

Trustway DataProtect DB

Trustway DataProtect DB brings to your organization a total protection of your database in the datacenter and the cloud.



Your organization's most valuable data assets reside in databases and it is imperative to protect them from the devastating and lasting impact of a breach. With internal and external threats growing, encryption provides a critical last line of defense by applying protection directly to sensitive information residing in databases across today's distributed enterprise.

In combination with Trustway DataProtect KMS based on certified architecture, Trustway DataProtect DB meets the strictest international standards and brings the highest level of confidentiality of your databases.

Connected to Trustway DataProtect KMS Trustway DataProtect DB brings to your organization a total protection of your database in the datacenter and in the cloud thanks to a centralized control of data access and a regular key rotation. Data field to encrypt is directly selected by you.

Secure sensitive column-level Data-at-Rest

Trustway DataProtect DB provides transparent column-level encryption of structured, sensitive data residing in databases, such as credit card, social security, account and national ID numbers, passwords, and email addresses.

The solution enables large amounts of sensitive data to be moved in and out of data stores by efficiently encrypting and decrypting specific fields in databases. No changes are required to applications and Trustway DataProtect DB can scale to support multiple data centers in on-premises, virtual and public cloud environments.

The solution is deployed with Trustway DataProtect KMS that provides centralized key and policy management.

Highlighted capabilities

Transparent and efficient column-level encryption

- Transparently encrypt sensitive column-level database data
- Apply granular access controls to ensure only authorized users or applications can view protected data
- Prevent database administrators (DBAs) from impersonating other users to access sensitive data.

Support cloud Initiatives

Trustway DataProtect DB and Trustway DataProtect KMS works in any cloud or virtualized environment to keep data secure so organizations can confidently pursue their cloud strategy. Even though data is in the cloud, customers remain in full control of both their data and their encryption keys.

- Deploy across on-premises, virtual and public cloud environments
- Set up encryption in the cloud more quickly with Chef recipes for easy automation.

Streamline ongoing management activities

- Built-in, seamless key rotation and data re-keying
- Reduce administration and overhead costs with centralized policy and key management.

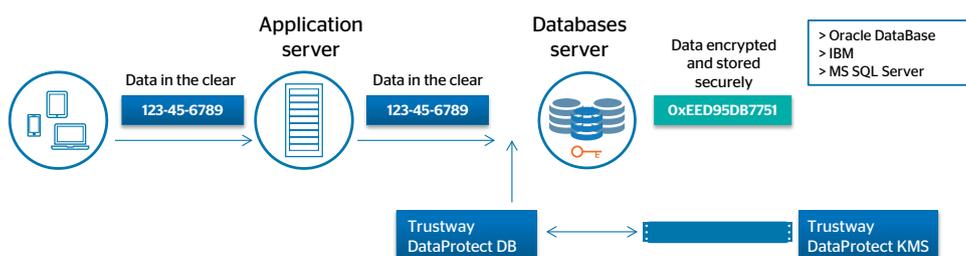
Deliver high performance

- Perform cryptographic operations locally or offload to Trustway DataProtect KMS to leverage external processing power
- Built-in connection pooling, health checking, and multi-tiered load balancing.

Achieve compliance

- Meet compliance mandates, such as GDPR, PCI DSS and HIPAA that require encryption of data and separation of duties
- Comprehensive auditing and logging capabilities to track access to encrypted data and keys.

Trustway DataProtect DB and Trustway DataProtect KMS



How Trustway DataProtect DB benefits your business

Persistent Protection

With Trustway DataProtect DB and Trustway DataProtect KMS you can ensure encrypted data remains secure throughout its lifecycle, while enabling authorized users and processes to access information when needed. Lifecycle protection increases overall security and facilitates collaboration by eliminating points of vulnerability outside the database.

Efficient encryption

With Trustway DataProtect DB and Trustway DataProtect KMS large amounts of sensitive data can be moved in and out of data stores rapidly by encrypting or decrypting specific fields in bulk within files that can contain millions of records. By focusing on select fields, you can encrypt and decrypt data efficiently, in a fraction of the time that it might take for the entire file.

Format preserving encryption functionality lets customers continue to run analytics on their data even though it is encrypted. Trustway DataProtect KMS also can be used to encrypt the entire binary file when you do not need field-level granularity.

