PKWARE®

DATA SHEET

PKWARE
DATA CLASSIFICATION

ENHANCED VISIBILITY AND CONTROL OVER SENSITIVE INFORMATION

Data classification is an essential component of enterprise data protection, allowing administrators and end users to identify files and messages that contain sensitive information. However, most classification products provide limited capabilities, requiring organizations to manage separate solutions in order to locate sensitive data before tagging and protect files afterward.

PKWARE provides the only data security platform that includes data classification in an automated workflow with data discovery and protection. It's the simplest, most efficient way for organizations to secure their sensitive information against loss, theft, or misuse.

THE VALUE OF INTEGRATION

When classification is integrated with data discovery and protection, organizations gain greater control over sensitive data while simplifying administration.

PKWARE's integrated approach to data classification enables automatic policy-based tagging for files that contain sensitive data on laptops, desktops, and servers across the enterprise.

PKWARE scans new or modified files for sensitive information as defined by the organization. When sensitive data is detected, PKWARE initiates classification tagging and applies encryption, masking, or other protective measures based on the organization's security policies. Classified files contain visual tags that alert users to the sensitivity of the data, as well as metadata tags that facilitate action by DLP scanners and other security technology.

PKWARE also allows end users to apply manual classification to files that require protection even though they do not fit the organization's definition of sensitive data. After manual classification, PKWARE will automatically apply the appropriate form of protection to the tagged file.

While other solutions lack the ability to tag files that were created before a classification tool was introduced, PKWARE can automatically classify legacy data, as well as classifying files at the point of creation.

SOLUTION HIGHLIGHTS

- Integrates data classification in a unified workflow with data discovery and protection
- Automatically applies visual and metadata tags to files that contain sensitive information
- Finds existing 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
- Smartkey technology enables enforced access control defined by classification or user/group
- Data Security Intelligence tools provide advanced reporting functionality

MINIMIZE HUMAN ERROR

Human error is to blame for a large percentage of security breaches. Heavy workloads, new technology, and insufficient training can lead employees to violate data security policies unintentionally.

Data classification keeps employees engaged in the data protection process by increasing user awareness and empowering users to take action when files require special handling.

Visual labels on classified files help employees maintain awareness of the organization's data protection policies and the need to handle data appropriately. PKWARE's email classification feature facilitates manual or automatic tagging of Outlook messages, extending the organization's data protection policies to partners, vendors, or other parties who receive sensitive information.

While other classification products can create a false sense of security by tagging files but leaving them otherwise unprotected, PKWARE applies policy-based protection as soon as sensitive data is discovered and classified. Protected data remains safe from unauthorized use, even when it is shared or copied outside the company network.

MAINTAIN ENTERPRISE-WIDE CONTROL

PKWARE ensures that the organization maintains complete access and control over sensitive data at all times.

Administrators use the PKWARE Enterprise Manager to define and apply the organization's data discovery, classification, and remediation policies. Policies can include detailed rules and security workflows for different user groups, locations, and forms of sensitive data.

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

TECHNICAL SPECIFICATIONS

PKWARE 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 7.5m
- IIS 8.0

SQL Server:

- 2008
- 2008 R2
- 2012
- 2014

PKWARE ENDPOINT AGENT

Operating Platforms:

- Microsoft Windows
- Linus RHEL and SLES

Algorithms:

- AES256 (encryption)
- RSA 2048 SHA 512 PSS (signing)

Certificate & Key Types:

- Smartkeys
- X.509 Digital Certificates
- OpenPGP