PKWARE | SMARTCRYPT

SMARTCRYPT ENTERPRISE MANAGER

ORGANIZATION-WIDE CONTROL OVER SENSITIVE DATA

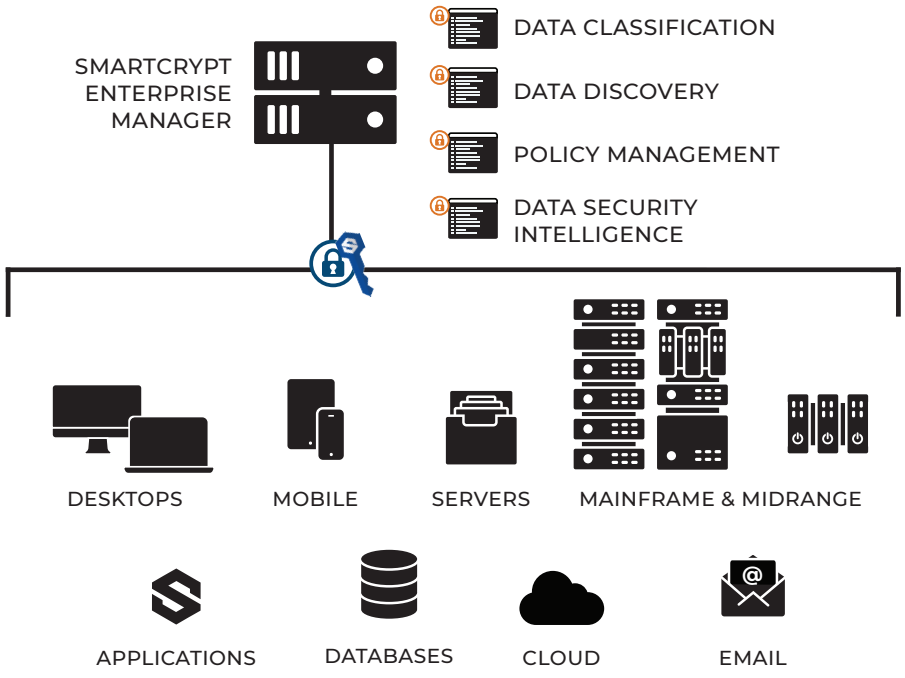
PKWARE's Smartcrypt is the only enterprise data protection solution that combines data discovery, automated classification, and protection ina single automated workflow. With Smartcrypt, organizations can secure sensitive data against internal and external cyber threats on every enterprise operating system.

EXCEPTIONAL FUNCTIONALITY AND EASE OF USE

The Smartcrypt Enterprise Manager is the central component of the Smartcrypt platform, managing the Smartcrypt agents that are installed on an organization's servers, mainframes, and user devices. It is available as software, a virtual appliance, or a hardware appliance with an optional FIPS 140-2 level 3 hardware security module and a full-entropy quantum random number generator.

The Smartcrypt Enterprise Manager allows administrators to define an organization's data security policies and apply them across the entire company. It controls encryption key management, key synchronization, and key delivery, as well as data discovery scanning, data classification, and remediation.

Administrators can use the Enterprise Manager to grant or revoke user access to encryption keys at any time, and can define policy keys to be included in every encryption operation.



PRODUCT SUMMARY

Web-based administration console used to define and apply data discovery, classification, and protection policies across the entire organization.

Manages Smartcrypt agents installed on user devices, servers, and mainframes. Provides centralized key delivery and key exchange, automating the key management process for end users.

Policy groups allow for retroactive access to content, without the need for re-encryption.

Data Security Intelligence tools provide detailed event reporting without the need for a third-party reporting tool.

Available as software-only or a hardened virtual appliance. Also available in a FIPS 140-2 Level 3 hardware appliance.

SMARTKEY TECHNOLOGY

At the core of the Smartcrypt platform is PKWARE's revolutionary Smartkey technology. With Smartkeys, businesses gain across-the-board control over who can decrypt files and read data.

A Smartkey is a unique key generated by the Smartcrypt agent for a specific file, folder, or other protected asset. Smartkeys allow administrators to add or revoke user access at any time—even if the files have been shared, copied, renamed, transferred, or emailed—ensuring full lifecycle protection.

Smartkeys are automatically generated, shared, and synchronized between authenticated devices without changing or interrupting user workflows. Smartkeys also allow users to encrypt data for external parties such as vendors or partners.

INTEGRATED WORKFLOW

Smartcrypt's data-centric security workflow provides the capabilities your organization needs to take control of your sensitive data and meet your information security goals.

Each time a file is created or modified, Smartcrypt initiates a scan based on the organization's definition of sensitive data. If the data fits one of the defined patterns, Smartcrypt initiates classification tagging and then applies strong data-level encryption or other forms of remediation, based on organizational policy.

ENTERPRISE-WIDE PROTECTION

Smartcrypt is the only data security solution that protects data on every enterprise computing platform. Encrypted files can be shared by authorized users on different systems, while remaining inaccessible to everyone else.

Administrators can use the Smartcrypt Enterprise Manager to include one or more policy keys in every encryption operation, facilitating access by DLP technology and ensuring that the organization always has control over its own data.

TECHNICAL SPECIFICATIONS

(Please refer to Smartcrypt agent datasheets for more details on supported systems.)

OPERATING PLATFORMS
Windows Server 2008, 2008 R2, 2012, 2012 R2

INTERNET INFORMATION SERVICES
IIS 7.0, IIS 7.5, IIS 8.0

SQL SERVER
SQL Server 2008, 2008 R2, 2012

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

FILE ENCRYPTION CERTIFICATE AND KEY TYPES
X.509 Digital Certificates
OpenPGP

PKWARE®

www.PKWARE.com

PKWARE provides a data-centric audit and protection platform that automates policy-driven discovery, classification, and encryption wherever sensitive data is used, shared, or stored.

CORPORATE HEADQUARTERS
201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

+ 1 866 583 1795

EMEA HEADQUARTERS
79 College Road
Suite 221
Harrow HA1 1BD

+ 44 (0) 203 367 2249