



A PRACTICAL PROTECTION BASELINE FOR MODERN OPERATIONS

Total Data Protection Solution Brief

How Soteria Cloud TDP helps customers prevent what they can, detect what they must, and recover what matters.

Resilience baseline

Partner-ready service

Recoverability outcomes

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/XDRRMM

Recoverability ready

SAAS BACKUP
Microsoft 365 and Google Workspace
Independent backup and granular recovery for core collaboration data.



EXECUTIVE SUMMARY

Protection tools often live in separate silos.

Many organisations believe they are protected because they have backup, antivirus or Microsoft 365 retention policies in place. The gap appears when implemented protection is mistaken for tested recoverability.

Soteria Cloud Total Data Protection gives MSPs, resellers and business customers a unified protection model for modern operations.

It packages backup, recoverability, security and management into a practical service powered by Acronis Cyber Protect Cloud and delivered through Soteria Cloud.

OBJECTIVE

Help customers prevent what they can, detect what they must, and recover what matters.

THE BUSINESS PROBLEM

- Workstations and servers need backup, endpoint security and operational monitoring.
- Microsoft 365 and Google Workspace data need independent backup.
- Ransomware and accidental deletion remain common causes of data loss.
- Backup success is too often treated as recoverability proof.
- MSPs need packages that are easy to sell, manage and report on.

Backup and restore

Policy-based recovery for supported workloads and SaaS collaboration data.

Security capability

EDR/XDR capability for applicable server, VM, workstation and NAS workloads.

Management visibility

RMM / Advanced Management, monitoring, reporting and centralised policy control.



HOW TDP IS STRUCTURED

Two clear protection tracks.

TDP separates full workload protection from SaaS data protection so the service remains easy to explain and commercially clear.

Full workload protection

Servers, VMs, workstations and NAS receive backup, EDR/XDR, RMM / Advanced Management, monitoring, reporting and fair-usage storage.

SaaS data protection

Microsoft 365 and Google Workspace receive cloud-to-cloud backup, granular recovery and fair-usage storage.

Managed resilience service

Soteria Cloud and Acronis Cyber Protect Cloud provide centralised management, reporting, policy governance and partner support.

Customer environment

- Servers
- Virtual machines
- Workstations
- NAS
- Microsoft 365
- Google Workspace

Protection capabilities

- Backup
- Restore
- EDR/XDR
- RMM / Advanced Management
- SaaS backup
- Fair-usage cloud storage

Service outcomes

- Centralised management
- Operational reporting
- Policy governance
- Partner/customer support
- Recoverability reviews

RESILIENCE PILLAR	TDP CONTRIBUTION
Prevention	Security controls for protected endpoint/server workloads and safer configuration.
Detection & Response	EDR/XDR visibility and response capability for applicable workloads.
Recoverability	Backup, restore, SaaS recovery and fair-usage cloud storage.
Operational Stability	RMM, monitoring, reporting and centralised service management.



COMMON CUSTOMER SCENARIOS

A baseline customers can understand.

TDP is built around the operational events that customers and partners regularly face: ransomware, accidental deletion, SaaS data loss and inconsistent protection baselines.

Ransomware on a workstation or server

Detect and respond through endpoint/server security capability, then recover from known-good backup points.

Accidental Microsoft 365 deletion

Recover deleted or corrupted Microsoft 365 data from independent backup instead of relying only on native retention.

Google Workspace data loss

Restore supported Gmail, Drive, shared drive, Calendar and Contacts data from protected backups.

MSP standard protection baseline

Attach a repeatable protection package to every customer with a clearer operational and account-review story.

PARTNER POSITIONING

- Easy to explain
- Easier to quote than multiple disconnected tools
- Aligned to recurring service revenue
- Suitable for account reviews and protection gap discussions
- Built around recoverability outcomes, not product checkboxes

SUGGESTED TALK TRACK

Total Data Protection gives your customer a practical cyber resilience baseline. Their servers, VMs, workstations and NAS get backup, security and management. Their Microsoft 365 and Google Workspace environments get independent SaaS backup. The goal is not just to say the customer is protected. The goal is to prove they can recover.



CUSTOMER OUTCOMES

Recoverability outcomes, not product checkboxes.

TDP gives partners and customers a simple way to discuss protection gaps, resilience priorities and proof of recovery.

OUTCOME	WHAT IT MEANS
Reduced tool sprawl	Backup, security and management are packaged together for core workloads.
Better recoverability	Customers can restore critical data and workloads from managed backups.
Clearer MSP service delivery	Partners can standardise onboarding, reporting and reviews.
Improved SaaS resilience	Microsoft 365 and Google Workspace data are protected beyond native retention assumptions.
Practical cyber resilience	Prevention, detection, recovery and operations are connected.

SERVICE ONBOARDING APPROACH

- 1 Identify protected workloads and SaaS tenants.
- 2 Confirm workload types and TDP eligibility.
- 3 Apply backup and protection policies.
- 4 Confirm storage and fair usage expectations.
- 5 Configure monitoring and alerting.
- 6 Run initial backup validation.
- 7 Schedule restore testing.
- 8 Report on protection health and recoverability.

ACCOUNT REVIEW QUESTIONS

- Which workloads are protected today?
- Which Microsoft 365 or Google Workspace data is not independently backed up?
- When last was a restore tested?
- Are backup alerts monitored and acted on?
- Does the customer understand recovery point and recovery time expectations?



BOTTOM LINE

A clear resilience baseline for customers and partners.

TDP gives customers a practical way to understand what is protected, where recoverability gaps may exist, and how backup, security, management and service reporting work together.

PARTNER VALUE

Soteria Cloud Total Data Protection gives partners a packaged way to deliver backup, security, management and recoverability without turning every customer conversation into a product-by-product comparison.

CUSTOMER VALUE

Clear cyber resilience baseline

PARTNER VALUE

Repeatable managed service package

COMMERCIAL FOCUS

Recoverability outcomes

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.