INDUSTRY'S FIRST ON-DEMAND DRAAS FOR THE ENTERPRISE PRIVATE AI ERA

Always ready.
Never idle.

Stop paying for idle compute. Protect your applications, your data, and your AI workloads with a **Pay-on-Activation** model that stays ready around the clock without sitting on your operating budget.

Replicate | Activate | Recover | Prove

THE CHALLENGE

DR fails on economics long before it fails on technology

Every organisation knows it needs disaster recovery. The reason so many run with partial coverage, stale runbooks, and untested failover is rarely ignorance — it is that the conventional model asks you to fund a second data centre for an event you hope never happens.

You pay for compute you never use

Standby capacity runs all year for an event measured in hours. The bill is certain; the benefit is contingent. That asymmetry is the single largest reason DR scope gets cut.

Coverage gets cut to fit the budget

When DR costs scale with protected estate, tier-two applications quietly fall out of scope — and reappear as the systems nobody could restore during the incident.

Ransomware changed what recovery means

Restoring quickly is no longer enough if you restore the malware with it. Recovery now requires immutability, clean-room restoration, and validated recovery points.

The AI stack has no DR plan

Model registries, training and inference data, vector stores, and serving endpoints have become production dependencies — and they sit outside most continuity plans.

Questions a continuity review will ask — and most estates answer poorly:

- When did you last complete a full failover test?
- What is your committed RPO and RTO, per application?
- Who recovers your model registry and inference data?
- Which tier-two applications are actually out of scope?
- Could you restore clean after a ransomware event?
- What does DR cost you in a year with no incident?

THE GAP

The problem was never whether DR is worth having. It was that the pricing model made full coverage unaffordable.

THE ANSWER

We changed the math

UPC DRaaS keeps replication warm and your RPO/RTO tiers committed at all times. You pay for storage and readiness continuously — and for heavy compute only when you actually activate DR or run a drill.

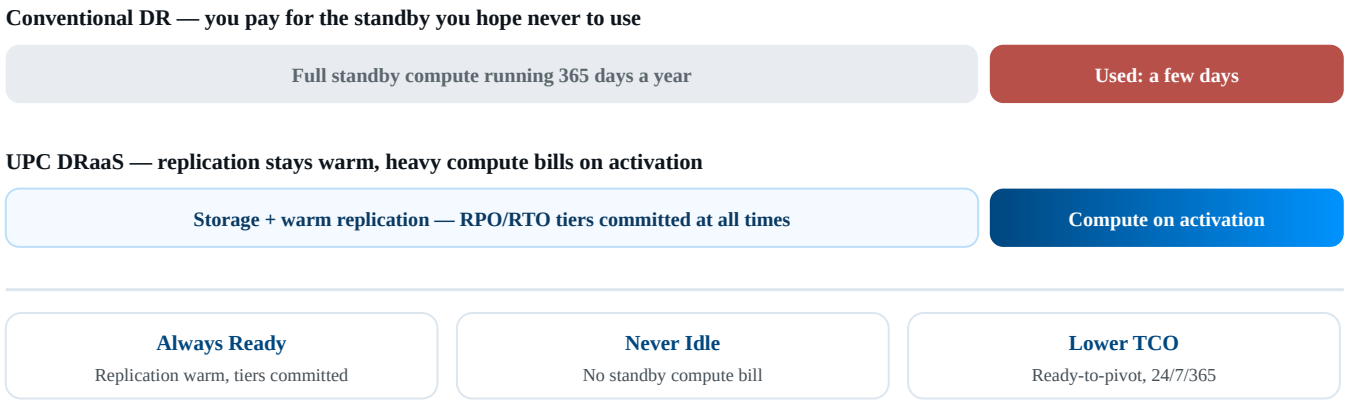

FIGURE — THE PAY-ON-ACTIVATION MODEL

Always ready, never idle

Replication stays warm and the tiers you subscribe to are committed around the clock. Readiness is not something you schedule — it is the resting state.

On-demand compute

You pay for the heavy-lifting compute only when you activate DR or run a drill, which removes the standing cost that forced trade-offs elsewhere.

Lower total cost

A substantially lower TCO while holding a ready-to-pivot stance 24/7/365 — which is what makes protecting the full estate viable rather than aspirational.

