Solution Brief

THALES
CYBERSECURITY

EDB POSTGRES AI

Securing Sovereign AI with EDB Postgres AI and Thales CipherTrust Manager

Empowering enterprises to confidently leverage AI with compliance and control across cloud and sovereign environments

cpl.thalesgroup.com

Outcomes at a Glance

- Maintain **data and AI model sovereignty** across hybrid and multi-cloud environments
- Enforce **regional compliance** through externalized, customer-controlled key management
- Simplify **AI governance** with centralized key and policy management
- Accelerate **secure AI innovation** using open, enterprise-grade Postgres infrastructure

As AI becomes central to national and enterprise strategy, organizations must balance innovation with sovereignty, ensuring that data, models, and infrastructure remain under their control. However, AI demands vast amounts of data to train models, opening the organization to the risk of sensitive data being sent beyond physical borders. In some cases, regulations may not allow data to leave a nation's borders. Ultimately, security and compliance involve ensuring that customers have control over their operations and data. So, how do customers maintain control as their operations and technology environments become more decentralized? Fortunately, EDB and Thales are combining forces to address these challenges as customers embark on making sovereign AI a reality.

EDB Postgres AI and Sovereignty

EDB has reimagined Postgres for the era of cloud and AI, delivering solutions that meet real customer security and compliance needs. With EDB Postgres AI, customers can deploy and manage their database however they prefer – on-premises, in private clouds, with cloud providers that meet their local or regional compliance requirements, or in hybrid architectures that balance the needs and benefits of each option.

In partnership with Supermicro, EDB Postgres AI is available in an all-in-one system that delivers production AI-ready Postgres to customers' private data centers, providing them with complete digital and operational control.

For customers leveraging the cloud's flexibility and easy scaling, EDB Postgres AI Hybrid Manager allows users to quickly set up containerized Postgres databases in AWS, GCP, Azure, and any Red Hat OpenShift environment, with data stored in the hyperscaler's storage services. Whether using the on-premises appliance, the cloud, or both, EDB Postgres AI Hybrid Manager consolidates data control into a single interface for improved visibility and management.

Every version of EDB Postgres AI employs transparent data encryption (TDE) to protect sensitive data, with encryption keys stored on the database server by default. EDB collaborates with Thales to offer enhanced key management for enterprise customers.

Thales CipherTrust Manager and EDB Postgres AI

Thales CipherTrust Manager strengthens EDB Postgres AI's data protection by externalizing TDE keys from the database server, establishing both logical and physical separation that significantly enhances security and compliance. Customers can store their TDE keys in their preferred environment: within a Thales Luna Hardware Security Module (HSM) for hardware-rooted security, inside a virtual CipherTrust Manager instance deployed in a sovereign or private cloud, or through Thales CipherTrust Cloud Key Management (CCKM) for organizations seeking cloud-based key lifecycle control while maintaining exclusive ownership of their cryptographic keys.

By anchoring encryption keys in Luna HSMs, organizations gain tamper-resistant protection supported by FIPS-validated hardware, ensuring that cryptographic material never leaves customer control. This separation, along with exclusive key ownership, reduces insider threats, enforces jurisdictional sovereignty, and meets compliance requirements such as GDPR, DORA, and NIS2. It is especially vital for AI workloads, where maintaining the confidentiality and integrity of training data and models within specific geographic boundaries is essential for secure and explainable AI operations.

What Digital Sovereignty Means with EDB and Thales

Digital sovereignty extends beyond data residency. With EDB Postgres AI and CipherTrust Manager, organizations maintain full control of their data, infrastructure, and AI models—deciding where information is stored, who manages it, and how it is secured. This architecture supports regional laws, AI governance frameworks, and audit trails while preserving long-term independence in an increasingly cloud-driven world.

Comply with Data Security and Sovereignty Regulations

When customers use CipherTrust Manager with EDB Postgres AI Hybrid Manager to secure and locate encryption keys within their chosen jurisdiction, they control the physical and logical security and legal governance of their encrypted cloud data. Encrypted data that is backed up or replicated outside its target jurisdiction remains unreadable until the customer supplies the required encryption keys. This adds a vital layer of control for AI training datasets and models, ensuring that proprietary or national security-level information stays fully sovereign. CipherTrust Manager provides extra reassurance when working with hyperscalers, whose extensive global presence can complicate compliance for large enterprises.

Streamline Key and Policy Administration Through Centralization

Over time, organizations develop encryption silos as they adopt native tools from various database, storage, and application solutions. Large enterprise customers should incorporate EDB Postgres AI TDE into their overall encryption management strategy. CipherTrust Manager consolidates key storage and centralizes key and policy management, eliminating these silos that are vital to modern AI pipelines operating across multiple environments. In collaboration with EDB, CipherTrust Manager offers both on-premises sovereign appliances and virtual options to ensure efficient, streamlined, and secure deployment.

Additionally, the centralized logging provided by CipherTrust Manager enhances an organization's ability to demonstrate compliance and meet data sovereignty requirements. This auditable control is essential for AI governance and explainability, especially when combined with EDB Postgres AI's native observability features. The platform's real-time query diagnostics and performance metrics provide transparency into how AI models access and use data. At the same time, CipherTrust Manager's logging ensures that the keys protecting that data are managed with the highest security standards.

Empowering Secure and Sovereign AI Innovation: The EDB + Thales Collaboration

EDB Postgres AI redefines database management for the cloud and AI era, while CipherTrust Manager and Luna HSMs ensure encryption keys and policies remain under customer control. Together, they enable organizations to protect sensitive data, preserve jurisdictional integrity, and drive AI innovation securely and at scale—secure, compliant, and sovereign by design.

The collaboration between EDB and Thales brings together two leaders in open-source data management and trusted data security. By combining EDB's flexible, AI-ready database architecture with Thales' proven encryption, key management, and hardware-based security, the partnership provides a foundation for sovereign AI, allowing customers to maintain full cryptographic and operational control without sacrificing agility or innovation.

About EDB

EDB provides a data and AI platform that enables organizations to harness the full power of Postgres for transactional, analytical, and AI workloads across any cloud, anywhere. EDB empowers enterprises to control risk, manage costs and scale efficiently for a data and AI-led world. Serving more than 1,500 customers globally and as the leading contributor to the vibrant and fast-growing PostgreSQL community, EDB supports major government organizations, financial services, media and information technology companies.

About Thales

Today's businesses and governments depend on the cloud, data and software to deliver trusted digital services. That is why the most recognized brands and organizations around the world, rely on Thales to help them protect sensitive information and software wherever it is created, stored or accessed – from the cloud and data centers to devices and across networks. As the global leader in data security, identity & access management, and software licensing, our solutions enable organizations to move to the cloud securely, achieve compliance with confidence, create more value from their software and deliver seamless digital experiences for millions of consumers every day.