



Acronis

SOTERIA CLOUD WHITE PAPER

From virtualisation platform to protected IaaS business

A practical framework for evaluating Acronis Cyber Frame across architecture, migration, protection, operations and service economics.



For service providers, the infrastructure decision is no longer only about which hypervisor runs a workload. It is about how quickly the provider can launch a trustworthy service, preserve operational control, protect every VM and build an economic model that scales.

Audience: MSP, CSP and hosting-provider leaders; infrastructure architects; product owners; commercial decision-makers.

Executive summary

Acronis Cyber Frame is a secure HCI and IaaS platform designed around service-provider delivery. It combines compute, software-defined storage, networking and optimised OpenStack orchestration with Acronis cyber protection and management services. The strategic value lies in joining the infrastructure layer to the service model.

The decision Cyber Frame is designed to support

A provider can start through Cyber Frame Cloud, where Acronis hosts the infrastructure, or deploy Cyber Frame Local on qualified provider-controlled infrastructure. This creates a path from rapid market entry to deeper infrastructure ownership without changing the central Acronis service motion.

Five questions should lead the evaluation

- Which workloads and customer segments justify a new infrastructure offer?
- Is speed to market or infrastructure ownership the stronger near-term priority?
- Which protection, recovery and management outcomes belong in the base service?
- What migration method best matches downtime tolerance and source-platform access?
- How will the provider package, meter, support and improve the service over time?

Core conclusion: Evaluate Cyber Frame as a protected IaaS service platform, not as a standalone hypervisor replacement. The business case becomes clearer when infrastructure, protection, migration, operations and customer experience are modelled together.

Why the infrastructure market has reopened

Three forces are causing customers and providers to reconsider where workloads live: changes in legacy virtualisation economics, the operational and cost complexity of hyperscale cloud, and rising demand for regional or sovereign infrastructure choices.



The opportunity is larger than a platform replacement

A simple lift-and-shift can reduce one cost while preserving a fragmented service model. A stronger response is to package infrastructure with a clear protection baseline, recoverability options, operational visibility, customer self-service and accountable support. That is where a provider can differentiate from both unmanaged infrastructure and low-margin resale.

Acronis positions Cyber Frame for VMware replacement, hyperscaler repatriation, provider-cloud creation, sovereign IaaS and local hosting of private AI workloads. These use cases share a common need: predictable infrastructure delivered through a trusted service relationship.

South African context

Regional performance, POPIA-aware data governance and commercial predictability are common buying considerations in South Africa. Acronis lists Johannesburg among example Cyber Frame Cloud locations. That is relevant, but it should never be turned into an automatic data-residency or compliance claim: the actual location, service scope, contractual chain and technical design must be verified for each customer.

Architecture and deployment models

Cyber Frame is a layered infrastructure stack integrated into the Acronis Cyber Protect Cloud management plane.

Foundation and control plane

- KVM-based compute, Acronis software-defined storage and software-defined networking form the HCI foundation.
- Optimised OpenStack handles orchestration, scheduling, multitenancy and automation across compute, network and storage.
- OpenStack-compatible APIs can support infrastructure automation and tools such as Terraform.
- Provider-defined quotas, delegated access and customer self-service support low-touch service delivery with retained governance.

Architecture decision	Cloud edition	Local edition
Underlying infrastructure	Acronis-hosted regional infrastructure	Qualified x86 cluster operated by the provider
Investment profile	Consumption-led and no initial hardware deployment	Infrastructure investment with greater long-term control
Operational ownership	Acronis operates the infrastructure layer	Provider owns cluster lifecycle, capacity and local operations
Minimum local footprint	Not applicable to the partner	Three nodes minimum; Acronis recommends five or more for production

Architecture discipline: Local edition sizing, network design, failure domains, storage media, supportability and operational skills require formal technical validation. Do not treat minimum specifications as a production design.

Migration without a cliff-edge

The migration method should be chosen per workload, not per campaign slogan. Cyber Frame supports multiple paths so providers can balance speed, validation and disruption.