Secure collaboration

A security solution is effective only if it enables you to use information to achieve business goals. Trustway DataProtect DB combines flexible encryption options with granular access policy capabilities so you can avoid the all-or-nothing approach of other encryption solutions. With Trustway DataProtect DB, you can encrypt data at the column-level in databases, or during batch-driven data transformation and transaction processes. The solution also lets administrators define access by variables such as: role, user, time of day and other variables.

Ensure compliance

Trustway DataProtect DB features comprehensive logging and auditing capabilities to enable you to track access to encrypted data and keys. As a result, you can effectively address your internal policies and all relevant regulatory mandates, including encrypting personally identifiable information (PII) and other sensitive, confidential data to comply with privacy mandates such as, Payment Card Industry Data Security Standard (PCI DSS) and the Health Insurance Portability and Accountability Act (HIPAA).

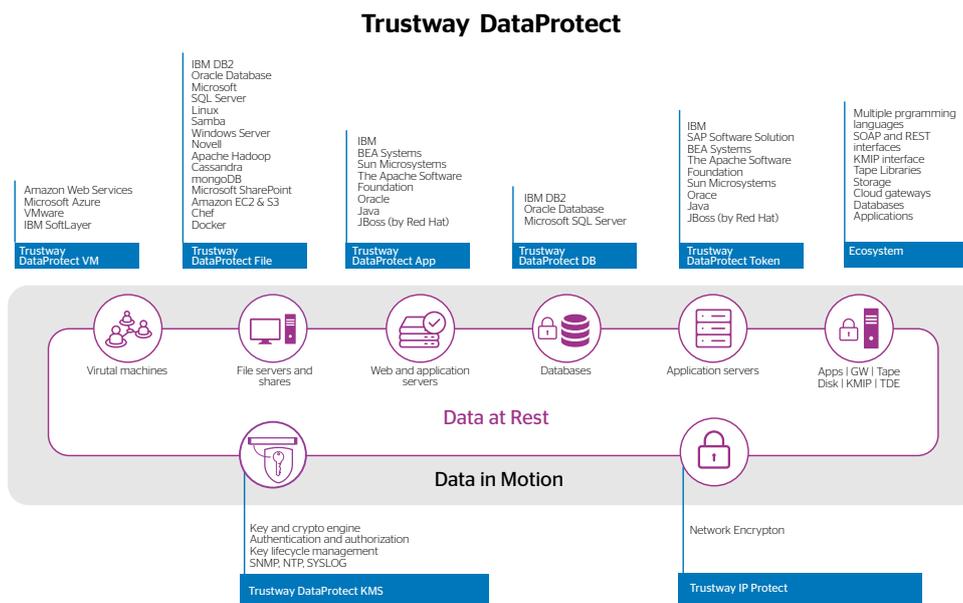
Leverage the cloud securely

Trustway DataProtect DB with Trustway DataProtect KMS cloud or virtualized environment to keep data secure so organizations can confidently pursue their cloud strategy. Even though data is in the cloud, customers remain in full control of both their data and their encryption keys.

Trustway DataProtect a scalable solution

Trustway DataProtect offers a comprehensive data encryption solution to guarantee data security and the control on the data access.

This solution provides the customer with the tools to the capabilities to encrypt all the data format as Virtual Machine, Database, File system, Application and Tokenization. Trustway DataProtect is a complete solution for cloud, virtual and on-premises infrastructures and is compliant with the most restrictive data privacy regulations as GDPR, HIPAA or PCI DSS.



Technical specifications

Features

Supported Databases	Oracle, Microsoft SQL Server, IBM DB2
Supported platforms	Microsoft windows, Linux, Solaris, HP-UX, AIX
Encryption algorithms	AES 128, 192, 256, 512 and 3DES 168
Cloud and virtual infrastructures	Works with all major cloud platforms, including AWS, Microsoft Azure and VMware

More information:

atos.net/data-encryption-trustway-dataprotect

Contact us:

atos.net/en/solutions/cyber-security-products/contact-us-cybersecurity

Atos, the Atos logo, Atos|Syntel, and Unify are registered trademarks of the Atos group. September 2020. © 2020 Atos. Confidential information owned by Atos, to be used by the recipient only. This document, or any part of it, may not be reproduced, copied, circulated and/or distributed nor quoted without prior written approval from Atos.