

Acronis Cyber Frame

Eine speziell für Service Provider entwickelte Lösung, die eine sichere, KI-gestützte hyperkonvergente Infrastruktur (HCI) und Infrastructure-as-a-Service (IaaS) bietet.



Die aktuellen Marktbedingungen im Infrastrukturbereich bieten Service Providern ideale Voraussetzungen, um ihr Geschäft auszubauen und den Umsatz zu steigern. Unternehmen suchen nach Alternativen zu VMware, verlagern Workloads von Hyperscalern zurück in andere Clouds und wechseln zu lokalen Cloud-Lösungen, um die Anforderungen an die Datenhoheit zu erfüllen.

Mit Acronis Cyber Frame können Service Provider IaaS-Services entweder über ihre eigene Infrastruktur oder über Acronis Datenzentren bereitstellen. Die Cyber Frame-VMs sind von Anfang an umfassend geschützt, da die nativ integrierten Cyber Protection-, Verwaltungs- und Automatisierungsfunktionen sofort standardmäßig aktiviert sind.

Eine Geschäftsplattform für Service Provider zur Bereitstellung von IaaS mit nativ integrierten Schutz-, Verwaltungs- und Automatisierungsfunktionen



Individuelle IaaS-Bereitstellung

- Stellen Sie virtuelle Maschinen, Netzwerke und Storage bereit
- Unterstützung von durch Service Provider oder Acronis gehosteten Bereitstellungsmodellen
- Basierend auf der Virtuozzo-Infrastruktur mit optimierter OpenStack-Version und KVM
- Keine Bindung an proprietäre Hypervisoren durch Open-Source-Technologien
- Unterstützung für schrittweise Migrationen und gleichzeitige Nutzung mit bestehenden Umgebungen



Integrierter Schutz von Anfang an

- Integriertes Backup für Cyber Frame-VMs
- Integriertes Disaster Recovery mit Failover und Failback
- Integrierte Sicherheitsfunktionen (z. B. Malware- und Ransomware-Schutz, Verhaltensüberwachung, EDR)
- Integriertes RMM-Tool (Remote Monitoring and Management)
- KI-Assistent zur Unterstützung bei Bereitstellung, Konfiguration und täglichem Betrieb



Speziell für Service Provider

- Native Mandantenfähigkeit mit Mandantenisolierung
- Kundenseitige Self-Service-Funktionen zur Bereitstellung von Infrastrukturrressourcen
- Integration mit Acronis PSA sowie PSA-Tools von Drittanbietern für Abrechnung und Betrieb
- Integration mit Acronis RMM sowie RMM-Tools von Drittanbietern
- Unterstützung für die White-Labeling-Bereitstellung als Teil der Acronis MSP-Plattform

Marktchancen nutzen und Ihr IaaS-Geschäft ausbauen

Ersatz für VMware

Modernisieren Sie vSphere-Umgebungen und vermeiden Sie steigende Lizenzkosten durch eine schnelle und sichere Migration.

Hyperscaler-Repatriierung

Unterstützen Sie Unternehmen dabei, ihre Workloads von Hyperscalern in andere Cloud-Umgebungen zu migrieren. So werden die Kosten wieder vorhersehbar und es wird lokale Kontrolle erlangt.

IaaS inklusive Datenhoheit

Erfüllen Sie die steigenden Anforderungen an die regionale Datenaufbewahrung und die immer strengeren Compliance-Vorschriften in der EU, in Kanada und in Lateinamerika.

Eigene Cloud-Lösung

Entwickeln Sie eine sichere, mandantenfähige IaaS-Plattform unter Ihrer eigenen Marke, um höhere Margen zu erzielen.

Profitabler Weiterverkauf von IaaS

Bieten Sie Cloud-Services auf Basis eines nutzungsabhängigen Abrechnungsmodells über die von Acronis gehostete Cyber Frame Cloud an.

