Acronis

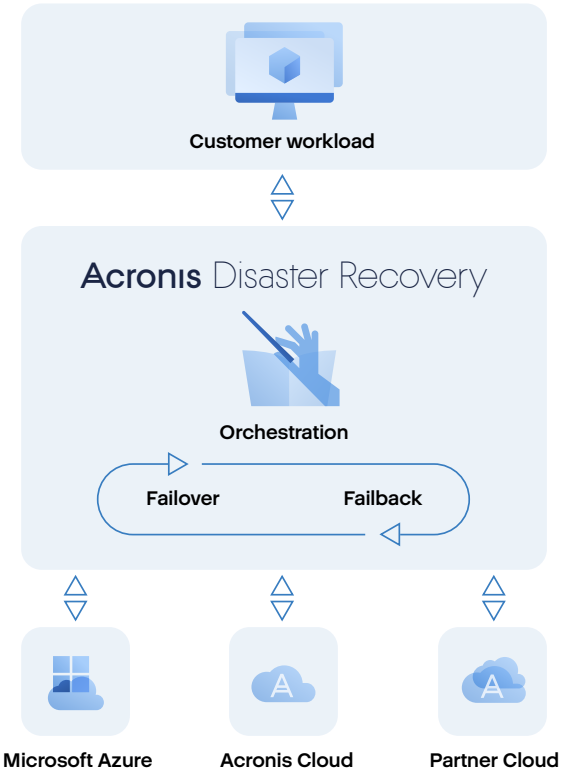
HIPAA COMPLIANT

Disaster Recovery

Acronis Cyber Protect Cloud

Bringen Sie alle Workloads im Falle eines Ausfalls oder Angriffs innerhalb weniger Minuten wieder online. Verwenden Sie eine einzige Konsole, um Daten zu schützen, zu testen und in der Acronis Cloud, in der Hybrid Cloud eines Partners oder in Microsoft Azure wiederherzustellen.

Acronis ermöglicht Ihnen die Bereitstellung skalierbarer Multi-Cloud-Recovery-Services, die moderne Cyber-Resilienz-Strategien unterstützen.



1

Passende Stufen für alle Kund:innen

Die Optionen „Cold", „Warm" (in Kürze verfügbar) und „Direkt einsetzbar" bieten kostengünstigen Schutz mit SLAs von unter 15 Minuten. Eine Konsole – jedes Budget.

2

Die schnellste Datenwiederherstellung

Backup, Cyber Security und Disaster Recovery werden über einen einzigen Agenten und ein einziges Management-Portal verwaltet. Dadurch ist ein Failover mit wenigen Klicks möglich und die Daten sind jederzeit synchronisiert.

3

Effiziente Bereitstellung für MSPs

Das mandantenfähige Portal, die nutzungsabhängige Abrechnung und die offenen APIs reduzieren die Servicekosten und steigern die Margen.

Auf einen Blick

- **All-in-one-Plattform:** Backup, Cyber Security und Disaster Recovery (DR) mit nur einem Agenten über eine einzige Benutzeroberfläche.
- **Unterschiedliche Clouds für unterschiedliche Kund:innen:** Wenn Sie ein direkt einsetzbares Recovery wünschen, ist die Acronis Cloud die richtige Wahl. Für Enterprise-Infrastrukturen und -Anpassungen wählen Sie Microsoft Azure.
- **Für Azure gibt es zwei DR-Typen:** das kosteneffiziente Cold DR und das Warm DR mit RTOs von nahezu null (bald verfügbar).
- **Mit mehr als 50 Acronis Datenzentren und über 70 Azure Regionen** können Sie die Datenhoheitsvorschriften einhalten.
- **Nutzungsabhängige Preise** – Sie zahlen nur für die tatsächlich verbrauchten Storage- und Computing-Ressourcen.

Disaster Recovery-Optionen

Nicht alle Kund:innen benötigen denselben DR-Plan. Wählen Sie das richtige Ziel in der Acronis Konsole.

