

# SMARTCRYPT DATA DISCOVERY

## Intelligent Identification and Protection for Sensitive Data

As companies around the world grow, transform, and compete, the amount of data they generate and process is growing exponentially. In order to build customer trust and create competitive advantage, businesses must protect their rapidly expanding data from internal and external threats.

To keep data safe, organizations must first find where sensitive information resides in their networks and devices, and then take steps to protect that data. Unfortunately, traditional discovery solutions provide limited remediation options—blocking actions or deleting data—that have little practical value. The few discovery solutions that offer data protection require customers to accept woefully inadequate implementations, often forcing entire companies to share a single encryption key.

Traditional data protection solutions are equally limited. The vendors who do offer quality data protection products don't offer discovery capabilities. The lack of adequate solutions for discovery and data protection can leave an organization vulnerable while it searches for a path forward.

### Smartcrypt: Integrated Data Discovery, Strong Encryption, and Key Management

PKWARE's Smartcrypt integrates intelligent data discovery with strong data-level encryption—and does it in the same workflow. It's the simplest, most integrated way for organizations to identify sensitive information and protect it against loss, theft or misuse.

Smartcrypt's data discovery feature uses the Smartcrypt for Files and Folders agent to continuously monitor storage locations for sensitive information. Each time a file is added or modified, Smartcrypt initiates a scan based on the organization's policies. If data fits one of the defined patterns, 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 the organization maintains complete control over encryption activity.

### WHAT IS SENSITIVE DATA?

Smartcrypt can detect and remediate sensitive data based on a wide range of criteria. Agents can be configured to search for data based on common formats such as credit card account numbers or Social Security numbers, or based on industry or government mandates including those listed below.

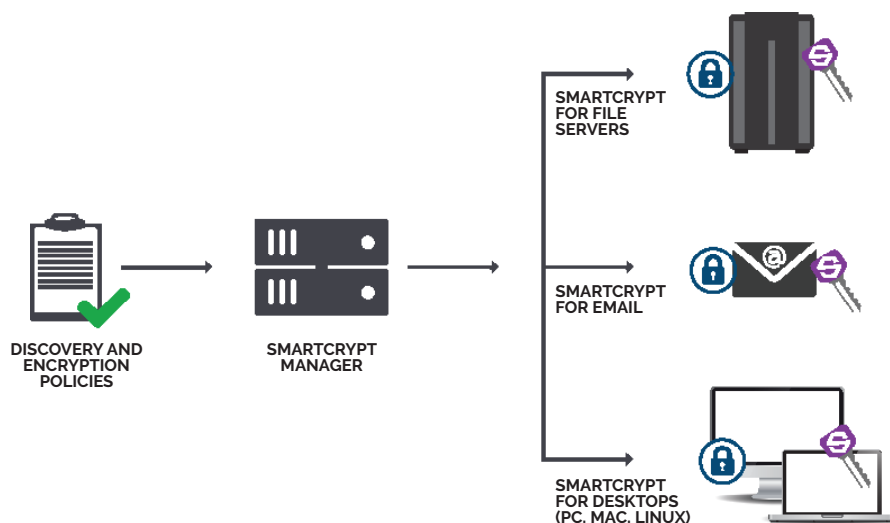
- » PII
- » PHI
- » PCI
- » GLBA
- » HIPAA
- » HITECH
- » FERC/NERC/CEII
- » FERPA
- » FISMA
- » ITAR
- » SOX
- » GDPR

In addition, Smartcrypt can identify and encrypt data that meets an organization's own definition of sensitive information, such as source code and other intellectual property.

## Encryption as Part of the Discovery Workflow

Organizations can use Smartcrypt to identify and encrypt sensitive information in network storage locations or user desktops and laptops, ensuring persistent data protection and unprecedented visibility.

- Administrators create filters consisting of one or more data patterns
- Filters can be grouped together in filter bundles based on compliance mandates (HIPAA, PCI, etc.) or business processes
- Administrators apply filters and filter bundles to employees, groups, or selected file storage locations on servers or NAS ("lockers")
- Administrators select the remediation to be applied when a file meets the definition of sensitive data (encrypt/delete/report), along with the encryption keys to be used in remediation
- Any file activity on an employee's device or in a locker triggers a discovery scan (and remediation if needed)
- When reporting is enabled, every remediation event is captured in full detail
- Administrators can grant or revoke access to encrypted information at any time



### TECHNICAL SPECIFICATIONS

#### OPERATING PLATFORMS

- » Microsoft Windows
- » Linux: RHEL (.rpm) and SLES (.deb)\*

#### 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

- » Smartkeys
- » X.509 Digital Certificates
- » OpenPGP

