WHITE PAPER · ENTERPRISE BACKUP & RECOVERY

COMPETITIVE ANALYSIS

Managed Bacula Enterprise vs. Acronis Cyber Protect

Enterprise backup without vendor lock-in, open-format storage, and security that Acronis does not enforce by architecture

How faaleoleo.io delivers Bacula Enterprise capabilities — hardened, encrypted, and compliance-ready — without the per-workload and per-GB cost model that makes Acronis expensive at scale.

A technical and commercial comparison of faaleoleo.io Managed Bacula Enterprise and Acronis Cyber Protect — covering security defaults, platform coverage, compliance readiness, vendor lock-in, and total cost of ownership.

PREPARED BY	SOLUTION	VERSION
faaleoleo	**Bacula Enterprise**	**1.0**

CONTENTS

Executive Summary

Acronis has built significant market presence in the SMB and mid-market backup space, bundling backup with anti-malware, endpoint detection, and cloud storage in a single agent. These are real capabilities — but they come at compounding cost as infrastructure grows, rely on a proprietary .tibx format that creates deep data portability risk, and place security on behavioural detection rather than architectural enforcement. Acronis's own 2023 data exposure incident raised direct questions about the security posture of a vendor selling cybersecurity alongside backup.

THIS WHITE PAPER IN THREE POINTS

- **Security by architecture, not by bundle.** Every faaleoleo.io installation ships with hardened, AES-256-encrypted repositories as a mandatory default. Bacula Enterprise's architecture structurally prevents compromised clients from reaching backup data. Acronis's Active Protection detects ransomware behaviour after the fact — it does not prevent a compromised system from accessing the backup agent and data path. Acronis's 2023 incident, in which customer data was exposed via compromised credentials, demonstrates that bundling cybersecurity features and practising structural security are different things.
- **Broader platform and plugin coverage.** Bacula Enterprise covers every production platform with dedicated plugins — including KVM, Proxmox, Nutanix AHV, OpenStack, Kubernetes, OpenShift, HPC, tape libraries, and mainframe. Acronis's strength is Windows workloads, VMware, and cloud VMs. Linux support exists but is secondary. Outside Windows and VMware, coverage is limited or relies on generic file-level agents rather than application-aware plugins.
- **Predictable costs, open format.** Acronis pricing compounds at scale: per-workload fees plus per-GB Acronis Cloud storage plus cybersecurity add-on tiers. faaleoleo.io's flat-rate managed service eliminates this escalation entirely. Bacula's open format means backup data is yours — readable and restorable without Acronis software — while Acronis's .tibx format ties data to an active Acronis licence.

Both solutions address backup reliability for their target markets. Acronis excels in Windows-dominant SMB environments where its all-in-one agent, polished console, and Acronis Cloud storage reduce administrative overhead. faaleoleo.io addresses organisations that require heterogeneous platform coverage, structural security defaults, international compliance readiness (NIS2, DORA, NIST, ISO 27001, SOC 2), and long-term cost independence from per-workload pricing.

1. Positioning & Target Audience

1.1 faaleoleo.io — Managed Bacula Enterprise

faaleoleo.io is a managed service built exclusively on **Bacula Enterprise Edition** — the commercial variant of the Bacula backup engine, trusted for over 20 years in mission-critical environments at NASA, international banks, defence ministries, and Fortune 500 companies. faaleoleo.io handles deployment, OS hardening, monitoring, patch management, and expert support — so customers receive Enterprise-grade backup capabilities without needing in-house Bacula expertise. Bacula Enterprise licences are managed separately: customers bring existing licences or acquire them alongside the service.

- Growing organisations without dedicated backup staff
- Organisations subject to international compliance frameworks: NIS2, DORA, NIST SP 800-171, ISO 27001, SOC 2
- Heterogeneous IT environments: Linux, physical servers, containers, databases, cloud, HPC, tape
- Organisations that actively need to avoid vendor lock-in and proprietary data formats
- Security-critical environments requiring structural ransomware protection, not behavioural detection

1.2 Acronis Cyber Protect

Acronis positions itself as a cyber protection vendor that combines backup and recovery with cybersecurity capabilities in a single agent. Acronis Cyber Protect (on-premises and cloud-delivered) targets SMBs and mid-market organisations through direct sales and a large MSP partner ecosystem via Acronis Cyber Protect Cloud. The product integrates backup, anti-malware, vulnerability assessment, patch management, and remote desktop into one platform.

