PKWARE | SMARTCRYPT

SMARTCRYPT

PKWARE's Smartcrypt is a data-centric audit and protection platform that automates data discovery, classification, and protection in a single workflow, managed from a single dashboard. With Smartcrypt, your organization can eliminate security gaps, maintain enterprise-wide control over sensitive data, and meet your data security goals.

POLICY MANAGEMENT

DISCOVERY

CLASSIFICATION

DATA PROTECTION

REPORTING

COMPANIES USE SMARTCRYPT TO

- Find and protect sensitive data on servers and endpoints
- Protect critical information from internal and external cyber threats
- Prevent the exposure of sensitive data in the event of a security breach
- Ensure compliance with cybersecurity mandates like GDPR, HIPAA, PCI DSS, and NYCRR 500
- Meet board of director requirements for information security
- Improve the effectiveness of data loss prevention processes and technology
- Securely exchange sensitive information with customers and partners
- Protect data outside the organization, including in the cloud
- Maintain control over all encryption activity across the enterprise
- Implement a corporate standard for data protection

CONTENTS

WHY SMARTCRYPT?

Cyber threats are getting harder to predict and harder to stop. The only way to be secure is to be sure sensitive data is protected everywhere, all the time.

However, **most security products leave gaps** because they:

- Focus on preventing intrusions, rather than protecting data itself
- Don't allow organizations to find out where their sensitive data really is
- Don't provide enough options for protecting data
- Only work on one or a few operating systems
- Encourage workarounds because they're too difficult to use and manage
- Or all of the above

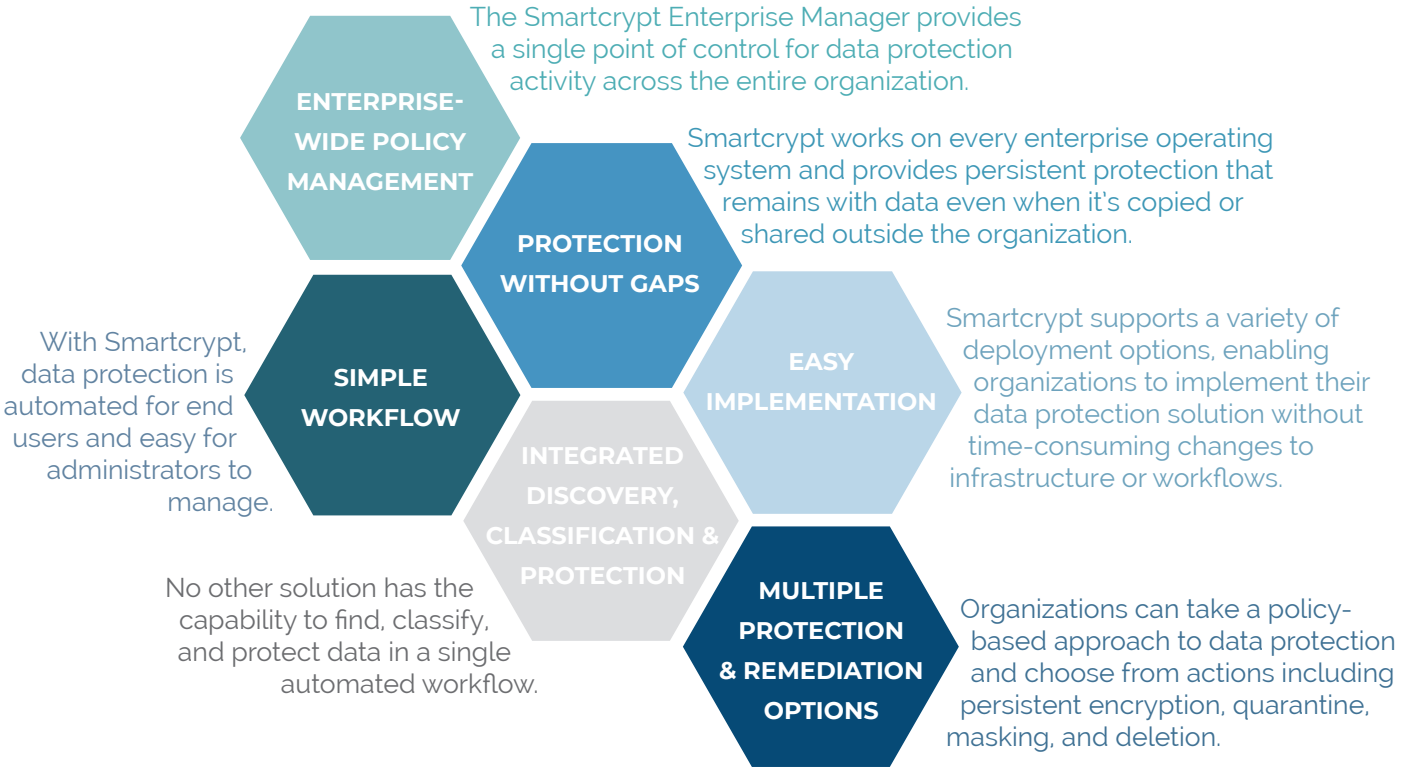
Despite the risks, many organizations continue to rely on inadequate security because they can't find solutions that address the complex challenge of protecting data in multiple locations on multiple operating systems.