Maximierung der IaaS-Rentabilität

40 %

niedrigere Gesamtbetriebskosten für Service Provider im Vergleich zu veralteten Plattformen

92.000 \$

Kostensparnis im Vergleich zur Nutzung von VMware innerhalb von drei Jahren

40 % gegenüber 5-10 %

Bruttomarge beim Weiterverkauf von Cyber Frame Cloud im Vergleich zu Hyperscalern

Kernfunktionen

Bereitstellung von VMs, Netzwerken und Storage

Über eine zentrale Konsole können Sie VMs, Netzwerke und Storage bereitstellen und verwalten. Dabei ist eine flexible Zuweisung von vCPUs, vRAM sowie IP-Adressen bzw. VPNs möglich.

Mandantenfähige Architektur für Service Provider

Die sichere Mandantenisolierung ermöglicht Service Providern, mehrere Kundenunternehmen über eine gemeinsam genutzte Infrastruktur zu unterstützen. Dadurch kann die Ressourcennutzung optimiert und der Zugriff über eine einheitliche Management-Konsole delegiert werden.

Kundenseitige Self-Service-Funktionen

Ermöglichen Sie Kundenunternehmen, Ressourcen innerhalb der vom Service Provider festgelegten Grenzen bereitzustellen und zu verwalten. Unterstützen Sie eine leicht umsetzbare Service-Bereitstellung, während gleichzeitig volle Kontrolle und Richtlinienhoheit gewährleistet sind.

Automatisierte IaaS-Bereitstellung über OpenStack-API

Automatisieren Sie das Lebenszyklusmanagement von VMs, Netzwerken und Storage-Systemen mithilfe OpenStack-kompatibler Tools wie Terraform.

Integriertes Backup und Disaster Recovery

Schützen Sie alle VMs mit nativen Backup- und integrierten Disaster Recovery-Funktionen. Dazu stehen sowohl agentenlose als auch agentenbasierte Optionen zur Verfügung. Unterstützen Sie die vollständige Wiederherstellung von VMs, Failover und Failback sowie plattformübergreifende Wiederherstellungen.

Integrierte Sicherheit und RMM

Zentrale Richtlinien für die Erkennung von Malware und Ransomware sowie für die verhaltensbasierte Erkennung können auf alle VMs angewendet werden. Überwachen Sie alle Systeme über das integrierte RMM direkt in der Acronis Konsole.

Tools für VMware-Migrationen

Migrieren Sie VMware-Workloads mithilfe integrierter Workflows, die sowohl die Validierung als auch das Rollback unterstützen.

PSA-Integrationen von Acronis und Drittanbietern

Nutzen Sie die PSA-Integrationen von Acronis und Drittanbietern für Abrechnung, Berichterstellung und Betrieb.

Acronis KI-Assistent unterstützt den Betrieb

Nutzen Sie den integrierten KI-Assistenten, um in Echtzeit Konfigurationshinweise und Betriebsempfehlungen zu erhalten.

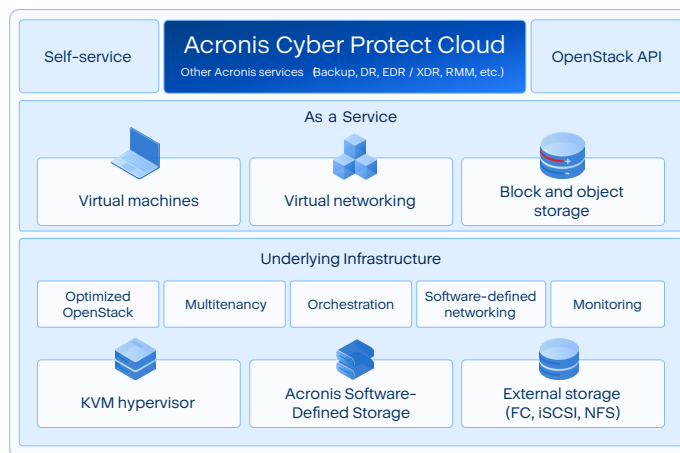
Architekturüberblick

Überblick: Acronis Cyber Frame ist ein mehrschichtiger Infrastrukturservice, der für Service Provider optimiert wurde und nahtlos in die zentrale Konsole der Acronis Cyber Protect Cloud integriert ist.

