Acronis Cyber Frame

A secure, AI-powered hyperconverged infrastructure (HCI) and infrastructure-as-a-service (IaaS) solution for service providers

Today's infrastructure market conditions are prime for service providers to expand their business and increase revenues. Customers seek alternatives to VMware, repatriating workloads from hyperscalers and moving to local cloud solutions to meet sovereignty requirements.

Acronis Cyber Frame enables service providers to deliver IaaS services using either their own infrastructure or Acronis data centers. Cyber Frame VMs are protected by default, with natively integrated cyber protection, management and automation enabled from day one.

A business engine for service providers to deliver IaaS with natively integrated cyber protection management and automation

Deliver IaaS on your terms

- Provision virtual machines, networks and storage.
- Support service provider-hosted and Acronis-hosted deployment models.
- Built on Virtuozzo Infrastructure with optimized OpenStack and KVM.
- No proprietary hypervisor lock in — uses open-source technologies.
- Support phased migration and coexistence with existing environments.

Protected by default

- Built-in backup for Cyber Frame virtual machines.
- Integrated disaster recovery with failover and failback.
- Built-in security including anti-malware, anti-ransomware, behavioral detection and EDR.
- Built-in remote monitoring and management (RMM).
- AI assistant for guidance on deployment, configuration and daily operations.

Built for service providers

- Native multitenancy with tenant isolation.
- Customer self-service for provisioning infrastructure resources.
- Integration with Acronis and third-party PSA systems for billing and operations.
- Integration with Acronis and third-party RMM tools.
- Support for white-label delivery as part of the Acronis MSP platform.

Realize market opportunities and build your IaaS business

Replace VMware

Modernize vSphere environments and avoid rising licensing costs with fast, protected migration.

Repatriate from hyperscalers

Support customers repatriating workloads from hyperscalers to regain predictable pricing and local control.

Offer sovereign IaaS

Meet growing regional data residency and compliance needs across the EU, Canada and Latin America.

Build your cloud

Create a secure, multitenant IaaS platform under your brand with higher margins.

Resell IaaS profitably

Deliver cloud services using Acronis-hosted Cyber Frame Cloud on a pay-as-you-go model.

Maximize IaaS profitability

40%+

TCO improvement for service providers vs. legacy platforms.

$92K

savings vs. VMware over three years.

40% vs. 5%–10%

gross margin for Cyber Frame Cloud resale compared to hyperscalers.

Key features

Provisioning of VMs, networks and storage

Provision and manage VMs, networks and storage from a central console with flexible vCPU, vRAM and IP / VPN assignment.

Multitenant architecture built for service providers

Run multiple customers on shared infrastructure with secure tenant isolation. Optimize resource usage and delegate access from a unified management console.

Customer self-service

Let customers provision and manage resources within provider-defined limits. Support low-touch service delivery while retaining full governance and policy control.

IaaS provisioning automation through OpenStack API

Automate VM, network and storage lifecycle management using OpenStack-compatible tools like Terraform.

Built-in backup and disaster recovery

Protect all VMs with native backup and integrated disaster recovery, including agentless or agent-based options. Support full VM restore, failover or failback and cross-platform recovery.

Integrated security and RMM

Apply centralized anti-malware, anti-ransomware and behavior-based detection policies across all VMs. Monitor systems through built-in RMM directly in the Acronis console.

VMware migration tools

Migrate VMware workloads using built-in workflows with validation and rollback support.

PSA and ecosystem third-party integrations

Connect with Acronis and third-party PSA integrations for billing, reporting and operations.

Acronis AI for operational guidance

Use the built-in AI assistant to get real-time configuration guidance and operational recommendations.

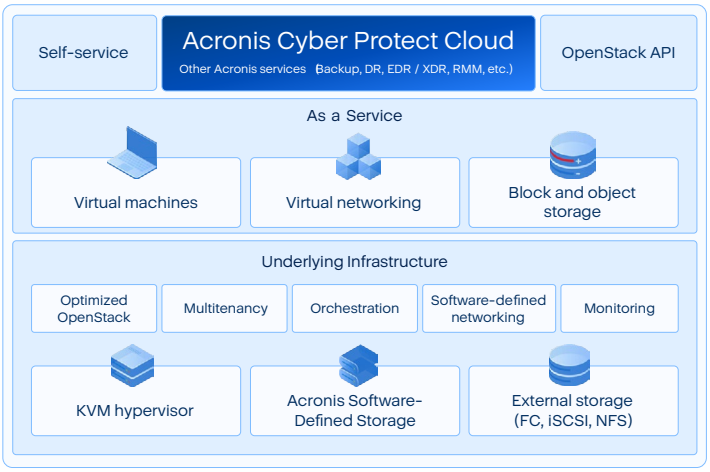
Architecture overview

Overview: Acronis Cyber Frame is a layered, service-provider-ready infrastructure stack built into the Acronis Cyber Protect Cloud console.