COMPLETE ENTERPRISE DATA PROTECTION

PKWARE's Smartcrypt eliminates security gaps by finding, classifying, and protecting sensitive data across the entire enterprise. Smartcrypt provides capabilities no other product can match, allowing each organization to create a tailored data protection solution.

Smartcrypt agents are installed anywhere sensitive data might be created or stored: laptops and desktops, mobile devices, file servers, even midrange and mainframe systems. Smartcrypt agents apply your organization's policies each time data is created or moved, ensuring that you always have control over your sensitive information.

THE SMARTCRYPT DIFFERENCE



THE DATA-CENTRIC SECURITY WORKFLOW

Data-centric security—security that protects data itself, rather than focusing on perimeter or device protection—is the best way to manage the risks associated with large volumes of sensitive data and increasingly complex IT environments.

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.

DEFINING POLICY

Data protection begins with policies that define which types of information require protection, how the data should be protected, and which groups or individuals should be able to access it.

The Smartcrypt Enterprise Manager enables organizations to define their data protection policies and apply them across the entire organization. With preconfigured policies and tools that allow administrators to copy and modify existing policies, Smartcrypt makes it easy to tailor your solution to meet your unique security needs.

DATA DISCOVERY

Smartcrypt's intelligent data discovery feature automatically scans not only file servers, but desktops and laptops as well, providing full visibility into your organization's unstructured data. Files matching your organization's definition of sensitive data can be tagged and protected according to policy, without the need for user intervention.

DATA CLASSIFICATION

Smartcrypt can add classification tags to indicate which files contain sensitive data and how those files should be used. Classification can be handled automatically whenever Smartcrypt detects the presence of sensitive data. End users can also add tags manually to indicate that files require protection.

PROTECTION AND REMEDIATION

Smartcrypt is the only data protection platform that can discover, classify, and protect sensitive data in a single automated workflow. Your organization's policies determine what action Smartcrypt will take with files containing sensitive information:

- **Encryption:** apply persistent strong encryption that remains with data even when it is shared or copied outside your organization's network
- **Quarantine:** move sensitive files to a specified location
- **Masking:** replace sensitive text with unreadable characters
- **Deletion:** permanently delete files containing sensitive data

AUDIT AND REPORTING

Smartcrypt's Data Security Intelligence feature provides insight into data protection activity across the organization, making it easy to demonstrate compliance with internal policies, customer requirements, and government mandates.

ORGANIZATION-WIDE CONTROL: SMARTCRYPT ENTERPRISE MANAGER

The Smartcrypt Enterprise Manager is the central component of the Smartcrypt platform, allowing organizations to maintain control over sensitive data across the enterprise.

Administrators use the Manager's web-based interface to define encryption policies and manage Smartcrypt agents installed on user devices, servers, and other IT assets.

The Enterprise Manager integrates with Active Directory to simplify administration and align encryption policies with existing business processes and workflows. Security administrators can configure policy groups to enable multiple levels of access for different departments or user profiles within the organization.

Smartcrypt's advanced reporting capabilities give security administrators and auditors full visibility into encryption activity. Administrators can monitor which files have been protected, who has access to the files, and where the files have been shared. Security reports can be generated using the data security intelligence interface in the management console.

DEPLOYMENT OPTIONS

The Smartcrypt Enterprise Manager is available as software, a virtual appliance, or a hardware appliance.

When deployed as software, the Smartcrypt Enterprise Manager can be integrated with an organization's existing database and application infrastructure.

Smartcrypt Appliances offer streamlined deployment, together with enhanced security capabilities, including an optional FIPS 140-2 Level 3 hardware security module and a full-entropy quantum random number generator.

Virtual Appliance: Smartcrypt Enterprise Manager 200v
The Smartcrypt Enterprise Manager 200v is suited for any customer that wants to take advantage of a turnkey virtual appliance.

