cpl.thalesgroup.com

THALES

Thales CipherTrust Manager for Kindite Cloud Database Encryption

Key Management for Kindite's Cloud Database Security

Key benefits:

Encryption That Preserves the User Experience

- Applications natively operate using encrypted data with no change to performance or the end-user's experience

Maximum Key Security

- CipherTrust Manager is available in a FIPS 140-2 Level 1 algorithm-safe and Level 3 tamper-proof hardware appliance – or as a virtual hardware appliance

A Fully Agnostic Solution

- Cloud agnostic by design, Kindite supports all databases and application servers.
- CipherTrust Manager can be deployed anywhere on-premises or in any cloud service provider infrastructure

Achieve Compliance

- Use key management to separate duties among administrators
- Maintain sole ownership of your encryption keys in infrastructure you control
- Track and audit access to protected data and keys

Secured, Assured Availability

- Flexible high-availability configurations suitable for geographically dispersed datacenters or service providers

The problem:

Organizations are targeted as they attempt to derive business value out of massive quantities of data.

Enterprise environments as they exist today often contain multiple applications pulling from the same large sets of data fragmented between different regions, physical data centers, or cloud service providers. Complicating the situation further is the ever-growing engineering skills gap widening with each new emerging technology which increases the risk that mistakes and misconfigurations will occur in these environments. As we see regularly, attackers often exploit these mistakes to successfully breach sensitive data.

KINDITE

The challenge:

Organizations need to secure sensitive data while keeping it available for use.

Organizations manage this against the backdrop of compliance of which control is the central tenet. When it comes to data security tools such as encryption, organizations must manage each deployment as part of a larger strategy in order to avoid key management silos with significant administrative overhead that makes demonstrating such control difficult. When these deployments include Cloud Service Providers (CSP), organizations have the added layer of concern that CSPs may have access to encryption keys which, in turn, complicates the tasks of demonstrating the level of control needed to meet their regulatory obligations. In many cases, organizations find themselves choosing amongst complicated administration processes, CSP tools that risk non-compliance or non-CSP tools that don't quite address their needs – especially when it comes to cloud databases as a service.

Fortunately, Kindite and Thales work together to address this challenge for enterprise customers.

The solution:

Kindite's end-to-end encryption solution maintains full application operability over encrypted data. Encrypted data and their associated encryption keys can be stored in physically separate locations to provide the highest level of protection and control to both data and keys. All the while, the application can process encrypted data without decryption to let business logic continue natively without needing any changes.

Thales CipherTrust Manager integrates with Kindite's encryption to securely store and centrally manage keys. Centralized key storage and management facilitates compliance and improves security by making surveillance, rotation, and deletion easier. Its access control features allow for separation of duties so that no single administrator is responsible for both the data and the cloud environment in which it resides. For sensitive, highly regulated data, external key storage and management – which assures that organizations, and not cloud service providers, are in control of the data – is a fundamental compliance requirement. Thales CiphterTrust Manager allows organizations to address their regulatory obligations in a streamlined, efficient manner.

Why use CipherTrust manager with Kindite encryption?

Securing database data without having to modify applications or database architecture better secures data without impacting business operations. Kindite and Thales offer a joint solution that helps organizations meet their database security needs.

Key Features:

- Encryption of cloud data without making application modifications
- Customer controlled key management of cloud encrypted data
- Reduced risk and improved compliance

Kindite

Kindite aims to enable enterprises unlock the full potential of their confidential and sensitive information. Kindite creates products that help organizations mitigate data leakage risks and create true zero trust environments.

For more detailed technical specifications, please visit cpl.thalesgroup.com or kindite.com

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.

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