Wichtige Produktkomponenten: Die Plattform basiert auf einer geclusterten HCI-Ebene mit Multinode-KVM-Computing und Software-definiertem Acronis Storage. Unterstützt werden Hochleistungs-Block-Storage und S3-kompatibler Objekt-Storage. Optional ist auch die Integration externer Storage-Lösungen (FC, iSCSI, NFS) möglich.

Grundinfrastruktur: Die Orchestrierung, Planung und Automatisierung erfolgt über eine optimierte OpenStack-Steuerungsebene. Darüber hinaus bietet Cyber Frame native Mandantenfähigkeit, Software-definierte Netzwerke (SDNs) sowie Day-2-Vorgänge für den Alltagsbetrieb.

Als Service: Die Plattform bietet Infrastructure-as-a-Service zur Bereitstellung von VMs, Netzwerken und Storage-Ebenen mit festgelegten Quotas.



Acronis Cyber Protect Cloud: Alle Prozesse werden in derselben Umgebung ausgeführt wie die Backup-, Sicherheits- und Verwaltungsdienste von Acronis. Backup, Disaster Recovery, Sicherheit und RMM sind standardmäßig in den Lebenszyklus der Workloads integriert.

In zwei Editionen verfügbar

Cyber Frame bietet zwei Bereitstellungsoptionen, um verschiedene Service Provider-Modelle zu unterstützen.

Cyber Frame Cloud

Die IaaS-Bereitstellung erfolgt direkt aus regionalen Acronis Datenzentren. Dadurch ist eine sofortige Bereitstellung von VMs, Netzwerken und Storage ohne eigene Hardware möglich. Die Abrechnung erfolgt nutzungsabhängig und es sind integrierte Schutzfunktionen vorhanden.

Von Acronis gehostete Infrastruktur

- Keine Hardware oder Datenzentren erforderlich
- Nutzungsabhängige Abrechnung
- Schnelle Aktivierung und rasche Umsatzgenerierung
- Integrierte Backup-, Disaster Recovery-, Sicherheits- und RMM-Funktionen für Cyber Frame-VMs
- 35 regionale Acronis Datenzentren
- Ideale Lösung für Partner zum IaaS-Einstieg oder -Ausbau ohne Kapitalkosten

Cyber Frame Local

Service Provider können damit ihre eigene mandantenfähige IaaS-Lösung auf handelsüblicher x86-Hardware betreiben. Dadurch haben sie die volle Kontrolle über die Infrastruktur, die Kosten und die langfristigen Margen. Local bietet native Mandantenisolierung, Abonnements auf Kern- und Storage-Ebene sowie VMware-Migrationstools. Für die Zukunft werden hohe Bruttomargen und ein hoher ROI prognostiziert.

MSP-gehostete Infrastruktur

- Bereitstellung auf Ihrer eigenen Hardware oder Colocation-Option
- Abonnement pro physischem Kern und Storage
- Volle Kontrolle über die Performance und den Speicherort
- Integrierte Backup-, Disaster Recovery-, Sicherheits- und RMM-Funktionen für Cyber Frame-VMs
- Für Cluster mit fünf oder mehr Nodes entwickelt
- Ideale Lösung für Partner mit langfristigem Interesse am Infrastrukturmarkt

Voraussetzungen für die Bereitstellung von Cyber Frame Local

Unter der Voraussetzung, dass sie die Hardware- und Netzwerkanforderungen von Cyber Frame erfüllen, können die meisten VMware-Hardwarekomponenten wiederverwendet werden. Um eine SLA von bis zu 99,95 % zu erreichen, sollten Umgebungen die folgenden Mindestanforderungen erfüllen:

- VMware-Hardware gemäß den Cyber Frame-Spezifikationen
- Empfohlener Arbeitsspeicher: 512 GB (Produktivumgebung) bzw. 256 GB (Testumgebung).

