

SMARTCRYPT TRANSPARENT DATA ENCRYPTION

Reliable Encryption for Structured and Unstructured Data

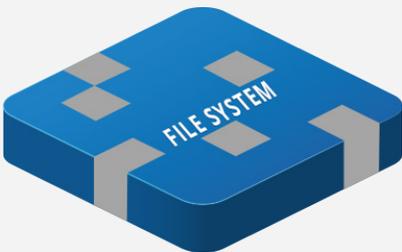
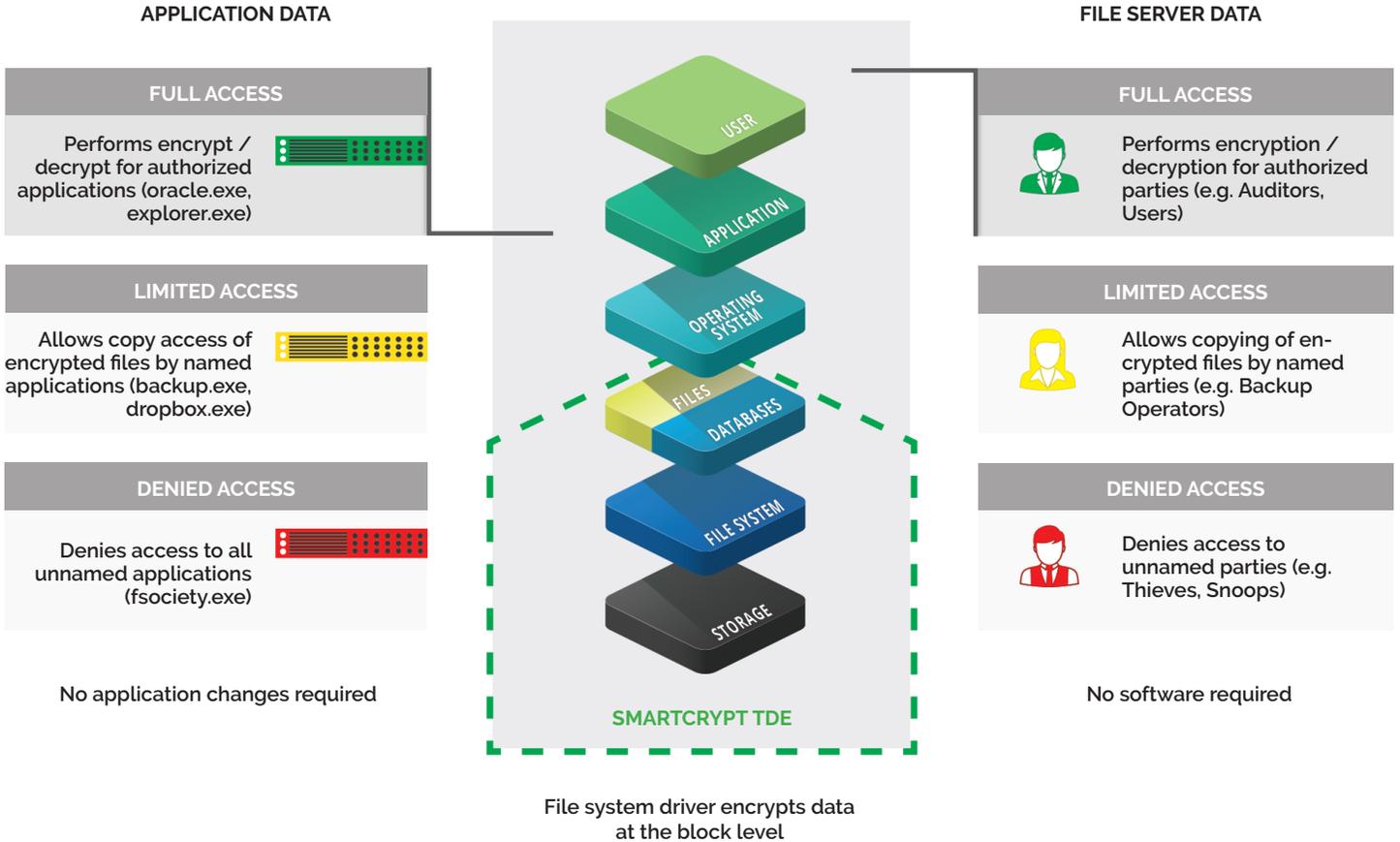
Smartcrypt Transparent Data Encryption (TDE) protects sensitive information at rest on enterprise servers, ensuring compliance with a wide range of regulatory requirements and customer privacy mandates. Smartcrypt TDE secures file and application data without application changes, additional infrastructure, or professional services. No endpoint software is required, and the user experience is unaffected.

Smartcrypt TDE is installed on application, file, and database servers containing sensitive information. Data is encrypted at the block level by a file system driver, between the operating system and the file system. Agents perform automatic encrypt/decrypt operations as data is written/read across the network.

Smartcrypt Enterprise Manager

- » Provides a web-based administration console for the deployment and management of Smartcrypt TDE agents.
- » Organizes agents into security groups for the purposes of segregating administrator access to policies, encryption keys, etc.
- » Generates encryption keys and assigns them to Smartpoints. Encryption keys can be stored in an encrypted state in the local database or via HSM.
- » Allows encryption keys to be managed in the customer's private cloud, even if servers and data reside in other public or private clouds.
- » Manages key rotation schedules for online and offline re-encryption of data. Offline key rotation is faster, but requires maintenance windows to take applications offline. Online key rotation is slower, but applications can continue to run.
- » Defines system and security administrators. Actions can be configured for single- or multiple-administrator mode requiring approval from other administrators for all actions.
- » Submits Manager and Agent events to designated SIEM or Syslog servers.

SMARTCRYPT TDE PROTECTION FOR DATA AT REST



Smartpoints

Smartpoints are designated locations on a file system that contain sensitive application data and files. Policy driven TDE agents manage encryption keys and rotation schedules for each Smartpoint. Policies support whitelists and blacklists, which allow only authorized users and applications to access and decrypt/encrypt data. TDE file system drivers manage access to specified directories and perform encryption and decryption during read and write operations.

The Smartcrypt Platform

Smartcrypt redefines enterprise data protection, providing complete administrative control while finding and protecting sensitive data on user devices, file servers, mainframes, and more, on every enterprise operating system.

The Smartcrypt Enterprise Manager, a web-based administration console, allows security managers to define encryption policies and monitor encryption and decryption activity across the organization. Smartcrypt automates key management, eliminating the complexity of key generation, exchange, synchronization, and rotation.

A Smartcrypt agent is installed on each user device or IT asset to encrypt and decrypt data in accordance with the organization's policies. Depending on the organization's unique needs, Smartcrypt agents can be deployed to address file and folder encryption, transparent data encryption, data discovery, or other data protection needs.

TECHNICAL SPECIFICATIONS: SMARTCRYPT TDE

OPERATING PLATFORMS

- » Microsoft Windows

ALGORITHMS

- » Encryption: AES256 (block level encryption in AES-CBC mode)
- » Signing: RSA 2048 SHA 512 PSS (metadata)

KEY STORAGE AND RETRIEVAL

- » OASIS KMIP
- » PKCS#11

HIGH PERFORMANCE

- » All-software solution that scales at the speed of your application
- » Takes advantage of existing hardware accelerators (Intel AES-NI and IBM Crypto Express)

HIGH AVAILABILITY / FAULT TOLERANCE

- » Each manager can support up to 2000 agents
- » Managers can be configured for failover providing fault tolerance
- » Managers can be clustered together across multiple regions for high availability