Hardware Appliances: Smartcrypt Enterprise Manager 300 series
The 300 series is suited for organizations that need or desire the higher rigor of an FIPS 140-2 Level 3-validated HSM or a full-entropy random number generator.

300h: includes FIPS 140-2 Level 3 hardware security module (HSM)
300r: includes full-entropy quantum random number generator
350: includes FIPS 140-2 Level 3 HSM and full-entropy quantum RNG

WHERE DOES SMARTCRYPT WORK?

In a word, everywhere.

Unlike products that protect data on only one or a few operating systems, Smartcrypt works on every enterprise computing platform, eliminating gaps in protection and eliminating the need for multiple point products.

Smartcrypt agents are installed anywhere sensitive data might be created or stored: laptops and desktops, mobile devices, file servers, even midrange and mainframe systems. Smartcrypt agents apply your organization's policies each time sensitive data is created or moved.

DESKTOPS & LAPTOPS

Smartcrypt agents monitor file activity on desktops and laptops, automatically classifying and protecting sensitive data as soon as it appears. Files containing sensitive data can be encrypted, quarantined, moved, masked, or deleted, based on your organization's security policies. Smartcrypt is compatible with Windows, Mac, and Linux operating systems and integrates with Microsoft Office applications.

EMAIL

Smartcrypt provides a streamlined, intuitive workflow for encrypting and decrypting emails. The Smartcrypt Outlook add-in encrypts outgoing messages that contain sensitive information without the need for user intervention. Authorized message recipients use Smartcrypt or PKWARE's free Smartcrypt Reader to decrypt and open encrypted messages.

FILE SERVERS

Administrators can create detailed encryption policies that govern which locations and types of files require protection, and what forms of protection should be applied. Smartcrypt's persistent encryption remains with files when they are moved or copied from servers, eliminating the possibility that an unauthorized user could access sensitive information in a stolen or mishandled file.

MAINFRAME

Smartcrypt is the most flexible, high-performance z Systems encryption solution available. Unlike other encryption products (including native mainframe encryption solutions), Smartcrypt applies persistent protection that stays with data even after it leaves the mainframe environment.

MIDRANGE

Smartcrypt is the only data protection solution that applies persistent encryption to information on IBM Power Systems, securing data against unauthorized access no matter where it is shared or stored. Data can be encrypted with passphrases or using OpenPGP or X.509 certificates, and decrypted by authorized users on any operating system.

MOBILE

Smartcrypt encrypts and decrypts data on iOS and Android mobile devices with a minimum of user involvement. The Smartcrypt mobile app is synchronized to each user's Smartcrypt profile, giving users access to the same encryption keys they use on other devices. Smartcrypt allows users to open encrypted files, and to encrypt files including documents, photos, and videos before sending them to other users or saving them in the cloud.

ENTERPRISE-WIDE PROTECTION, NO DATA SILOS

Thanks to Smartcrypt's cross-platform operability, data protected by Smartcrypt on one operating system can be accessed by authorized users on any other operating system. PKWARE's innovative Smartkey technology automates encryption key management and makes it easy for administrators to grant and revoke access to protected information.

TYPICAL USE CASES

Smartcrypt can help your organization meet its most significant data protection challenges. From meeting compliance obligations to protecting data against internal and external threats, Smartcrypt offers capabilities that no other data protection product can match.

SECURE DATA EXCHANGE

Secure data exchange takes place between individuals, applications, and servers. Smartcrypt applies encryption at the file level so that the protection travels with the information, preventing unauthorized access no matter where the files are copied or shared.

Smartkeys, PKWARE's innovative key management technology, can be used to manage access control at the folder or individual file level, even after a file has left the organization.

CLOUD DATA PROTECTION

Cloud storage is widely used by organizations and by employees who store work-related files in their personal cloud accounts. Sensitive data often remains unprotected in the cloud, vulnerable to a wide range of threats.

Smartcrypt can be configured to scan and protect files that are synced with cloud locations, and to apply persistent protection that remains with files in the cloud.

MAKING DLP MORE EFFECTIVE

When integrated with existing DLP, Smartcrypt provides policy key access to DLP personnel and technology, enabling decryption and scanning of end-to-end encrypted content when it has been encrypted elsewhere in the organization.

After scanning, DLP can pass the encrypted content along, allowing the security to remain intact, or block the transmission after it has scanned the encrypted content.

ENDPOINT DATA PROTECTION

With Smartcrypt, organizations maintain complete control over sensitive information on laptops, desktops, phones, and tablets, even after the data is copied or shared.