- Windows-dominant SMB and mid-market environments
- MSPs seeking a single-vendor backup and security bundle for their customers
- Organisations prioritising ease of onboarding and a polished all-in-one console
- Environments where Acronis Cloud storage convenience outweighs per-GB cost at scale
- Organisations comfortable with a US-domiciled vendor managing cloud storage and control plane

2. Technical Architecture

2.1 Core Engine

CRITERION	FAALEOLEO.IO (BACULA ENTERPRISE)	ACRONIS CYBER PROTECT
Engine	Bacula Enterprise Edition	Acronis proprietary (closed source)
Licence model	Commercial open-core — no format lock-in	Proprietary subscription + cloud storage
OS base	Linux-native	Windows-primary (Linux agent available)
Architecture	Director / Storage Daemon / File Daemon (modular)	Single agent per machine + management server
Backup format	Open Bacula format — directly readable	Proprietary .tibx — requires Acronis software

2.2 Component Architecture

FAALEOLEO.IO (BACULA ENTERPRISE)

```
Client (File Daemon)
  └─ TLS tunnel (AES-256) → Bacula Director (central controller)
       └─ Storage Daemon
            ├─ Local: Hardened & Encrypted Repository  [DEFAULT]
            │    └─ Disk / NAS / Tape — AES-256 at rest
            └─ Cloud: Hardened & Encrypted Repository  [DEFAULT]
                 └─ S3 / Azure Blob / GCS — AES-256 at rest + in transit
```

Every faaleoleo.io installation — local or cloud — ships with a hardened, AES-256-encrypted repository as a mandatory default. This is not a feature to enable: it is the baseline every customer receives.

ACRONIS CYBER PROTECT

```
Protected machine
  └─ Acronis Agent (installed per machine — Windows, Linux, macOS)
       └─ Acronis Management Server (on-prem) / Acronis Cloud Console (SaaS)
            ├─ Local backup destination (disk, NAS)
            │    └─ .tibx format  [encryption: optional, must be configured]
            └─ Acronis Cloud Storage (per-GB subscription)
                 └─ Geo-distributed Acronis datacentres
Active Protection module: behavioural anti-ransomware (agent-side detection)
```

Acronis requires an agent installed on every protected machine. The management plane can be deployed on-premises (Acronis Cyber Protect management server) or consumed as a SaaS console through Acronis Cloud. Encryption at rest for local backup destinations must be explicitly enabled per backup plan — it is not active by default.

2.3 Supported Workloads

WORKLOAD	FAALEOLEO.IO (BACULA ENTERPRISE)	ACRONIS CYBER PROTECT
Linux (physical / VM)	**Full, native**	Agent available — file-level and image backup
Windows (physical / VM)	Full	**Excellent — primary platform, application-aware**
macOS	Agent available	**Good — dedicated agent**
VMware vSphere	Full — agentless via plugin	**Good — agentless via VADP**
Microsoft Hyper-V	Full	Good
KVM / QEMU / Xen	**Full, native plugins**	Limited — agent-based only
Proxmox (incl. v9.0)	**Full plugin**	Not supported
Nutanix AHV	**Full plugin**	Limited — agent-based only
OpenStack	**Full plugin**	Not supported
Databases (Oracle, PostgreSQL, MySQL, MSSQL, SAP HANA, DB2, MongoDB)	**Deep — Enterprise plugins per engine**	Moderate — MSSQL, MySQL via agent; Oracle limited
Containers / Kubernetes	**Full — namespace-level plugin**	Limited — no native Kubernetes plugin
OpenShift	**Full plugin**	Not supported
HPC / Lustre file systems	**HPC Accelerator plugin**	Not supported
Tape	**Full, mature**	Not supported
Cloud (AWS, Azure, GCS) VMs	Full — S3-compatible + VM agents	**Good — cloud VM agents, Acronis Cloud**
Microsoft 365	**Full plugin — Exchange, SharePoint, OneDrive, Teams**	Good — dedicated M365 backup
Mainframe / AIX / HP-UX	**Full — Enterprise plugins**	Not supported