>30%
YoY saving vs hyperscale providers

50%
Better than on-premises DR

70%
Better than private cloud DR

30+
Global compliance standards

COMMITMENTS

Pick the tier each application deserves

Not every workload needs near-zero data loss, and paying as though it does is how DR budgets get consumed. Three tiers let you match commitment to business impact, application by application.

Platinum	Gold	Silver
RPO — DATA LOSS: Near-zero	RPO — DATA LOSS: < 15 minutes	RPO — DATA LOSS: < 1 hour
RTO — DOWNTIME: 15 minutes	RTO — DOWNTIME: 1 hour	RTO — DOWNTIME: 4 hours
SUITED TO: Mission-critical, revenue-bearing	SUITED TO: Core business applications	SUITED TO: Supporting and internal systems

RECOVERY TOPOLOGIES

Active-Active

Resiliency for mission-critical environments that require the lowest recovery time objectives, with both sites carrying live workload.

Active-Passive

A standby environment that can be put to work for test and development when it is not in disaster mode, rather than sitting unused.

Active-Replicated

For applications that are not mission-critical and need not be recovered instantly, held in a cold site at the lowest cost point.

POLICY-DRIVEN DR AND BACKUP MANAGEMENT

- Centralized backup policy
- Resource quota enforcement
- Multi-cloud backup
- Configurable alerts & notifications
- Role-based access management
- DR policy orchestration

SOLUTION SUITE

Four problems one platform solves

AI-Ready Resilience

Production-grade disaster recovery designed for the entire enterprise AI stack, not just the applications around it.

- Model registries & VLMs
- Training & inference data
- Full-stack observability
- AI delivery continuity

Immutable Defence

Advanced cyber resilience designed to protect the integrity of the entire environment, so recovery restores clean.

- Cyber recovery
- Immutability by default
- Model integrity protection
- Clean-room recovery

Strategic VMware Exit

Modernization should be an opportunity, not a disruption. A controlled bridge for transitioning away from legacy VMware environments.

- Seamless migration
- Migration-ready DR
- Modern hypervisor support
- Cloud-ready recovery

Powering Your Private AI Strategy

Disaster recovery is no longer standalone. It is a foundational layer of a broader enterprise private AI architecture.

- DR built-in
- Observability built-in
- AI-powered recovery
- Platform-level resilience

BUILT FOR ENTERPRISE RESILIENCE

Elastic cost model

Avoid idle DR infrastructure. Pay primarily for storage consumption and invoke additional on-demand services as required.

On-demand services

Provision virtual compute, firewalls, load balancers, point-to-point connectivity, and backup-as-a-service without relying on multiple vendors.

99.999% HA compute

True resilience with N+M high-availability compute, designed to keep compute running even under component failure.

Secure multi-tenancy

Run multiple workloads in secure, isolated environments on shared infrastructure, with tenant isolation and security controls.

Global availability

Delivered from Frankfurt, Germany and Santa Clara, California to enterprises across the globe.

24×7 security & expert support

Continuous monitoring and expert support ensure recovery readiness, enabling rapid and reliable execution during DR events.

SOLUTION AT A GLANCE

A software-defined platform, end to end

UPC DRaaS is delivered as a multitenant DRaaS and private-cloud platform built on software-defined networking, compute, and storage — with Direct Connect to Azure, AWS, and GCP available on demand.

Network

Software-defined networking supporting enterprise solutions from Cisco, Juniper, F5, Palo Alto, Citrix and others, on UnitedLayer's standard Core/Edge design. Two 500 Mbps managed virtual firewalls with IDS/IPS in high availability. 100 Mbps internet expandable to 10G or 100G. 1G Layer 2 secured connectivity between the customer data centre and the DRaaS region.

Compute

High-performance software-defined compute with high availability included. UPC multitenant DRaaS cloud with KVM. Virtual machines configurable using available UPC vCPU and vRAM, delivered on a vDC architecture where each organisation maps to one or more Org vDCs backed by UnitedLayer resource clusters.

Storage

Multi-tiered software-defined storage with high availability included, billed per front-end storage capacity. Enterprise Performance Storage included for currently utilised capacity, delivering 2,500 IOPS per TB up to 100K IOPS per LUN. Backup storage across primary and secondary sites available on demand.

