

Safeguarding Sensitive Data and Solving Compliance Obstacles with Neo4j Graph Database



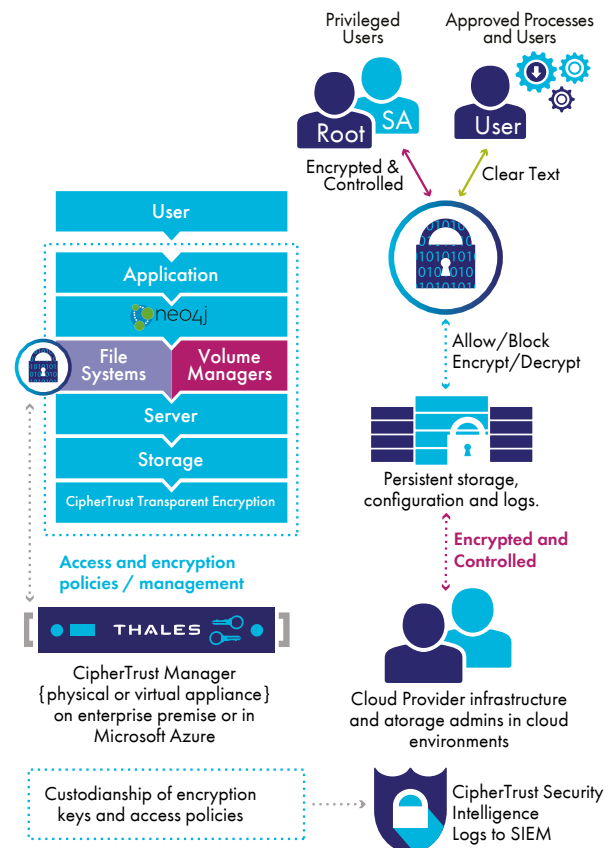
Key benefits:

- Transparent file-system-level data encryption
- Centralized enterprise key management
- Policy-based user access controls protect against privileged insider risks
- Detailed logging and audit trails for improved compliance reporting

The Problem: Databases Are Central Repositories Of Highly Sensitive Data That Require Security

By their mission, databases serve as repositories for vast quantities of data much of which is considered highly sensitive. The value of this kind of centralization to enterprises is invaluable as it allows for a range of uses that drive operations. Yet, for the same reasons that these kinds of repositories are attractive to enterprises, so too are they attractive to attackers. In addition to worrying about the risk of a data breach, organizations must also address the compliance obligations that come along with handling such sensitive, highly regulated data.

Neo4j amplifies the power and value that organizations traditionally would find in a database by extending the degrees to which relationships between data are stored and queried. Its graph technology and visualization tools allow organizations to extract



greater insights from their data and innovate more creatively. Yet, the data that enterprises store in Neo4j Graph Database is still sensitive and subject to the same risks and obligations as in traditional relational databases. For an enterprise to safely get the most out of their Neo4j deployments they need to think about security.

Fortunately, Thales partners with Neo4j to address these common security and compliance concerns.

The Solution

CipherTrust Transparent Encryption (CTE) secures Neo4j Graph Database data at the file system-level with centralized key management, privileged user access controls and detailed data access audit logging. With CTE, enterprises can secure their Neo4j Graph Database data as it resides on-premises or in cloud infrastructure.

CTE agents deploy quickly and simply on the same operating file-system as a Neo4j Graph Database. Administrators define which directories are to be encrypted and the agent will secure data as it is written to, or read from, those directories. By operating at the file-system layer, encryption and decryption operations are transparent to the Neo4j database and all applications so organizations do not need to make architecture changes, Graph Query Language (GQL) changes, or plan for downtime in order to secure their data. CTE's convenient, transparent approach allows organizations to address a wide range of data security compliance obligations with minimal disruption. CTE works together 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 Neo4j?

Combining Neo4j with CTE lets organizations secure their sensitive data while preserving the deep connections and relationships that generate greater value for on-going operations. Through the use of Thales' CipherTrust centralized key management, organizations can also incorporate their Neo4j deployment into their larger organization-wide security strategy. And, CTE's privileged user access controls and audit logging separate database security and system administration responsibilities to facilitate regulatory compliance and increase security oversight.

Simplified Deployment and Administration

CipherTrust Transparent Encryption minimizes the time and effort required to implement and maintain data at rest security for Neo4j Graph Database. CTE's implementation does not require application code, database architecture, or GQL changes making security an easy addition. Moreover, CipherTrust Manager serves as a consolidated, central management plane for encryption keys and policies for Neo4j and a wide range of enterprise storage, database and application security solutions.

Granular User Access Policy Controls and Enforcement

Through CTE, organizations have the ability to define and enforce granular, least-privileged user access policies (e.g. by user, process, file type, time of day) to Neo4j Graph Database. These policies allow specific individual users and processes access to data in clear-text while restricting the file system commands they can perform. Access controls serve as an additional layer of protection between data and systems that makes data safer. Using these access controls, organizations can allow system administrators to manage configurations and ongoing maintenance without having clear-text access to sensitive Neo4j data.

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 mean 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 Neo4j

Neo4j is the leader in graph database technology. As the world's most widely deployed graph database, we help global brands – including Comcast, NASA, UBS and Volvo Cars – to reveal and predict how people, processes, and systems are interrelated. Using this relationships-first approach, applications built with Neo4j tackle connected data challenges such as analytics and artificial intelligence, fraud detection, real-time recommendations, and knowledge graphs.

For more detailed technical specifications, please visit <https://cpl.thalesgroup.com/> or <https://neo4j.com/>



> cpl.thalesgroup.com <    

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