3. Plugin Ecosystem

Acronis's architecture is agent-centric: one agent per machine handles backup, anti-malware, and patch management. This simplifies Windows deployment but limits depth for heterogeneous environments. Bacula Enterprise's plugin model delivers application-aware, platform-native coverage that a single generic agent cannot match.

3.1 Bacula Enterprise — Extensive Plugin Library

Bacula Enterprise ships with a large and actively growing plugin ecosystem. The most recent release (18.2.1) added the HPC Accelerator, OpenStack, and LibVIRT plugins while enhancing Kubernetes, OpenShift, Proxmox, QEMU, and XenServer — demonstrating the pace at which coverage continues to expand.

CATEGORY	BACULA ENTERPRISE PLUGINS
Virtualisation	VMware, Hyper-V, KVM/QEMU, Xen, Proxmox (incl. v9.0), Nutanix AHV, OpenStack, LibVIRT
Containers	Kubernetes (namespace-level scalability), OpenShift (incl. Longhorn, KubeVirt/ OpenShift VM)
Databases	Oracle RMAN, PostgreSQL, MySQL/MariaDB, Microsoft SQL Server, SAP HANA, IBM DB2, Sybase, Informix, MongoDB
Cloud storage	AWS S3, Azure Blob, Azure VM, Google Cloud Storage, Microsoft 365 (Exchange, SharePoint, OneDrive, Teams)
HPC & storage	HPC Accelerator (Lustre, petabyte-scale), NDMP (NAS), Tape libraries
Platforms	RHEL 10, Debian 13, AIX, HP-UX, mainframe environments

3.2 Acronis — Agent-Centric Coverage

Acronis delivers backup through a single agent installed on each protected machine. This architecture works well for Windows endpoints and servers but does not provide the application-aware, hypervisor-native depth that dedicated plugins offer. There is no external plugin API for extending coverage to unsupported platforms.

Strong coverage: Windows physical and virtual machines, VMware vSphere (agentless VADP), Microsoft Hyper-V, macOS endpoints, Microsoft 365 (Exchange, SharePoint, OneDrive, Teams), Google Workspace, cloud VMs (AWS EC2, Azure VM), Microsoft SQL Server, MySQL.

Limited or absent: KVM, Proxmox, Nutanix AHV, OpenStack, Kubernetes (no native plugin), OpenShift, Oracle (limited), IBM DB2, Sybase, MongoDB, HPC/Lustre, tape libraries, mainframe/AIX/HP-UX.

KEY FINDING

Organisations with heterogeneous environments — particularly those running Linux-heavy, KVM, Proxmox, OpenStack, or container workloads — must operate a second backup toolchain alongside Acronis. faaleoleo.io covers the full environment from a single platform with application-aware protection at every tier.

4. Security Architecture

Security architecture is the most important differentiator in this comparison. Acronis markets itself as a cyber protection vendor and bundles anti-malware, behavioural ransomware detection, and vulnerability assessment with backup. However, Bacula Enterprise's security operates at the architectural level by default, and Acronis's 2023 data exposure incident raises direct questions about the gap between cybersecurity marketing and internal security practice.

4.1 faaleoleo.io Security Defaults

DEFAULT	WHAT IT MEANS
Hardened repos by default	Every installation — local or cloud — ships with a hardened, AES-256-encrypted repository. No administrator decision required; no feature to activate later.
End-to-end encryption	TLS for all communication channels. AES-256 for backup data at rest and in transit, regardless of whether storage is on-premises or in the cloud.
Architectural ransomware protection	The Storage Daemon accepts connections only when initiated by the Director. A compromised client cannot reach backup data — this is structural, not behavioural detection.
NIST-hardened OS images	faaleoleo.io delivers preconfigured, NIST-hardened images (QCOW/Docker) with signed releases and audit reports at every deployment.