Why it matters

Isolated vLANs and vLAN segmentation for tenant separation. A dedicated vDC with a built-in intelligent layer. Shared out-of-band management with secured access. A SOC-compliant secure private cloud. Internal connectivity built on 25G/40G with redundancy, and distribution, storage-replication, and management planes separated across dedicated switching tiers.

REFERENCE DESIGN

The preferred design uses **private Layer 2 connectivity** for replication and recovery traffic, with a virtual firewall providing secure external access between the customer site and the UPC DRaaS platform. An edge gateway bridges internal vApp networks to the external network, and management firewalls secure the management switch and out-of-band access.

SERVICE SPECIFICATIONS

What you are buying, in detail

SERVICE	SPECIFICATIONS	AVAILABILITY
United Private Cloud	AMD / Intel Xeon, Gen 2 / Gold processors respectively, with DDR4 RAM	99.99%
Storage EPS	2,500 IOPS per TB, up to 100K IOPS per LUN	99.99%
Backup / Management	Solution based on Veeam software licenses	99.99%
Firewall	Virtual firewall in high availability	99.99%
Internet	Dual-homed	99.99%

INFRASTRUCTURE VENDORS

Networking	Cisco, Juniper or equivalent
Security	Cisco, Palo Alto or equivalent
Compute nodes	Dell, Lenovo or equivalent
Storage nodes	Dell, Lenovo or equivalent

DATA CENTRE

Tier	Tier III
Generator redundancy	N + 1
UPS redundancy	2N
Cooling redundancy	N + 1
Certifications	ISO 14001 / 9001 / 27001, SOC 1 & 2

SLA MATRIX

SEVERITY	DEFINITION	TIER 1 RESPONSE	TIER 2 ENGAGEMENT	TARGETED RESOLUTION
P1 — Urgent	Severe business impact rendering services inoperative or causing catastrophic failure; no workaround	**15 mins**	**30 mins**	**3 hours**
P2 — High	An essential component is not performing as documented, creating significant operational impact	**15 mins**	**1 hour**	**4 hours**
P3 — Normal	A non-essential component is underperforming, with moderate or minor operational impact	**30 mins**	**2 hours**	**1 business day**
P4 — Normal	Questions on day-to-day usage or documentation; suggestions and enhancement requests	**30 mins**	**4 hours**	**7 business days**

WHY UPC DRAAS

Continuity you can afford to apply everywhere

The value of the Pay-on-Activation model is not only the saving. It is that removing the standing compute cost removes the reason to leave systems unprotected — which is what turns a partial DR plan into a complete one.

STAKEHOLDER	CHALLENGE	UPC DRAAS BENEFIT
CIO	DR budget competes with every other initiative	Full-estate protection at a materially lower total cost of ownership
CFO	Paying continuously for capacity that is never used	Storage and readiness billed continuously; heavy compute only on activation
Head of Infrastructure	Failover is rarely tested because drills are expensive	Drills use the same on-demand model, so testing becomes routine
CISO	Fast recovery can restore the ransomware with the data	Immutability by default, clean-room recovery, model integrity protection
Business continuity	RPO and RTO commitments are aspirational	Platinum, Gold, and Silver tiers committed at all times per application
Data & AI teams	The AI stack sits outside the continuity plan	Model registries, training and inference data, and serving covered
Compliance	Evidence of tested recoverability is hard to produce	SOC-compliant platform, 30+ standards, documented drill outcomes

BOTTOM LINE

Always ready, never idle — disaster recovery that stays committed 24/7/365 and bills for compute only when you need it.

Let's build your continuity plan.

Speak with a specialist, or ask us to model your RPO/RTO tiers and DR cost against your current estate.

UPC DRaaS™
UNITEDLAYER.COM

EMAIL
contact@unitedlayer.com

PHONE
+1-888-853-7733

X
x.com/unitedlayer

LINKEDIN
linkedin.com/company/unitedlay

Product positioning, specifications, service tiers, and comparative cost figures reflect UnitedLayer published materials for UPC DRaaS. Availability figures, regional coverage, vendor selections, and SLA targets vary by region, configuration, and contract, and should be confirmed for your deployment. Comparative savings are indicative and depend on estate profile and baseline. UnitedLayer®, United Private Cloud®, and UPC DRaaS™ are marks of UnitedLayer.

© 2026 UNITEDLAYER. ALL RIGHTS RESERVED.