Key product components: The platform is based on a clustered HCI layer with multinode KVM compute and Acronis software-defined storage. It supports high-performance block storage and S3-compatible object storage, plus optional external storage integration (FC, iSCSI, NFS).

Underlying infrastructure: An optimized OpenStack control plane handles orchestration, scheduling and automation. It also delivers native multitenancy, SDN and day-two operations.

As-a-service: The platform provides infrastructure-as-a-service for provisioning VMs, networks and tiered storage within quotas.



Acronis Cyber Protect Cloud: All operations run in the same environment as Acronis backup, security and management services. Backup, DR, security and RMM are integrated into the workload lifecycle by default.

Available in two editions

Cyber Frame offers two deployment options to fit different service-provider models.

Cyber Frame Cloud

Delivers IaaS directly from Acronis regional data centers, enabling instant VM, network and storage provisioning without owning hardware, with consumption-based pricing and built-in protection tools.

Acronis-hosted infrastructure

- No hardware or data center required.
- Pay-as-you-go consumption model.
- Fast activation and time to revenue.
- Built-in backup, DR, security and RMM for Cyber Frame VMs.
- 35 regional Acronis data centers.
- Ideal for partners starting or expanding IaaS without CapEx.

Cyber Frame Local

Allows providers to run their own multitenant IaaS on commodity x86 hardware, giving them full control over infrastructure, costs and long-term margins. Local includes native tenant isolation, per-core and storage subscriptions, VMware migration tools, and strong projected economics such as high gross margins and ROI.

MSP-hosted infrastructure

- Deploy on your own hardware or colocation.
- Subscription per physical core and storage.
- Full control over performance and location.
- Built-in backup, DR, security, RMM for Cyber Frame VMs.
- Designed for five-node or larger clusters.
- Ideal for partners building a long-term infrastructure business.

Prerequisites for Local edition deployment

Most VMware hardware can be reused if it meets Cyber Frame hardware and network requirements. To achieve up to 99.95% SLA, environments should meet the following baseline recommended requirements:

- VMware hardware meeting Cyber Frame specs.
- Recommended memory: 512 GB (Production), 256 GB (Staging).
- Firewall: pfSense or modern device supporting NAT, VPN, load balancing.
- Servers: At least five (three for staging / POC), 24-core CPU, RHEL7/9 compatibility, virtualization flags enabled, redundant / hot-plug power.
- Network: Configured VLANs, switches supporting 802.3ad, jumbo frames (MTU 9000), L2 connectivity, compatible NICs, 2 x 25G ports (4 for RDMA), remote IPMI access.
- Drives: Enterprise-grade, DWPD ≥ 10, at least one SSD / HDD / NVMe for storage, two SSD / NVMe (RAID1, min. 200 GB) for OS+MDS.
- Internet: Two providers with 1G connections.

Migration from VMware or public clouds

Cyber Frame supports multiple migration paths to move workloads gradually and with minimal disruption:

Built-in VMware and Azure migration wizard: Automates bulk migration for entire hosts or selected VMs directly into Cyber Frame.

Backup-based migration: Restore a VMware or public cloud VM backup into Cyber Frame. Note: The backup location must be accessible to the Cyber Frame agent.

Convert to VM feature: Perform incremental conversion of VMware-based backups into bootable VMs inside Cyber Frame without needing access to the original VMware infrastructure.

Key advantages vs. competitors

Vs. VMware vSphere

- Lower total cost and higher ROI with built-in backup, security and RMM.
- Native multitenancy built for service providers; no vCloud Director add ons.
- OpenStack and KVM foundation with no proprietary hypervisor lock in.

Vs. hyperscalers (AWS / Azure / GCP)

- 40%–45% gross margin vs. 5%–10% resale margin.
- Predictable pricing with no hidden API or ingress fees.
- Local and sovereign deployment options; full service provider control.

Vs. Nutanix / HPE GreenLake

- Purpose built for service providers, not enterprise IT.
- Integrated cyber protection included by default.
- Flexible cloud or service provider-hosted deployment model.

Vs. open-source platforms (OpenStack, Proxmox)

- Enterprise support and commercial backing.
- Built-in backup, security and RMM; no separate integration required.
- Turnkey multitenant design; no custom architecture effort.

Learn more and get started with Acronis Cyber Frame

Deliver IaaS on your own terms

Acronis

Learn more at
acronis.com