



PACKAGED CYBER RESILIENCE SERVICE PROFILE

Total Data Protection Datasheet

A clear view of TDP service components, workload coverage, SaaS backup scope, fair-usage storage positioning and recommended operational baselines.

Workload protection

SaaS backup

Fair-usage storage

TDP

Total Data Protection

Managed cyber resilience stack

Ready service

Backup

Security

Management

SaaS

PROTECTION SUMMARY**Backup, security, management, and recoverability.**

Servers / VMs / Workstations / NAS

EDR/XDR

RMM

Recoverability ready

SAAS BACKUP**Microsoft 365 and Google Workspace**

Independent backup and granular recovery for core collaboration data.



PRODUCT SUMMARY

A packaged cyber resilience service.

Soteria Cloud Total Data Protection combines workload backup, recoverability, endpoint and server-style cyber protection, remote monitoring and management, and fair-usage cloud storage into a simplified protection model.

BACKUP AND RECOVERY	Policy-based backup and restore for supported workloads.
CLOUD STORAGE	Storage included under Soteria Cloud fair usage policy.
EDR/XDR	Security capability for servers, VMs, workstations and NAS workloads.
RMM / ADVANCED MANAGEMENT	Monitoring and management for servers, VMs, workstations and NAS workloads.
SAAS BACKUP	Cloud-to-cloud backup for Microsoft 365 and Google Workspace data.
REPORTING	Operational visibility into protected workloads, backup health and service usage.

SERVICE MODEL

Acronis-powered, Soteria Cloud-delivered

PRIMARY AUDIENCE

MSPs, resellers, business customers

COMMERCIAL AIM

Simpler protection packaging

DIFFERENTIATOR

TDP connects backup, security and management for core workloads while adding SaaS backup coverage for Microsoft 365 and Google Workspace.



COVERAGE MATRIX

The right capabilities for the right workload type.

Servers, VMs, workstations and NAS receive the full TDP workload protection model. Microsoft 365 and Google Workspace are treated as SaaS backup workloads focused on collaboration data recoverability.

WORKLOAD / SERVICE	BACKUP	GRANULAR RESTORE	RMM	EDR/XDR	STORAGE
Windows workstations	Yes	Yes	Yes	Yes	Fair usage
macOS workstations	Yes	Yes	Yes*	Yes*	Fair usage
Linux workstations	Yes	Yes	Yes*	Yes*	Fair usage
Physical servers	Yes	Yes	Yes	Yes	Fair usage
Virtual machines	Yes	Yes	Yes	Yes	Fair usage
NAS	Yes	Yes	Yes	Yes	Fair usage
Microsoft 365	Yes	Yes	No	No	Fair usage
Google Workspace	Yes	Yes	No	No	Fair usage

FULL WORKLOAD BUNDLE

Servers, VMs, workstations and NAS receive backup, restore, EDR/XDR capability, RMM / Advanced Management, fair-usage storage, monitoring, reporting and policy-based operational management.

SAAS BACKUP WORKLOADS

Microsoft 365 and Google Workspace receive cloud-to-cloud backup, restore and fair-usage storage. RMM and EDR/XDR do not apply to SaaS seats in the same way they apply to device and server workloads.

* Capability may depend on operating system, agent support, Acronis edition, add-ons and policy configuration.



SAAS BACKUP SCOPE

Independent recovery for cloud collaboration data.

TDP helps reduce reliance on native retention assumptions by protecting supported Microsoft 365 and Google Workspace data through cloud-to-cloud backup and granular recovery.

MICROSOFT 365

- Exchange Online
- OneDrive
- SharePoint Online
- Microsoft Teams where supported
- Files, folders, mail items, attachments and permissions where supported

GOOGLE WORKSPACE

- Gmail
- Google Drive
- Shared drives / Team Drives
- Calendar
- Contacts
- Item-level and point-in-time recovery where supported

FAIR USAGE STORAGE

TDP includes cloud storage under a Soteria Cloud fair usage policy. General commercial positioning is commonly around 10 TB per protected workload unless a specific quote, agreement or product schedule states otherwise.

OPERATIONAL USE CASE	TDP FIT
Recover a deleted Microsoft 365 mailbox item	Microsoft 365 backup and granular recovery
Recover Google Drive files after deletion	Google Workspace backup and restore
Recover clean data after ransomware	Backup + EDR/XDR + restore
Standardise MSP customer protection	Policy-based bundled protection
Monitor protected endpoints and servers	RMM / Advanced Management



BASELINE AND COMMERCIAL NOTES

A service model designed for account reviews.

TDP simplifies service positioning, but exact licensing and pricing still depend on workload mix, storage consumption, required add-ons, support model and commercial agreement.

BACKUP FREQUENCY	Align to business RPO. Critical systems may require more frequent backups.
RETENTION	Define by workload, compliance and customer requirements.
RESTORE TESTING	Schedule regular restore tests, not only backup success checks.
ALERTING	Monitor failed backups, stale agents, storage anomalies and security events.
ACCESS CONTROL	Use least privilege and role-based access.
REPORTING	Provide customer-facing protection and recoverability reports.

Target audience

- MSPs and resellers
- Business owners
- IT managers
- Compliance-conscious SMEs
- Microsoft 365 and Google Workspace customers

Differentiators

- Acronis-powered cyber protection
- Soteria Cloud partner enablement
- Local South African operational context
- Backup, security and management bundled for core workloads
- Simple resilience language for sales and customers

ABOUT SOTERIA CLOUD

Soteria Cloud helps South African MSPs, resellers and organisations deliver practical cyber resilience through prevention, detection and response, recoverability, and operational stability. Soteria Cloud is an Acronis Platinum Partner and Cloud Aggregator, with local Acronis Cyber Protect Cloud hosting in Teraco Johannesburg and Cape Town.

IMPORTANT NOTE

Specific features, licensing and workload support can vary by Acronis edition, add-on, tenant configuration and commercial agreement. Final scope should always be confirmed against the active Soteria Cloud quote and Acronis tenant configuration.