



# SMARTCRYPT FOR ENTERPRISE DESKTOP SOLUTIONS

Maintaining organizational control over increasing amounts of sensitive data demands a more evolved enterprise solution. Your organization is confronted with increasing amounts of sensitive data. Simple encryption solutions just don't get the job done. In order to maintain control over sensitive data without placing additional pressure on your IT infrastructure, you need a solution that can identify and protect sensitive information amidst increasing volumes of data, while ensuring your organization remains in control.

## Find, protect and manage sensitive information

An effective data security strategy includes the ability to identify, protect and maintain control over sensitive data, while ensuring the right individuals within your organization can access it at any time.

Smartcrypt's discovery and encryption capabilities allow security managers to apply tailored security policies to individual employees, groups or the entire organization. When sensitive information is detected, the system can apply remediation via encryption, deletion or reporting. The discovery and encryption process is transparent to end users, while PKWARE's Smartkey technology ensures that the organization maintains complete control over encryption activity. Sensitive information is secure. Access to your data is guaranteed.

## Features & Benefits

### Ensure regulatory compliance

Maintain compliance with government and industry mandates by protecting sensitive information with the most well-vetted encryption technology available. Meet requirements for auditing and reporting through Data Security Intelligence.

### Mitigate business risk.

Enforce data security and ensure data availability to mitigate risk associated with unstructured data.

### Securely sign, seal, and deliver.

Encrypt files using passphrases, X.509 digital certificates, or both. Ensure data integrity with digital signatures.

### Reduce IT infrastructure costs.

Add an additional layer of end-to-end security that does not require replacement of existing technologies.

## Protect Sensitive Information & Maintain Organizational Control of Data

Protecting and maintaining control of data requires a comprehensive solution for audit and recovery. Smartcrypt enforces encryption capabilities according to organizational policies, allowing administrators to determine what data is sensitive and should be encrypted, as well as which employees have the ability to encrypt that data. Data can be accessed by authorized individuals within the organization, ensuring data availability without fearing the auditors.

## Exchange Data Securely with External Partners

Daily business activities require information to be exchanged outside the perimeter of your organization. Huge amounts of data need to be transferred to various external partners without the risk of it being lost, stolen, or exposed once it leaves your network. Smartcrypt works across all major enterprise computing platforms, enabling secure exchange with a multitude of endpoints. Information is seamlessly and securely exchanged with external partners without impacting their budgets.

## Protect Sensitive Information during Transfer, in Storage, and on Removable Media

In order to efficiently and effectively respond to business needs, large amounts of potentially sensitive data are exchanged frequently within an organization. Smartcrypt's data-centric approach to security ensures that strong encryption is applied to the data and remains with it in storage and during all steps of the transfer process. In addition, information placed on removable media, including CDs, tapes, and USB drives also remains protected, even if lost or stolen. Reducing file size using ZIP compression and adding strong encryption ensures that information can be moved securely and efficiently.

## Meet Data Security Compliance Standards and Requirements

Internal policies, industry mandates, and government regulations demand strong protection of sensitive data. Smartcrypt strongly encrypts data using passphrases, X.509 digital certificates, or both to meet a host of compliance requirements, including the FIPS 140 data security standard. Using FIPS mode, burden on individual users is eliminated as all sensitive data transmitted is in compliance with FIPS requirements.

## Avoid Liability Risk by Protecting Information Exchanged via Email

A data security breach could lead to irreparable damage to your reputation and revenue. Smartcrypt integrates naturally into existing workflows and provides end-to-end data encryption, ensuring your sensitive information is always protected both inside and outside your organization, even when sent via email. Avoid the costs, legal penalties, and damaged reputations that can be caused by compromised data.

**PKWARE**<sup>®</sup>[www.pkware.com](http://www.pkware.com)**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**

PKWARE is a trusted leader in global business data protection. For three decades PKWARE has focused on data. Building on our compression expertise with the latest encryption technology, PKWARE protects data for over 35,000 customers, including government agencies and global corporations. Our software-defined solutions provide cost-effective and easy-to-implement protection that is transparent to end users and simple for IT to administer and control.