Garantir

Solution Brief

Simplified App-Level Encryption & Tokenization with GaraTrust

No code changes. No proxies. No problem.

Transparent database encryption (TDE) has been the cornerstone of database security for over a decade, but **PCI DSS 4.0, DORA, GDPR, HIPAA, as well as other regulatory threat models** are exposing the deficiencies of TDE and the need for datum-level encryption. For enhanced security and true compliance, data protection must be applied at the field, column, or application layer. TDE and full-disk encryption protect against physical theft, but **leave plaintext exposed** to anyone with database access, including the DBA. Application-level encryption and tokenization close this gap but have historically been too costly and difficult to deploy, until now.

Traditional approaches to ALE often fail to keep up.

- **Per-Application Code Changes:** SDK-based approaches force development teams to instrument every application, multiplying cost, slowing deployments, and excluding systems and applications where code changes are not possible.
- **Database Proxies:** Proxy-based architectures inject a network hop between applications and the database, negatively impacting performance and effectively becoming another transparent layer of encryption.

Unified ALE & Tokenization

Dramatically reduced time-to-value and reduced implementation costs.

Garantir's **GaraTrust** platform delivers application-level encryption and tokenization, using standard and format-preserving methodologies from a single cohesive architecture — protecting sensitive data **at the point of use**. For additional security, GaraTrust also supports HSM-backed non-exportable keys. GaraTrust is the cryptographic governance layer for the data your applications protect.

- ✓ **Transparent Driver-Level Integration:** GaraTrust database driver wrappers deliver field-level encryption and tokenization with zero application code changes — covering the major data sources used in production today.
- ✓ **Non-Exportable Keys with HSM-Backed Custody:** Encryption keys can be configured for HSM-backed deployments and used within the secure boundary of the HSM, or deployed at the application where necessary.

- ✓ **Multiple Data-Protection Methods, One Platform:** Choose between application-level encryption, or tokenization, or use both.
- ✓ **Federated Authentication & Authorization:** Each cryptographic operation is authorized against an enterprise identity provider. A compromised database or DBA account cannot decrypt the data it stores.
- ✓ **Crypto Agility:** GaraTrust provides centralized control over the algorithms used to encrypt data at the application level. This allows for easy transition from one algorithm to the next, ensuring alignment with emerging compliance standards.

One Platform for the Data You Protect

The central challenge enterprises face isn't a lack of data-security tools. It's a fragmented patchwork of them with no single place to manage keys, audit access, or enforce policy across the applications that touch sensitive data.

The GaraTrust cryptographic services platform deploys application-level encryption across the databases, file stores, and data flows teams use today without rip-and-replace or code changes. Gain centralized visibility, access control, audit capability, and more across the data the enterprise protects, as well as a platform that grows with the organization's needs.

Software Supply Chain

CLM & PKI

Passwordless Authentication

Data Security

AI Agent Security

Key Features & Benefits

GaraTrust is built for high availability, transparent integration, and rapid deployment.

Better Security

Data is encrypted at the point of use and keys never leave the HSM. Key-based authorization stops privileged-user data theft.

Enhanced Compliance

Supports data privacy and encryption mandates with field-level encryption and centralized audit logging across operations.

No Code Changes

Deploys across internal and third-party applications without code changes, accelerating time-to-value and ease of deployment.

Supported Technologies

GaraTrust integrates seamlessly into existing data flows with a suite of supported integrations and easy-to-use APIs, engineered for multi-vendor environments and a wide range of technologies.

- ✓ **We support** the major HSM and key managers, both cloud-based and on-prem.
- ✓ **We integrate** with leading authentication providers: Okta, Microsoft Entra ID, Ping, Duo, and standards-based federation (SAML, OIDC, OAuth).
- ✓ **We work with** existing databases. GaraTrust connects at the driver level, allowing it to be agnostic to the back-end database technology.

Integration Methods:	JDBC and ODBC driver wrappers, and language-native SDKs. Wrapper-based deployment requires zero application code changes; SDK and REST integrations are available where deeper application-level control is required.
Formats & Standards:	Aligned with widely adopted data security and cryptographic standards including FIPS 140-2 / 140-3 validated HSMs, NIST SP 800-38 (block cipher modes), 800-57 (key management), 800-131A (cryptographic transitions), and 800-207 (Zero Trust). Compliance-aligned data protection under PCI DSS 4.0, SOX, HIPAA, GDPR, and CCPA. AES-256 symmetric encryption (GCM, CBC, and CTR modes). Format-preserving and standard encryption. Deterministic and non-deterministic tokenization.
Deployment Models:	Self-managed (customer deployed), standard SaaS (Garantir-operated, multi-tenant, customer owned keys), and dedicated SaaS (Garantir-operated, single-tenant) — all on the same platform with the same cryptographic guarantees.

Ready to take your data protection and compliance to the next level?