PKWARE

PKWARE DATA SECURITY

PKWARE's data security platform monitors and protects sensitive information in files on endpoints, servers, and beyond. With PKWARE, you can protect each type of data the right way, and enforce your organization's security policies in real time.

PKWARE detects sensitive data as files are created and modified, and takes automated action based on company policy.

- Data is protected from the moment of creation, and stays protected as it's copied and shared
- Data security rules and workflows can be tailored to meet your unique requirements
- Administrators gain visibility into file contents and user actions
- End users can do their jobs without disruption and without putting data at risk

PKWARE helps you take control of sensitive data and meet your data security and compliance goals.

COMPANIES CHOOSE PKWARE TO HELP THEM...

CLOSE COMPLIANCE GAPS

PKWARE solutions can help you meet requirements under GDPR, CCPA, PCI DSS and other regulatory and industry mandates.

- Encrypt personal information
- Classify files containing sensitive data
- Redact credit card data in files
- Report on file contents and activity

MEET CUSTOMER REQUIREMENTS

PKWARE gives you the capabilities you need to secure your customers' data, build trust, and gain a competitive advantage.

- Exchange sensitive data with confidence
- Protect intellectual property
- Meet service level agreements

IMPROVE SECURITY WORKFLOWS

PKWARE has the expertise and technology to solve even the most complex security use cases.

- Integrate encryption with DLP scanning
- Simplify encryption key management
- Exchange data securely across platforms
- Eliminate gaps in protection

SUPPORT ORGANIZATIONAL CHANGE

PKWARE's flexible solutions help you pursue new opportunities and take advantage of new technology without compromising on security.

- Move data to the cloud without giving up control
- Scale your security solutions to accommodate growth
- Share data securely with new partners

AUTOMATED DATA SECURITY

PKWARE's automated technology monitors file activity in real time, and takes policy-based action every time sensitive data is saved or modified in a file.

POLICY MANAGEMENT

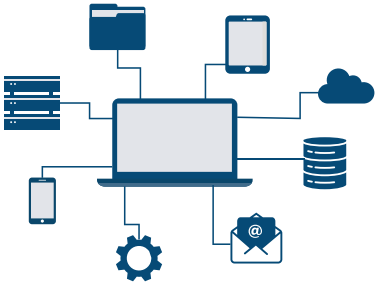
Administrators use the PKWARE Enterprise Manager to define data security policies and deploy PKWARE agents on endpoints and servers.

Policies determine which types of data require remediation, and which actions the system should take. Policies can specify different forms of remediation based on file format, file contents, file location, and user profiles.

DISCOVERY AND REMEDIATION

PKWARE agents on laptops, desktops, servers, and other IT assets enforce the organization's security policies as files are created and modified.

When PKWARE detects sensitive data in a file, it applies the correct form of remediation (including classification, encryption, redaction, quarantine, or deletion) without the need for user intervention.



ORGANIZATION-WIDE INTEGRATION

PKWARE is the only security platform that supports every enterprise operating system, including Windows, Mac, Linux, UNIX, mainframe and midrange systems, and mobile devices.

PKWARE also integrates with productivity software, reporting tools, and other security technology such as DLP and multi-factor authentication solutions.

REPORTING

PKWARE's Data Security Intelligence tools provide real-time, immutable logging of data discovery scans, file classification changes, and file encryption and decryption events. PKWARE's detailed reporting makes it easy to demonstrate compliance to auditors, regulators, and customers.

SOLVING THE COMPLIANCE PUZZLE

PKWARE provides a feature-rich framework for meeting requirements under GDPR, the California Consumer Privacy Act, PCI DSS, and many other data protection laws and standards.

With PKWARE, organizations can create tailored policies and workflows to meet their unique compliance goals, or use PKWARE's preconfigured policies to streamline implementation.

PKWARE'S APPROACH TO COMPLIANCE

PKWARE knows that compliance is a multi-faceted effort, requiring involvement from multiple departments, vendors, and partners. Our solutions are designed to fit into—and enhance—your organization's overall compliance strategy.

FLEXIBILITY

PKWARE's data-centric approach makes it possible to apply the right protection to each type of sensitive data. Whether you need to take action based on file format, file location, file contents, or user profiles, PKWARE gives you the tools to get it done.

INTEROPERABILITY

PKWARE supports every enterprise operating system, facilitating company-wide policy enforcement. Sensitive data stays protected (and reportable) as it moves throughout your organization.

INTEGRATION

PKWARE solutions integrate with productivity software, reporting systems, and existing security technology within your IT ecosystem. PKWARE can take action based on input from other applications, and/or apply tags to trigger action by downstream technology.

A TRUSTED PARTNER

Fortune 100 companies, government agencies, and other organizations use PKWARE to meet requirements under data security laws and industry mandates around the globe:

- GDPR
- California Consumer Privacy Act
- PCI DSS
- HIPAA
- HITECH
- NYCRR 500
- TISAX
- NIST Cybersecurity Framework
- FIPS 140-2

AUTOMATION

PKWARE handles tasks automatically, simplifying user training and minimizing disruption. Once your PKWARE agents are deployed, they monitor file activity in real time, applying your policies every time files are created or modified.

PKWARE DATA SECURITY: USE CASES

AUTOMATED FILE ENCRYPTION

PKWARE file and folder encryption is the only enterprise data protection solution that combines intelligent data discovery, persistent encryption, and streamlined key management.

With PKWARE, organizations can apply encryption policies across every enterprise operating system. protect sensitive data from unauthorized use, and meet their data security compliance obligations.

PKWARE's automated data protection technology detects sensitive data as soon as it appears on a laptop, desktop, or server, and applies persistent strong encryption based on organizational policy.

Unlike solutions that protect data only on certain devices or networks, PKWARE's persistent protection travels with the data no matter where the file is sent or shared, even when it's stored outside the company network.

DATA CLASSIFICATION

PKWARE Data Classification is a complete, automated solution that applies visual tags and metadata to files containing sensitive information.

PKWARE's automated technology scans new or modified files for sensitive information as defined by the organization. When sensitive data is detected, PKWARE classifies the files 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 other security technology.

In addition to automated classification, PKWARE provides the option for users to apply labels manually to files they create or modify. 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.

DATA REDACTION

One of the biggest risks for organizations is sensitive information that exists outside the organization's controlled database environment.

PKWARE's automated data redaction technology removes sensitive data from files, leaving other file contents unchanged.

Real-time file scanning ensures that sensitive data is detected and remediated as soon as it appears. PKWARE's file redaction technology can also be used to remediate existing files on user devices or servers, reducing the risk of audit failures or data breaches.

Unlike tokenization and similar technology, redaction is not reversible, allowing organizations to remove redacted files from the scope of compliance requirements.

SECURE EMAIL FOR CLIENTS AND PARTNERS

Secure email gateways create nearly as many problems as they solve. The multi-step process required to open a protected email, together with forgotten passwords and account lockouts, create frustration for message senders and recipients.

PKWARE provides a simpler, better approach for organizations that need to share sensitive information with external recipients.

Message senders can use PKWARE's Outlook add-in to encrypt emails containing sensitive data. PKWARE can encrypt the message body and any attachments, using keys that only the intended recipient can use.

To open a secure email, the authorized recipient simply downloads the message file and uses the free Smartcrypt Reader to open it with simple drag-and-drop decryption. Secure emails cannot be accessed by anyone but the intended recipient, even if they are accidentally sent or forwarded to other parties.