Smartcrypt integrates with Microsoft Office, allowing users to protect and access sensitive data without disruptions to their normal workflows.

ELIMINATING UNCONTROLLED ENCRYPTION

Uncontrolled encryption can be as problematic as a lack of encryption. Smartcrypt can be configured to include at least one of the organization's public keys in every encryption operation, eliminating the possibility that the organization could lose access to its own data.

REGULATORY COMPLIANCE

Businesses, government agencies, and other organizations must deal with constantly-changing requirements that dictate how sensitive data must be protected. Smartcrypt makes it easy to comply with government regulations and industry mandates like GDPR, HIPAA, PCI DSS, and NYCRR 500.

MORE OPTIONS: SMARTCRYPT TDE & APPLICATION ENCRYPTION

At PKWARE, we know that one size does not fit all. Each organization faces unique security challenges and has a unique set of data protection priorities.

The Smartcrypt platform includes additional options for organizations that need to address specific concerns relating to data at rest, or that need to incorporate strong data protection into their proprietary applications.

SMARTCRYPT TRANSPARENT DATA ENCRYPTION (TDE)

Smartcrypt Transparent Data Encryption (TDE) protects sensitive information at rest on enterprise servers and ensures compliance with a wide range of regulatory requirements and customer privacy mandates while protecting data from unauthorized access.

Installs in one hour: Smartcrypt TDE is easy to implement and can often be installed in one hour or less. Smartcrypt's ease of deployment makes it a popular choice for organizations who need to implement encryption on short timelines and without heavy demands on IT resources.

Easy configuration and management: The Smartcrypt Enterprise Manager, PKWARE's data protection administration console, provides a powerful, easy-to-use interface for information security managers. Using the Smartcrypt Enterprise Manager, administrators can deploy TDE agents on servers, define encryption policies, grant access to users and applications, and monitor data protection activity in real time.

Software-defined solution: Unlike TDE products that require specialized hardware, Smartcrypt TDE is a software-defined solution that can be installed on an organization's servers without the need for additional infrastructure. Smartcrypt's software-only approach makes it more cost effective than other solutions, as well as easier to implement and manage.

SMARTCRYPT APPLICATION ENCRYPTION

Smartcrypt Application Encryption is the ideal solution for organizations who need to incorporate strong encryption into their products or systems. A powerful software development kit, Smartcrypt Application Encryption delivers high performance, cross-platform security that is easily embedded, insulating sensitive data from weaknesses in other systems that may handle the information.

Smartcrypt Application Encryption is available in all major programming languages, including C++, Java, and C#, and can be used to encrypt both structured and unstructured data. Changes to existing applications typically consist of two or three lines of code.

Encryption for structured data: Smartcrypt Application Encryption supports multiple options for preserving data length and formatting to ensure referential integrity across the database. This approach streamlines the integration of the SDK and minimizes disruptions for developers and database administrators.

Encryption for unstructured data: For applications that process sensitive information stored in files, Smartcrypt provides persistent encryption that prevents unauthorized access, even when files are moved or copied outside an organization's network.

The Smartcrypt platform includes additional options for organizations that need to address specific concerns relating to data at rest, or that need to incorporate strong data protection into their proprietary applications.

MORE SOLUTIONS ON MORE OPERATING SYSTEMS

No other company can match PKWARE's data protection capabilities. Smartcrypt gives your organization the ability to create a tailored solution that protects sensitive data on every enterprise operating system, without disrupting the way you do business today.

CAPABILITY	DIGITAL GUARDIAN	GEMALTO	IBM	IONIC	PROTEGRITY	SECLORE	SOPHOS	SYMANTEC	THALES	VERA	VOLTAGE	PKWARE
File Encryption: Desktops and Laptops	✓			✓		✓	✓	✓		✓	✓	✓
File Encryption: Servers	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Data Discovery	✓		✓		✓		✓	✓				✓
Data Classification	✓			✓	✓	✓		✓				✓
Data Masking		✓	✓		✓			✓	✓		✓	✓
Email Encryption	✓			✓		✓	✓	✓		✓	✓	✓
Cloud Encryption	✓	✓	✓	✓	✓	✓		✓	✓	✓	✓	✓
Mobile Encryption				✓		✓	✓	✓		✓	✓	✓
Database Encryption		✓	✓	✓	✓				✓		✓	✓
Application Encryption		✓	✓	✓	✓			✓	✓	✓	✓	✓
Mainframe Encryption (z Series)			✓		✓						✓	✓
Midrange Encryption (IBM i)			✓		✓						✓	✓
Persistent Encryption	✓			✓	✓	✓		✓		✓	✓	✓

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