- Firewall: pfSense oder ein modernes Gerät mit Unterstützung für NAT, VPN und Lastverteilung
- Server: mindestens fünf (drei für Test bzw. Proof-of-Concept), CPU mit 24 Kernen, Kompatibilität mit RHEL 7/9, Virtualisierungs-Flags aktiviert, redundante/Hot-Plug-Stromversorgung
- Netzwerk: konfigurierte VLANs, Switches mit 802.3ad-Unterstützung, Jumbo-Frames (MTU 9000), L2-Konnektivität, kompatible Netzwerkkarten, zwei 25-Gbit-Ports (vier für RDMA) sowie Remote-IPMI-Zugriff
- Laufwerke: Enterprise-Klasse, DWPD ≥ 10 , mindestens eine SSD/HDD/NVMe als Storage, zwei SSD/NVMe (RAID 1, mindestens 200 GB) für Betriebssystem und MDS
- Internet: zwei Anbieter mit 1-Gigabit-Verbindungen

Migration von VMware oder Public Clouds

Mit Cyber Frame lassen sich Workloads schrittweise und mit minimalen Störungen migrieren. Dazu stehen mehrere Migrationsoptionen zur Verfügung:



Integrierter VMware- und Azure-Migrationsassistent:

Automatisiert die Massenmigration für gesamte Hosts oder ausgewählte VMs direkt zu Cyber Frame.



Backup-basierte Migration:

Ermöglicht die Wiederherstellung eines Backups von VMware- oder Public Cloud-VMs in Cyber Frame. Hinweis: Der Cyber Frame-Agent muss Zugriff auf den Speicherort des Backups haben.



Konvertierung in eine VM:

Mit dieser Funktion können VMware-basierte Backups schrittweise in bootfähige VMs innerhalb von Cyber Frame konvertiert werden. Ein Zugriff auf die ursprüngliche VMware-Infrastruktur ist dafür nicht notwendig.

Wichtige Vorteile im Vergleich zu Konkurrenzprodukten

VMware vSphere

- Cyber Frame bietet niedrigere Gesamtkosten, einen höheren ROI und integrierte Backup-, Sicherheits- sowie RMM-Funktionen.
- Native Mandantenfähigkeit, die speziell für Service Provider entwickelt wurde, ohne dass vCloud Director-Add-ons erforderlich sind.
- Dank der OpenStack- und KVM-Architektur besteht keine Bindung an proprietäre Hypervisoren.

Hyperscaler (AWS, Azure, GCP)

- Cyber Frame bietet eine Bruttomarge von 40–45 % im Vergleich zu einer Wiederverkaufsmarge von 5–10 % bei Hyperscalern.
- Die Kosten sind vorhersehbar, es gibt keine versteckten API- oder Ingress-Gebühren.

- Service Provider haben bei lokalen und selbstverwalteten Bereitstellungsoptionen die vollständige Kontrolle.

Nutanix / HPE GreenLake

- Cyber Frame wurde speziell für Service Provider und nicht für die Unternehmens-IT entwickelt.
- Es sind standardmäßig Cyber Protection-Funktionen integriert.
- Es gibt zwei flexible Bereitstellungsoptionen: Cloud oder vom Service Provider gehostet (Local).

Open-Source-Plattformen (OpenStack, Proxmox)

- Cyber Frame bietet Partnern Enterprise-Support und kommerzielle Unterstützung.
- Backup-, Sicherheits- und RMM-Funktionen sind bereits nativ integriert (keine separate Integration erforderlich).
- Die Lösung kann direkt eingesetzt werden und ist mandantenfähig (keine individuellen Architekturanpassungen erforderlich).

Erfahren Sie mehr und legen Sie mit Acronis Cyber Frame los

Bieten Sie IaaS zu Ihren eigenen Bedingungen an