- **Multi-factor authentication** — integrated at the protocol level
- **Air-gap capable** — full offline operation modes including tape rotation
- **Immutable audit logs** — signed and tamper-evident by default
- **Proven in the most sensitive environments** — Bacula Enterprise is the backup solution of choice for western defence and intelligence organisations, a standard no other backup vendor has publicly matched

4.2 Acronis Security Track Record

Acronis markets cyber protection as a core positioning — combining backup and cybersecurity in a single agent. Its Active Protection module uses behavioural heuristics to detect ransomware activity on the protected machine and can roll back affected files from a local backup cache. However, several factors require scrutiny:

- **2023 Acronis data exposure** — In March 2023, a hacker published approximately 12 GB of data allegedly extracted from Acronis systems. The leaked archive contained customer certificates, command logs, system information files, Python scripts used in Acronis operations, and configuration data. Acronis confirmed the data originated from credentials compromised at a single customer. A cybersecurity vendor whose customer data is accessible via compromised credentials — and whose internal operational tooling is exposed — raises direct questions about privileged access controls and defence-in-depth practices.
- **Active Protection is behavioural, not structural** — Acronis detects ransomware by monitoring file-system activity patterns on the protected endpoint. This catches known ransomware behaviour but does not prevent a compromised system from accessing the backup agent's data path. A sophisticated attacker who disables or bypasses the agent can access local backup data directly.
- **Encryption at rest is not the default** — Backup encryption must be explicitly enabled per backup plan. Local backup destinations do not encrypt data by default. This is a configuration decision, not a structural guarantee.

- **Agent attack surface** — The Acronis agent runs with elevated privileges on every protected machine. Agent vulnerabilities have been disclosed in multiple CVEs across Acronis product lines, creating a privileged attack vector on the machines it is supposed to protect.
- **No open-core model** — The codebase is not auditable. Customers rely entirely on Acronis's security attestations with no ability to independently verify implementation.

> **The critical difference is structural.** faaleoleo.io's ransomware protection is architectural — a compromised client cannot reach the Storage Daemon because the connection model does not permit it. Acronis's Active Protection detects ransomware behaviour on the endpoint but does not prevent a compromised system from accessing the agent and its local backup data. Structural prevention and behavioural detection are fundamentally different security properties.

5. Compliance

faaleoleo.io supports international compliance frameworks and serves organisations worldwide. The combination of Bacula Enterprise and faaleoleo.io's hardened managed service approach substantially reduces the effort required for compliance evidence — regardless of the regulatory framework in force.

REQUIREMENT	FAALEOLEO.IO	ACRONIS CYBER PROTECT
NIS2 (EU)	**Out-of-the-box ready**	Possible, configuration required; cybersecurity bundle adds complexity to scoping
DORA (EU financial)	**Explicitly addressed — immutable audit logs, documented recovery procedures**	Partial — financial-sector mapping requires additional documentation work
NIST SP 800-171 (US)	**NIST-hardened OS image as standard**	Possible — agent hardening and encryption must be explicitly configured
ISO 27001	**Supported via hardened deployment and audit trail**	Possible, requires configuration and documentation across backup and security modules
SOC 2	**Supported**	Acronis holds SOC 2 Type II for its cloud services
GDPR / Data sovereignty	**Full control — local, cloud, or hybrid; always AES-256 encrypted**	Acronis Cloud available in EU datacentres — but company is US-domiciled; legal review required for data transferred to Acronis systems
Audit logs	**Immutable, signed**	Present — not architecturally immutable or cryptographically signed by default

Data sovereignty consideration: Acronis is a US-domiciled company (incorporated in Switzerland, headquartered in Schaffhausen, with significant US operations). Organisations in the EU subject to GDPR and data residency requirements should review the legal basis for data processing when using Acronis Cloud storage or the Acronis Cloud management console, even when an EU datacentre is selected. faaleoleo.io's fully on-premises or EU-hosted deployment avoids this concern entirely.