- **Acronis Cloud** – einfache, direkt einsetzbare DR-Lösung; keine benutzerdefinierte Konfiguration erforderlich.
- **Hybrid Cloud** – sensible Daten bleiben unter Kontrolle.
- **Microsoft Azure** – Cold DR: geringste Kosten; Sie zahlen nur für die Computing-Ressourcen, wenn Sie ein Disaster Recovery benötigen.
- **Microsoft Azure** – Warm DR: Schnelles Failover mit RTOs von fast Null (bald verfügbar).

Acronis Disaster Recovery – Funktionsumfang

Allgemeine Funktionen (alle DR-Ziele)	Ausschließlich für DR in Azure
▪ Eine Konsole und ein Agent für Backup und DR. ▪ Drag-and-Drop-Runbooks automatisieren das Failover. ▪ Test-Failover mit KI-Screenshot-Validierung. ▪ Inkrementelles Failback – Workloads laufen weiter, während die Daten synchronisiert werden. ▪ Mehrere Konnektivitätsoptionen: Site-to-Site- oder Point-to-Site-VPN-Verbindung, IPsec-Multisite-VPN-Verbindung. ▪ Unterstützt mehr als 20 physische, virtuelle und Cloud-Workloads. ▪ Zeitpunktgenaue Wiederherstellung für jedes frühere Backup. ▪ Failover zu einem Malware-freien Zeitpunkt, um eine erneute Infektion zu vermeiden. ▪ One-Click Failover mit Acronis EDR bzw. XDR. ▪ Echtzeit-DR-Dashboard, das auch die RPO-Compliance überwacht. ▪ Unterstützt Backups, die mit AES-256 verschlüsselt sind. ▪ Im Anmeldespeicher werden Kennwörter für verschlüsselte Backups gespeichert.	▪ Cold DR-Stufe: Backups werden gespeichert, Computing-Ressourcen sind nur im DR-Fall zahlungspflichtig. ▪ Warm DR-Stufe: Inkrementelle Backup-Replikation in den Azure Warm Storage mit RTOs von fast Null (bald verfügbar). ▪ Failover von vorhandenen Backups, die in Azure, der Acronis Cloud oder einem vom Partner gehosteten Storage gespeichert sind. ▪ On-demand-Funktionalität – keine ständig aktiven Appliances. ▪ Die Kund:innen behalten die volle Kontrolle über die Netzwerkfunktionen und die Konnektivität von Azure. Sie können die nativen Funktionen der Azure-Plattform flexibel nutzen oder eigene benutzerdefinierte Lösungen einsetzen. ▪ Festpreis pro Workload, direkte Backups auf Azure-Lizenz inklusive.

Warum sich MSPs für Acronis entscheiden?

- Eine All-in-one-Lösung reduziert die Kosten, da weniger Einzel-Tools benötigt werden, der Schulungsaufwand sinkt und die Abrechnungskosten niedriger ausfallen.
- Eine integrierte Lösung verkürzt die Wiederherstellungszeit.
- Unkompliziertes Upselling von DR mit Managed Backup Services.
- Die integrierte Endpunktsicherheit bietet Schutz vor Ransomware, bevor ein Failover erforderlich wird.
- Sie bezahlen nur für das, was Sie tatsächlich nutzen: Speicherplatz (GB) und Computing-Ressourcen (vCPU/RAM-Stunden).
- Azure CSP-Partner können ihren Azure-Verbrauch und ihre Margen steigern.
- Erfüllt Compliance-Vorschriften: ISO 27001, SOC 2, HIPAA, DSGVO und PCI DSS. AES-256-Verschlüsselung im Storage und bei der Übertragung Tier-IV- und Tier-III-Datenzentren mit Verfügbarkeits-SLAs von 99,9 %.

Acronis Cyber Protect Cloud erhält mit Acronis Disaster Recovery leistungsstarke Disaster Recovery-Funktionen. Service Provider erhalten damit die branchenweit erste Integration, mit der sie ihre Services für Cyber Security, Data Protection, Dateisynchronisierung und -freigabe sowie Endpunktverwaltung in einer integrierten Lösung bereitstellen können.

Acronis

Weitere Informationen finden Sie auf www.acronis.com.