THALES

Thales Transparent Encryption for YugabyteDB

The problem: cloud native databases store sensitive data that needs security

Enterprises are driving to become more cloud native. Speed, scalability, resilience and geographically distributed operations are table stakes in an increasingly globalized marketplace. Until recently enterprises have been forced to make difficult tradeoffs between traditional SQL and NoSQL databases, but now they can benefit from new distributed SQL databases like YugabyteDB that offer the best of both worlds. One thing remains unchanged, however, these new distributed SQL databases still serve as repositories of highly sensitive data.

The challenge: organizations still have security and compliance needs

Yet, organizations still face security and compliance obligations even if their database vendor doesn't offer the full suite of security tools they need. Many industry regulations call for encryption and external key management. Organizations must consider and address the privileged insider risk that comes from system administrators, or other personnel with root user access. All of these concerns become increasingly important when organizations use public cloud technology with operations spread across geographic regions. Taken together, organizations face a daunting task in securely becoming cloud native.

Fortunately, YugabyteDB and Thales partner to address these security and compliance concerns.

Key benefits:
- Robust File-system-level data encryption
- Administrative simplicity
- Granular privileged user access policy enforcement
- Comprehensive compliance controls and audit trails
- Transparent data at rest encryption for YugabyteDB
- Encrypted data backups for YugabyteDB

CipherTrust Transparent Encryption for YugabyteDB

The solution

CipherTrust Transparent Encryption (CTE) secures YugabyteDB data at-rest with file system-level encryption supported by centralized key management, privileged user access controls and detailed data access audit logging. CTE transparently encrypts YugabyteDB clusters without needing any configuration changes in the database.

CTE deploys quickly, simply, and in a scalable manner. Agents install on the same operating file-system or device layer as YugabyteDB. Encryption and decryption remain transparent to the database and all applications so organizations don't have to worry about downtime or architecture changes. Organizations use CTE to address data security compliance and best practice requirements with minimal disruption, effort, and cost. CTE works in conjunction with the CipherTrust Manager, a FIPS 140-2 up to Level 3 validated centralized encryption key and policy platform.

Why use Thales CipherTrust Transparent Encryption with YugabyteDB?

YugabyteDB cloud native features coupled with transparent data encryption provided by CTE allows enterprises to implement strong encryption and compliance practices for geographically distributed cloud-native applications.

Thales' CipherTrust centralized key management efficiently incorporates YugabyteDB into their larger organization-wide encryption strategy. CTE's privileged user access controls and data access audit logging separate database security and administration duties between individuals, and increases visibility and oversight of the data's security – both improving effectiveness and satisfying key compliance requirements.

Simplified Deployment and Administration

CipherTrust Transparent Encryption minimizes the time and effort required to implement and maintain YugabyteDB's data at rest security. CTE secures data without requiring application or database code or architecture changes. Additionally, CipherTrust Manager provides a consolidated, central management point for encryption keys and policies from across an enterprise's storage, databases and applications.

Granular User Access Policy Controls and Enforcement

Security teams use CTE to institute and enforce granular, least-privileged user access policies (e.g. by user, process, file type, time of day) to YugabyteDB. Admins use such policies to allow specific users access to clear-text data while limiting the file system commands they can perform. Access controls place an additional layer of security between systems and data that makes data safer and renders its access more visible to security teams. Using these types of controls, organizations can permit system administrators to manage configurations and ongoing maintenance on YugabyteDB's infrastructure without having clear-text access to the sensitive content within.

Comprehensive Compliance Controls and Audit Trails

CTE's detailed data access audit logging addresses many common regulatory compliance controls for encryption, data sovereignty, least-privileged policy and data access auditing. Auditors use intelligence logs to assess the effectiveness of encryption, key management and access policies. Logs reveal when users and processes access data, under which policies, whether requests were allowed, and even when a privileged user submits a command like "switch user" to attempt to imitate another user. Additionally, CTE's pre-built integration to leading Security Information and Event Management (SIEM) systems means this log data is available for use to provide immediately actionable insights.

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation.

Decisive technology for decisive moments.

About Yugabyte

YugabyteDB is a Distributed SQL database serving both scale-out RDBMS and internet-scale OLTP workloads with low query latency, extreme resilience against failures, and global data distribution. YugabyteDB Kubernetes offering provides a helm chart for deploying Yugabyte Platform which is best fit for mission-critical deployments, such as production or pre-production testing. Yugabyte Platform provides deployment, orchestration, and monitoring to manage YugabyteDB universes. Yugabyte Platform can create a YugabyteDB universe with multiple Pods provided by Tanzu Kubernetes Grid Integrated Edition (TKGI) and logically grouped together to form one logical distributed database. Yugabyte Platform also helps with linear scaling of workloads by transparently adding new nodes to the cluster without any downtime.

For more detailed technical specifications, please visit https://cpl.thalesgroup.com/ or www.yugabytes.com.

Contact us – For all office locations and contact information, please visit cpl.thalesgroup.com/contact-us