1. **Discover and classify.** Map applications, owners, dependencies, network flows, data volumes, recovery objectives, maintenance windows and source-platform constraints.
2. **Select the migration path.** Use direct bulk migration for supported environments and faster cutover; staged or backup-based migration for validation and synchronisation; selective restore for pilots and individual workloads.
3. **Build the target service.** Define VM sizes, network zones, identity, quotas, backup policy, security policy, monitoring, DR tier and customer access before cutover.
4. **Prove recoverability.** Test backup, restore, failover where applicable, monitoring and escalation. A successful boot is not the same as a proven business service.
5. **Cut over with rollback criteria.** Agree decision points, communication, data synchronisation, fallback and acceptance checks before the production window.

Coexistence is a valid strategy

Providers do not need to force every workload into one wave. New customer workloads, development environments or a defined application group can establish the operating model first. Legacy platforms can then be reduced as confidence, automation and customer demand grow.

Protection and operations belong in the design

Cyber Frame's differentiation comes from connecting the infrastructure lifecycle to cyber protection and service operations inside the broader Acronis platform.

Service layer	Design question	Evidence to produce
Backup	Which workloads, frequency, retention, storage location and restore targets are required?	Protection-plan baseline and successful restore evidence
Disaster recovery	Which applications require failover, what RPO/RTO is promised and who operates the event?	Test schedule, runbook, network design and acceptance result
Security	Which anti-malware, behavioural, EDR/XDR or managed response capabilities are included?	Policy set, licensing statement and escalation workflow
RMM and monitoring	Who owns alerts, patching, capacity, guest-OS health and customer communication?	Responsibility matrix, thresholds and service reporting
Billing and PSA	How are usage, changes, incidents and service entitlements reconciled?	Metering model, product catalogue and workflow integration

Packaging rule: Do not use 'protected by default' as a substitute for a service definition. State which capabilities are included, which are optional or separately billed, who operates them and what outcome the customer can expect.

Design the commercial service around outcomes

A reusable service catalogue gives sales, operations and customers the same understanding of what is being bought.

Suggested Soteria service architecture

- Core IaaS: VM, storage, network, portal access, standard monitoring and defined support.
- Protected IaaS: Core IaaS plus backup, security baseline, protection reporting and restore assistance.
- Resilient IaaS: Protected IaaS plus designed DR, regular testing and documented recovery objectives.
- Managed Platform: Resilient IaaS plus patching, advanced monitoring, capacity management, change support and service reviews.

Use economic claims responsibly

Acronis publishes illustrative margin and ROI scenarios for Cyber Frame Cloud and Local. These can be useful as modelling inputs, but they are not forecasts. Actual outcomes depend on utilisation, partner pricing, hardware, data-centre cost, service labour, customer mix, protection add-ons and support scope. Build the provider's own model and stress-test low, expected and high utilisation cases.

Commercial evidence: Approve the offer only when the team can explain unit cost, target margin, oversubscription rules, capacity triggers, support effort, migration cost, contractual exclusions and the customer's measurable outcome.

A practical adoption roadmap

A good Cyber Frame launch moves through governed decisions, not technology enthusiasm alone.

1. **Opportunity brief.** Define target customers, source platforms, workloads, regional needs and the commercial problem the service will solve.
2. **Architecture gate.** Validate edition, sizing, networking, storage, identity, protection, recovery, observability and operational ownership.
3. **Business-case gate.** Model pricing, utilisation, service labour, migration cost, support and margin under multiple scenarios.
4. **Proof of concept.** Use representative workloads and test performance, migration, protection, restore, customer access and billing evidence.
5. **Controlled launch.** Start with a defined service catalogue, acceptance criteria, runbooks, monitoring and an escalation path.
6. **Quarterly optimisation.** Review capacity, protection success, support effort, customer adoption and margin; then adjust tiers and automation.

Next decision

Use Soteria Cloud to structure the workload assessment, deployment route, proof-of-concept scope and partner-ready service catalogue.

[Ask AB about Cyber Frame](#)

Sources and product notes

1. Acronis Cyber Frame product page - [official source](#)
2. Acronis Cyber Frame service-provider data sheet - [official source](#)
3. Acronis Cyber Frame Cloud end-client data sheet - [official source](#)
4. Acronis Cyber Frame general availability announcement - [official source](#)
5. Acronis Cyber Protect Cloud 26.05 release notes - [official source](#)
6. Acronis Cyber Frame administrator documentation - [official source](#)
7. Protection of Personal Information Act 4 of 2013 - [official source](#)
8. South African Information Regulator - POPIA - [official source](#)

Sources reviewed 24 August 2026. Acronis product capability, licensing and availability may change. Verify current official documentation before publication or contracting.