6. Licensing & Cost Model

faaleoleo.io — Flat-Rate Managed Service

PLAN	PRICE	WHAT'S INCLUDED
Professional	from €599 / month	Mon–Fri support, email, 4 custom builds per year
Managed Hosting	Custom	24/7 dedicated support, fully cloud-hosted Bacula, SLA guarantees, uptime monitoring
Enterprise	Custom	Dedicated infrastructure, multi-region, unlimited custom builds, strategic consulting

Bacula Enterprise licences are not included in the faaleoleo.io subscription — customers bring existing licences or add them. The faaleoleo.io pricing model is **flat-rate**: no per-workload, per-CPU, or per-TB fees. The managed service cost stays stable as the infrastructure grows; only the Bacula Enterprise licence scales with workload count.

Acronis — Subscription and Cloud Storage Pricing

Acronis pricing is workload-based and compounds as infrastructure grows:

- **Per-workload subscriptions:** Acronis Cyber Protect is licensed per workload (server, VM, endpoint, mobile device). Tiers — Essentials, Standard, Advanced, Backup Advanced — determine which features are available. Advanced features including extended detection, EDR, and enhanced security require higher tiers.
- **Cloud storage costs:** Acronis Cloud storage is priced per GB per month. For organisations with large backup footprints, cloud storage costs escalate rapidly and add an unpredictable variable to the total cost of ownership.
- **Microsoft 365 backup:** Licensed separately per user per month — not included in the base workload licence.
- **Google Workspace backup:** Licensed separately per user per month.
- **Disaster Recovery add-on:** Cloud-based DR with compute time billed separately — not included in backup licensing.
- **MSP vs direct pricing:** Organisations purchasing through Acronis's MSP channel may see different pricing structures than direct customers, with complexity added by the Cyber Protect Cloud platform tier.

> For a 200-server environment with 20 TB of cloud backup data, Acronis per-workload and per-GB costs routinely reach five figures per month. faaleoleo.io's flat-rate model means the managed service cost is fixed regardless of workload count or data volume — providing genuine long-term cost predictability that Acronis's model cannot offer.

7. Vendor Lock-in & Data Portability

CRITERION	FAALEOLEO.IO (BACULA ENTERPRISE)	ACRONIS CYBER PROTECT
Backup format	**Open format, directly readable**	Proprietary .tibx format — requires Acronis software to read or restore
Switching providers	**At any time — config and data are portable**	Full data restore required before migration; .tibx data unusable without Acronis
Storage location	**Local, cloud, or both — any S3-compatible backend; AES-256 encrypted**	Local disk or Acronis Cloud — cloud storage locked to Acronis pricing and infrastructure
Code transparency	**Open-core — code audit possible**	Closed source — no code audit
Hardware dependency	**None — fully software-defined**	None — software only, but cloud storage dependency creates cost lock-in
Control plane dependency	**None — fully on-premises capable**	Acronis management server (on-prem option available) or Acronis Cloud console (SaaS)

The lock-in with Acronis is primarily at the data format and storage layer. Backup data stored in .tibx format is unreadable without Acronis software — a lapsed licence, a price dispute, or Acronis discontinuing a product line leaves data inaccessible. Organisations storing large volumes in Acronis Cloud face compounding exit costs: per-GB egress fees plus the time cost of full data restoration before migration.

Bacula's open format means data and configuration belong to the customer — always. A customer can read, restore, or migrate backup data independently of faaleoleo.io at any time using standard Bacula tools.

8. Operations & Support

	FAALEOLEO.IO	ACRONIS CYBER PROTECT
Customer operational effort	**Minimal — faaleoleo.io absorbs Bacula complexity**	Low for Windows workloads — console is polished and intuitive
Expertise at vendor	**Bacula specialists directly reachable**	Tiered support — quality varies by contract level
Custom builds / plugins	**Included by plan, or as add-on**	Not possible — proprietary closed platform
Updates / patches	**Automated, signed releases with audit report**	Automated agent and server updates
Plugin development	**Available — Bacula Enterprise Plugin API**	Not possible — no external plugin API
Linux expertise	**Linux-native architecture, deep OS-level support**	Secondary — Windows is the primary platform
Tape & HPC	**Full operational support included**	Not supported

Acronis's operational experience for Windows workloads is genuinely good: agent deployment is straightforward, the management console is well-designed, and recovery workflows for Windows servers and VMs are fast. For organisations whose entire environment is Windows-centric, operational overhead is low.

