



# Disaster Recovery

## Acronis Cyber Protect Cloud

Keep every workload online — in minutes — after an outage or attack. Use one console to protect, test and recover to the Acronis Cloud or to a partner's hybrid cloud or to Microsoft Azure.

Acronis enables you to deliver scalable, multicloud recovery services that support modern cyber resilience strategies.

1

### Right-sized tiers for any client

Cold, Warm (coming soon) and turnkey options cover low-cost protection through sub-15-minute SLAs. One console, any budget.

2

### Fastest recovery

Backup, cybersecurity, and DR share one agent and management portal, so failover starts in clicks and data stays in sync.

3

### Efficient delivery for MSPs

Multitenant portal, pay-as-you-go billing, and open APIs cut service overhead and raise margins.

## At a glance

- **All-in-one platform:** Backup, cybersecurity and disaster recovery from a single agent and UI.
- **Different clouds for different customers:** choose Acronis Cloud for turnkey recovery or Microsoft Azure for enterprise-grade infrastructure and customizations.
- **Two DR types for Azure:** Cost-efficient Cold DR and near zero RTO Warm DR (coming soon).
- **50+ Acronis data centers and 70+ Azure regions** help meet data sovereignty rules.
- **Pay-as-you-go pricing** — You only pay for consumed storage and compute.



## Disaster recovery options

Not all customers need the same DR plan. Pick the right target from the Acronis console.

- **Acronis Cloud** — Simple turnkey DR; no custom setup.
- **Hybrid Cloud** — Keep sensitive data under control.
- **Microsoft Azure** — Cold DR: Lowest cost; pay for compute only in a disaster.
- **Microsoft Azure** — Warm DR: Fast failover with near-zero RTO (coming soon).



## Acronis Disaster Recovery capabilities

General features (all DR targets)	Exclusive to DR to Azure
<ul style="list-style-type: none"> <li>▪ Single console and agent for backup and DR.</li> <li>▪ Drag-and-drop runbooks automate failover.</li> <li>▪ Test failovers with AI screenshot validation.</li> <li>▪ Incremental failback — workloads keep running while data syncs.</li> <li>▪ Multiple connectivity options: Site-to-site or point-to-site VPN, IPsec multisite VPN.</li> <li>▪ Support for 20+ physical, virtual, and cloud workloads.</li> <li>▪ Point-in-time recovery for any past backup.</li> <li>▪ Failover to a malware-free point to avoid reinfection.</li> <li>▪ One-click failover with Acronis EDR / XDR.</li> <li>▪ Real-time DR dashboard with RPO-compliance tracking.</li> <li>▪ Encrypted-backup support with AES-256.</li> <li>▪ Credential Store keeps passwords for encrypted backups.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Cold DR tier: store backups, pay for compute only in a disaster.</li> <li>▪ Warm DR tier: Incremental backup replication to Azure warm storage for near-zero RTO (coming soon).</li> <li>▪ Failover from existing backups stored in Azure, Acronis Cloud or partner-hosted storage.</li> <li>▪ On-demand workers — no always-on appliances.</li> <li>▪ Customers retain full control over Azure networking and connectivity, with the flexibility to leverage native Azure platform capabilities or bring their own custom solution.</li> <li>▪ Flat per-workload price, direct backups to Azure license included.</li> </ul>

## Why MSPs choose Acronis

- Single stack reduces costs with fewer tools, less training and lower billing overhead.
- Integrated solution cuts recovery time.
- Easy DR upsell with managed backup services.
- Prevent ransomware risk before failover is needed with integrated endpoint security.
- Pay only for what you use: storage (GB) and compute (vCPU / RAM hours).
- Azure CSP partners can grow Azure consumption and margin.
- Compliance-ready: ISO 27001, SOC 2, HIPAA, GDPR and PCI DSS aligned. AES 256 encryption at rest and in transit. Tier IV and Tier III data centers with 99.9% availability SLA.

Acronis Disaster Recovery adds powerful disaster recovery capabilities to Acronis Cyber Protect Cloud. It's an industry-first integration that enables service providers to deliver cybersecurity, data protection, file sync and share and endpoint management services through one integrated solution.