pgEdge™

Case Study: Thales

Thales Achieves Ultra-High Availability for CipherTrust Data Security Platform with pgEdge

The Challenge

As a leader in cybersecurity and data protection, Thales delivers CipherTrust as an appliance that customers install and host in their own environments. This architecture means Thales never has direct access to customer systems, placing extraordinary demands on the underlying database infrastructure for reliability, flexibility, and autonomous operation.

Thales encountered several strategic and operational challenges with its existing database platform. Collaboration and product flexibility were limited, making it difficult to adapt the solution quickly to meet Thales' evolving technical and business requirements. More fundamentally, Thales needed a distributed solution capable of supporting customers who deploy CipherTrust in distributed environments across multiple locations and cloud platforms.

The Solution

Thales selected pgEdge Distributed Postgres as an OEM solution for CipherTrust Data Security Platform, to embrace a truly open source, distributed PostgreSQL architecture. Each pgEdge node runs on one VM or one physical appliance, with each hosting a database instance of PostgreSQL with the Spock extension for advanced replication capabilities.

The solution architecture aligns perfectly with Thales' deployment model. Customers can launch VMs with hardware of their choice, with Thales providing minimum requirements and recommendations—typically 4 CPUs/cores minimum and 16 GB RAM, with higher specifications recommended for larger deployments and production systems. For customers preferring physical deployments, Thales offers dedicated appliances with specifications optimized for CipherTrust Manager workloads.

The pgEdge implementation provides unlimited distribution of the pgEdge Distributed Postgres bundled with Thales CipherTrust Data Security Platform, along with 24x7 expertise, guidance, and support for the pgEdge Distributed Postgres. This ensures that Thales has the technical partnership they sought—responsive support and the flexibility to evolve the solution as their requirements change.

A critical capability that pgEdge brought to CipherTrust is enhanced conflict

THALES

Thales delivers advanced cybersecurity across regulated industries, specializing in data protection, encryption, and cloud security. Its CipherTrust Manager centralizes key management, policies, and compliance, simplifying operations and enforcing consistent data security across on-prem, hybrid, and multi-cloud environments while reducing complexity and strengthening enterprise protection.

Industry: Cybersecurity

management, handling conflicts on both primary and secondary unique indexes—something the previous solution struggled with. The platform's Z0DAN (Zero Downtime Add Node) feature enables node addition with zero downtime, and the cluster can scale to support up to 20 nodes, providing the distributed architecture Thales' global customer base demands.

The Results

The migration to pgEdge has transformed the operational capabilities and reliability of CipherTrust Data Security Platform. Thales achieved Ultra-High Availability, ensuring the system remains online even during node maintenance and when adding new nodes to the cluster. This level of availability is essential for mission-critical cybersecurity infrastructure where downtime is simply not acceptable.

The upgrade process saw dramatic improvements, with downtime reduced from hours to near-zero during patching operations. This means Thales customers can maintain security patches and updates without disrupting their critical data protection operations—a significant competitive advantage in industries where compliance and security posture must be maintained continuously.

Resilience increased substantially, as nodes can now be upgraded independently while preserving application stability. This eliminates the cascading risk that comes with monolithic database upgrades and gives Thales customers greater control over their maintenance windows.

By leveraging an open, non-proprietary solution, Thales escaped vendor lock-in and gained the transparency and control needed to innovate rapidly in response to evolving cybersecurity threats. The open source foundation means Thales can inspect, modify, and enhance the platform as needed, rather than waiting on a vendor's roadmap.

The advanced conflict management capabilities pgEdge provides have proven essential for CipherTrust's distributed deployment model, handling conflicts on primary and secondary unique indexes reliably and automatically. Combined with Z0DAN's ability to add nodes with zero downtime and support for clusters up to 20 nodes, Thales now has the distributed, highly available architecture their global enterprise customers require.

Most importantly, Thales found the true business partnership they were seeking. pgEdge's commitment to complete cooperation, technical flexibility, and responsiveness has enabled Thales to enhance CipherTrust based on customer requirements quickly and confidently—turning their database infrastructure from a constraint into a competitive advantage in the demanding cybersecurity market.

About pgEdge

pgEdge® delivers open-source, 100% Postgres infrastructure for Agentic AI and other enterprise applications that demand high availability, reliability, and/or data sovereignty. Our mission is to make it easy to build, deploy, and manage enterprise-grade applications at scale on the open source Postgres database.