PKWARE & BOLDON JAMES

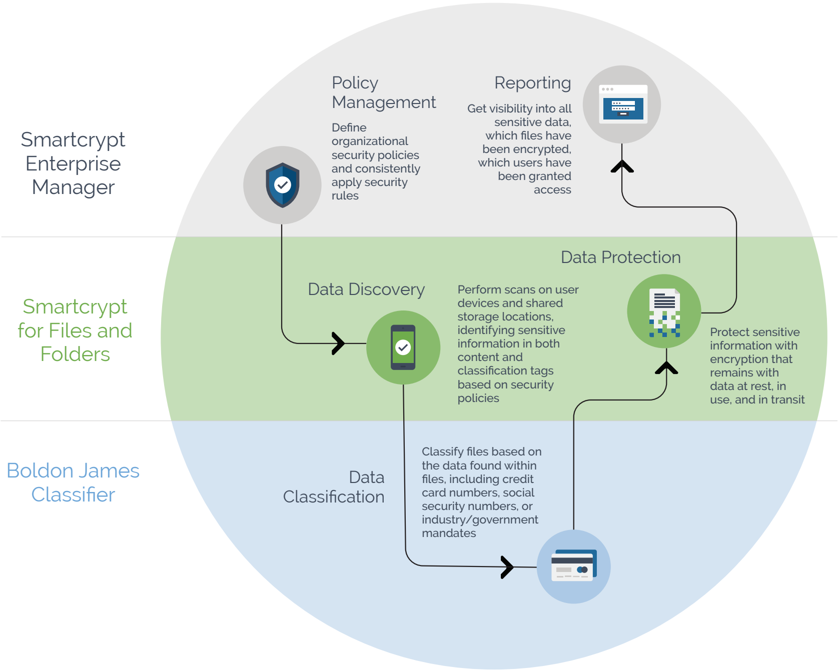
BRINGING DATA DISCOVERY, CLASSIFICATION, AND DATA PROTECTION INTO ONE SIMPLE WORKFLOW

Security experts often recommend using data discovery, data classification, and encryption to keep data safe from internal and external cyber threats. But the options are less than ideal: organizations either have to manage three or more stand-alone products, settle for solutions that are missing required capabilities, or—worst of all—choose to leave their sensitive data undiscovered, unclassified, and unsecured while they search for a path forward.

INTEGRATED DISCOVERY, CLASSIFICATION, AND ENCRYPTION

PKWARE's Smartcrypt and Boldon James Classifier integrate to combine these capabilities in one simple workflow. It's the simplest, most efficient way for organizations to control and secure their sensitive information against loss, theft, or misuse.

Smartcrypt automatically scans servers, laptops, and desktops for sensitive data, based on classification tags or file contents. When sensitive data is detected, Smartcrypt initiates tagging vis Boldon James Classifier (for files that are not already classified), and applies encryption, masking, or other protective measures based on the organization's security policies.



Smartcrypt Enterprise Manager

Policy Management

Define organizational security policies and consistently apply security rules

Reporting

Get visibility into all sensitive data, which files have been encrypted, which users have been granted access

Smartcrypt for Files and Folders

Data Discovery

Perform scans on user devices and shared storage locations, identifying sensitive information in both content and classification tags based on security policies

Data Protection

Protect sensitive information with encryption that remains with data at rest, in use, and in transit

Boldon James Classifier

Data Classification

Classify files based on the data found within files, including credit card numbers, social security numbers, or industry/government mandates

SOLUTION HIGHLIGHTS

Integrated data discovery, classification, and encryption

Finds legacy sensitive data throughout the organization and automatically applies classification and remediation

Supports user-driven classification, automatic classification, or a combination of approaches

Applies persistent encryption that remains with data at rest, in use, and in transit

Metadata associated with encrypted files remains readable by DLP tools

PKWARE's data compression technology reduces file sizes by up to 90%,

Smartkey technology enables enforced access control defined by classification or user/group

Data Security Intelligence tools provide advanced reporting functionality

Protection can be applied to files at the point of creation, as well as to legacy files that were created before the solution was introduced.

With this joint solution, organizations can ensure that their sensitive data is appropriately protected and classified across the enterprise.

DEFINE POLICIES AND RULES

Administrators use the Smartcrypt Enterprise Manager to define and apply the organization's data discovery, classification, remediation, and encryption policies. Smartcrypt ensures complete access and control of sensitive data at all times.

FIND FILES CONTAINING SENSITIVE DATA

Smartcrypt uses an agent to continuously search for Boldon James Classifier-tagged files on servers, laptops, and desktops.

Smartcrypt can also identify sensitive files by inspecting file contents and comparing them to the organization's definition of sensitive data. Administrators define both the sensitive information they want to find as well as the locations they want to search for it.

CATEGORIZE SENSITIVE FILES

Boldon James Classifier allows users to assign a visual label to the files they create, and then turns that visual label into metadata classification labels. These labels are used by Smartcrypt to identify and protect sensitive information.

Companies can choose the right data classification approach for their business whether it be user-driven classification, automatic classification, or a blend of classification techniques.

APPLY REMEDIATION

Smartcrypt applies remediation based on the classification label or content found within a file. Available actions include deletion, masking, reporting, quarantine, or application of persistent encryption using a predefined encryption key.

MONITOR AND REPORT

Administrators can use Smartcrypt's Data Security Intelligence tools to monitor data protection activity and provide reports for audit and compliance needs.

PRODUCTS NEEDED FOR THIS INTEGRATION:

SMARTCRYPT ENTERPRISE MANAGER (available as a hardware or virtual appliance)

OPERATING PLATFORMS: Windows Servers 2008, 2008 R2, 2012,2012 R2

INTERNET INFORMATION SERVICES: IIS 7.0, IIS 7.5, IIS 8.0

SQL SERVER: 2008, 2008 R2, 2012, 2014

SMARTCRYPT FOR FILES & FOLDERS

OPERATING PLATFORMS: Microsoft Windows (Vista or later); Linus RHEL and SLES

ALGORITHMS: AES256 (encryption); RSA 2048 SHA 512 PSS (signing)

CERTIFICATE & KEY TYPES: Smartkeys, X.509 Digital Certificates, OpenPGP

SMARTCRYPT FOR FILES & FOLDERS

OPERATING PLATFORMS: Microsoft Windows (Vista or later)

MICROSOFT OFFICE: 2007-2016; OFFICE 365

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