For organisations with heterogeneous environments — Linux, containers, databases, HPC, tape — teams must manage Acronis for Windows workloads and separate backup tooling for everything else. faaleoleo.io addresses the full environment from a single platform with Linux-native architecture and deep OS-level expertise built in.

9. Decision Matrix

REQUIREMENT	FAALEOLEO.IO	ACRONIS
Security-critical / government environments	**Strong advantage**	Adequate
Hardened & encrypted repos by default	**Standard in every deployment**	Configuration required — not a default
Structural ransomware protection	**Strong advantage**	Behavioural detection only
International compliance (NIS2, DORA, NIST, ISO 27001)	**Strong advantage**	Adequate — requires configuration work
No vendor lock-in	**Strong advantage**	Proprietary .tibx format
Open, auditable backup format	**Strong advantage**	Not supported
Predictable, growth-independent costs	**Strong advantage**	Per-workload + per-GB escalates at scale
Heterogeneous / Linux-heavy infrastructure	**Strong advantage**	Limited — Windows primary
Broad plugin ecosystem	**Strong advantage**	Agent-centric — limited depth
KVM / Proxmox / OpenStack / OpenShift	**Strong advantage**	Not supported
Kubernetes (namespace-level)	**Strong advantage**	Not supported
HPC / Tape / Mainframe	**Strong advantage**	Not supported
Air-gap / offline / tape	**Strong advantage**	Not supported
GDPR / EU data sovereignty	**Strong advantage**	Requires legal review (US-domiciled vendor)
Deep Oracle / SAP HANA / DB2 backup	**Strong advantage**	Limited
Windows endpoint & server backup	Adequate	**Strong advantage**
macOS endpoint backup	Adequate	**Strong advantage**
Microsoft 365 protection	**Good — full plugin included**	Good — strong but licensed separately
All-in-one security bundle (anti-malware, patch)	Out of scope	**Strong advantage**
Polished UI / fast Windows onboarding	Adequate	**Strong advantage**

10. Conclusion

Acronis Cyber Protect is a capable all-in-one platform for organisations whose infrastructure is primarily Windows — its polished console, straightforward agent deployment, and bundled anti-malware capabilities deliver real value for SMBs and MSPs serving Windows-dominant customer bases. macOS endpoint coverage and fast Windows onboarding are genuine strengths.

faaleoleo.io with Bacula Enterprise is the stronger choice for organisations that:

- Must meet international compliance requirements (NIS2, DORA, NIST, ISO 27001, SOC 2) structurally and demonstrably
- Need hardened, encrypted storage as a non-negotiable default — for local and cloud alike — not a configuration exercise
- Require structural ransomware protection rather than behavioural detection that can be bypassed
- Operate heterogeneous or Linux-heavy infrastructure
- Require the broadest possible plugin and platform coverage — including KVM, Proxmox, Nutanix, OpenStack, Kubernetes, OpenShift, HPC, or mainframe workloads
- Must protect tape libraries, NDMP NAS, or air-gapped environments
- Cannot accept proprietary .tibx format lock-in or per-GB cloud storage cost escalation
- Have EU data residency requirements requiring careful review of US-domiciled vendor relationships
- Need predictable, growth-independent backup costs at scale
- Have the highest security requirements: financial services, public sector, defence, critical infrastructure
- Want Enterprise backup quality without building in-house Bacula expertise

> faaleoleo.io's value proposition is precise: **Enterprise backup quality without Bacula complexity** — with the security architecture trusted by western defence organisations, the broadest plugin ecosystem in the industry, open-format data portability, and the compliance posture that international regulatory requirements demand.