachability to the Veeam Data Platform server, a DHCP-enabled PCD network, and a dedicated security group.

What the move looks like

When you go ahead with the migration, it looks like this: You stand up PCD next to your existing Veeam Data Platform deployment, starting with one non-production tenant. vJailbreak converts that tenant's VMs so they boot on PCD ready to run. Backup jobs are created in Veeam Data Platform exactly as they are today, full restores land within your RTO, and cross-tenant restores stay cleanly isolated. Platform9 and Veeam are alongside your team throughout, and the Veeam integration is in from the start, not bolted on later.

Next step

Bring your current Veeam topology to a joint architecture review with the Platform9 and Veeam alliance teams. Your per-tenant layout maps to PCD's proxy-per-tenant model, and the review scopes the pilot to your first tenant in your own environment. Contact your Platform9 or Veeam representative to schedule.

Website:
https://platform9.com

Email:
info@platform9.com

Phone:
+1 650-898-7369

© 2026 Platform9. All Rights Reserved.