Microsoft Sovereign Data Protection

WHAT IT IS

A Microsoft sovereign data protection offering that gives clients a practical way to protect sensitive data, preserve customer control, and keep critical services defensible as regulatory, sovereignty, and operational pressures rise. It bridges Microsoft-native resilience with externally controlled keys, policies, evidence, and highly sensitive content.

The offering solves the core problem that availability alone is not enough: organizations also need lawful access, provable control, and protection against data loss, oversharing, fragmented key ownership, and cloud-only dependency. The urgency is now because data is already distributed across Azure, Microsoft 365, AI, SaaS, and hybrid estates, while regulators, boards, and threat actors increasingly focus on where sensitive data resides, who controls the keys, and whether the business can continue to operate securely under constraints.

KEY COMPONENTS

- Data discovery, classification, Purview labels, DLP policies, and privacy enforcement.
- Azure Key Vault / Managed HSM with CMK, BYOK, and HSM-backed service encryption.
- Thales CipherTrust CCKM for key lifecycle, discovery, rotation, reporting, and automation.
- Thales Luna HSM / Luna Key Broker for top-tier roots of trust and Microsoft 365 DKE custody.
- Integrity, masking/tokenization, secrets management, audit trail, and Sentinel evidence chain.
- Reference architecture that separates customer-controlled trust from cloud-provider operations.

eKMS + Data Protection

Purview DLP detects and enforces; Thales protects, tokenizes, governs, keys, and supplies evidence.

Microsoft + Thales Sovereign Data Protection Reference Architecture

Microsoft Control Fabric
- Purview DLP + labels
- Entra ID / PIM
- Sentinel + Defender
- M365 + Azure services

Unified Data Protection Plan
- Discovery + classification
- Encryption + BYOK/CMK
- Masking / tokenization
- Secrets + lifecycle
- Audit + evidence

Thales Trust Layer
- CipherTrust CCKM
- Luna HSM / Key Broker
- External custody + control

Detect	Protect	Control	Evidence
Purview scans, classifies, and labels sensitive data	DLP, encryption, tokenization, and secrets policies apply	Customer-held keys and HSM roots govern access	Sentinel, CCKM logs, approvals, and audit trail prove control

Reference pattern: classify first, then apply the lightest defensible control for the data class.

OUTCOMES

- Lawful continuity of critical data and digital services under sovereign constraint.
- Reduced data-loss risk through DLP detection, policy enforcement, encryption and tokenization.
- Board- and regulator-defensible evidence through CCKM, HSM, Sentinel, and approval logs.
- Stronger customer control of keys, secrets, and highly sensitive Microsoft 365 content.
- Faster cloud modernization with lower control fragmentation and repeatable architecture patterns.