Trustway DataProtect File

Trustway DataProtect File provides transparent and automated file system-level encryption of server data at rest in the distributed enterprise.

Today, perimeter-based security defenses cannot adequately secure the growing volume of sensitive data residing on servers in physical, virtualized, and public cloud storage environments. To be completely protected, organizations must employ a solution that attaches security to the data itself.

Trustway DataProtect File ensures data security through fully automated file encryption of unstructured data contained in network drives and file servers. Your files can not be read by unauthorized users anymore.

In combination with Trustway DataProtect KMS based on certified architecture, Trustway DataProtect File meets the strictest international standards and brings the highest level of security of your file.

Connected to Trustway DataProtect KMS Trustway DataProtect File brings to your organization a total protection of your files thanks to a centralized control of data access.

Secure sensitive server Data at Rest in the distributed enterprise

Trustway DataProtect File provides transparent and automated file system-level encryption of server data at rest in the distributed enterprise. This includes data-centric protection of Direct Attached Storage (DAS), Storage Area Network (SAN) and Network Attached Storage (NAS) servers using CIFS/NFS file sharing protocols.

Trustway DataProtect File also features granular access controls, centralized policy and key management and comprehensive auditing capabilities. Once deployed, files containing sensitive data are rendered useless in the event of a breach, misuse or hijacking of privileged accounts, physical theft of servers, and other potential threats.

Trustway DataProtect File is deployed in tandem with Trustway DataProtect KMS, for centralized key and policy management across multiple sites. The solution encrypts sensitive data on servers, such as credit card numbers, personal information, logs, passwords, and more in a broad range of files, including word processing documents, images, database files, archives and backups.

Once deployed and initiated on a server, Trustway DataProtect File transparently encrypts and decrypts data in local and mapped network folders at the file-system level based on policies, without disruption to business operations, application performance or end-user experience.

Highlighted capabilities

Transparent, strong and efficient encryption

- Apply transparent and automated file system-level encryption in physical, virtual, and cloud environments
- Define and enforce granular access control policies.

Privileged user control

- Prevent rogue root administrators from impersonating other users and accessing protected data.

Secure data archival and destruction

- Keep data encrypted and unreadable to server administrators performing back-up and restore tasks
- Ensure all secured, sensitive data is rendered unreadable in the event data destruction is required.

Easy implementation and management

- Utilize remote, silent automation tools for quick and easy deployment in large and small environments
- Streamline administration with centralized policy and key management in FIPS certified hardware
- Built-in, automated key rotation
- Set up encryption in the cloud more quickly with automated chef recipes.

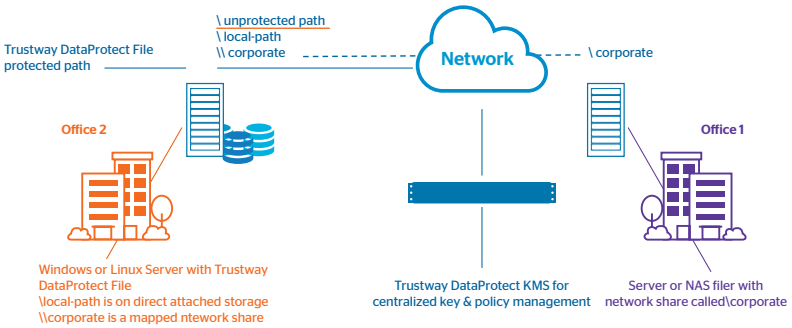
Achieve compliance

- Ensure separation of duties
- Track and audit user access to protected data and keys.

Multi-language support

- Encrypt files and folders written in Arabic, Japanese, Korean and other languages. Encryption and collaboration aren't mutually exclusive across geographies.

Trustway DataProtect File and Trustway DataProtect KMS



gemalto | SOFTWARE INSIDE

Atos

How Trustway DataProtect File benefits your business

Segregate sensitive data on shared servers

In shared server environments, different departments and work groups may store sensitive data to the same server. With Trustway DataProtect File and Trustway DataProtect KMS administrators can easily isolate data by department on a server and set policies to allow users to access segregated data only when they hold the proper encryption key.

Enable strong separation of duties

The ability to separate duties based on business-need-to-know is fundamental to security best practices, and ensures regulatory compliance, while protecting sensitive data against internal threats.

Trustway DataProtect File and Trustway DataProtect KMS enable the implementation of granular access controls that decouple administrative duties from data and encryption key access. For example, server administrators can access files and folders containing sensitive data to perform physical infrastructure management tasks, such as the back-up and archiving of data, but they will not be able to access or view the data.

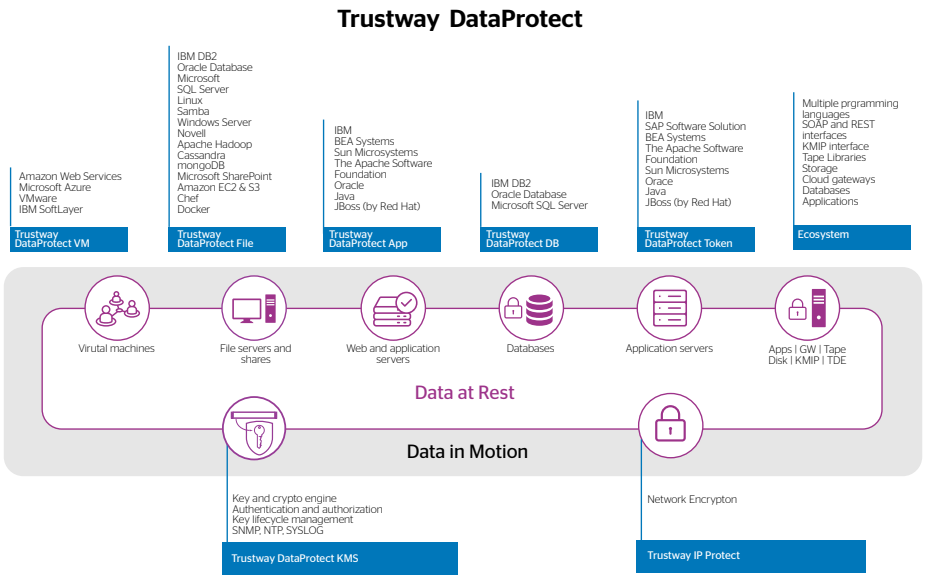
Improved compliance

Trustway DataProtect File helps achieve compliance with a variety of regulations that require encryption of data including, but not limited to, credit card numbers for Payment Card Industry Data Security Standard (PCI DSS) compliance, Personally Identifiable Information (PII) to comply with state data breach and data privacy laws, and Electronic Patient Health Information (EPHI) in accordance with HIPAA.

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	
File-system level encryption	**Servers**: A file server, web server, application server, database server, or other machine running compatible software **Network Shares**: SMB/CIFS, NFS, Remote silent installation for easy deployment in any size environment.
Supported platforms	**Linux**: Oracle, Red Hat Enterprise Linux, SUSE, Microsoft Windows **Big Data**: Apache Hadoop, IBM InfoSphere BigInsights **Cloud**: All public clouds, including AWS **Cloud Management**: Chef **Databases**: Cassandra, IBM DB2, Microsoft SQL Server, Microsoft SharePoint, mongoDB, Oracle, Couchbase **Containers**: Docker
Encryption algorithms	AES

Find out more about us
atos.net/ atos.net/en/products/cyber-security/data-encryption/trustway-dataprotect-file-encryption

CT_180921_LPM_Fs_Trustway_DataProtect_File_en1