PKWARE

PK Protect

PK Protect

Persistent Data Security that Enhances DLP Processes and Technology

Data loss prevention (DLP) processes and technology prevent unauthorized data exfiltration and are a critical component of data breach detection strategies. Traditional DLP decision points include allowing and blocking transmissions or redirecting transmission to another party for additional decision making. But as more organizations adopt end-to-end encryption solutions, their DLP processes and technology become less effective. This results in more blocks and redirects, which in turn hinder business velocity.

DETECT DATA BREACH

PREVENT DATA LEAKING

PREVENT EXFILTRATION

Organizations need flexible data security solutions that work with existing DLP to satisfy audit and compliance requirements. This includes the capability to inspect encrypted content and provide encrypted remediation as an additional decision point.

PK Protect Suite

PK discovery

PK classification

PK masking

PK encryption

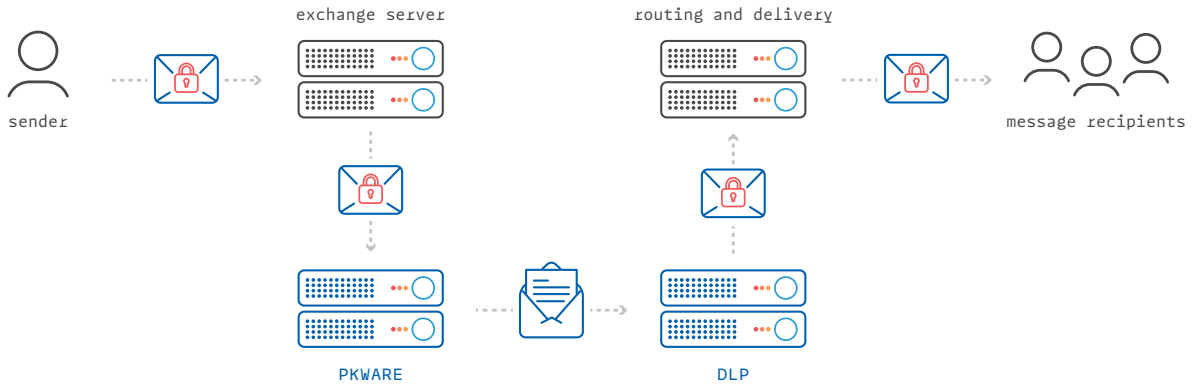
PK privacy

Policy-Based Encryption to Enhance Existing DLP

PKWARE's PK Protect suite integrates with DLP for both sensitive information discovery and encrypted remediation.

PK Protect provides policy key access to DLP personnel, along with the ability to decrypt and scan content that has been encrypted elsewhere in the organization. For network DLP, PK Protect can help DLP make informed decisions with regard to encrypted content. For example, a sender can use PK Encryption, an application of PK Protect, to encrypt sensitive data before sending a message. If the sender is permitted to share the type of information contained in the transmission, DLP will pass it along, allowing the security to remain intact. If the sender is not allowed to share the information, DLP will block the transmission after it has scanned the encrypted content.

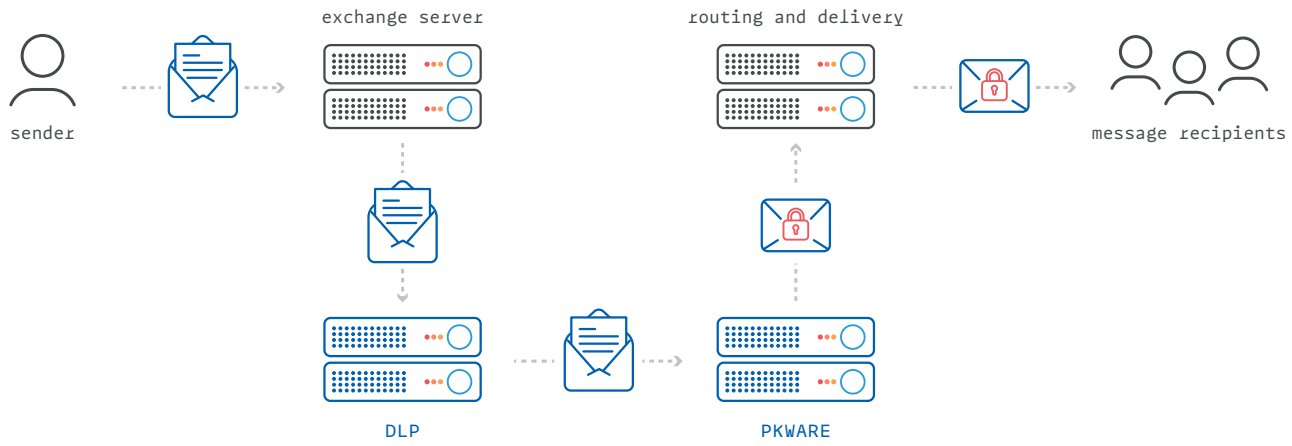
PK Protect Outlook Integration auto-encrypts email attachments using receipient key and policy key. PK Protect DLP Integration uses policy key for sensitive information discovery.



Sensitive content remains end-to-end encrypted.

For remediation, PK Protect allows DLP to secure transmissions that would otherwise be blocked. If a sender is authorized to transmit sensitive information but fails to encrypt the data before sending, PK Encryption can encrypt the message using a public key or a unique Smartkey, rather than re-routing or blocking the transmission.

DLP detects sensitive content being transmitted. Sender and Receipient are authhorized.
PK Protect provides DLP remediation.



Sensitive content now encrypted.

Efficient and Effective DLP Prevention Integration

PK Protect resides on servers, desktops, and mobile devices and is used to apply persistent file encryption. This protection travels with the files, ensuring they remain encrypted wherever they are transmitted or stored. Strong encryption can be performed with passphrases, PGP keys, X.509 digital certificates, or Smartkeys (PKWARE's embedded encryption key management system).

Regardless of which encryption system is used, administrators can use the manager console to define policy keys to be transparently included in every encryption operation. This ensures that the organization never loses access to encrypted information, and enables administrators to issue and retract policy keys for enterprise IT and audit users as needed. Policy keys can also be issued to third-party DLP and discovery tools, allowing the tools to decrypt any files they need to scan.

PK Protect can not only encrypt sensitive files within endpoints, but can discover and protect enterprise data repositories such as warehouses and lakes. By allowing users to set up intelligent data processors at petabyte-level data repositories both on-premises and in the cloud, PK Protect ensures users can utilize DLP measures across their holistic environments.

Supported Key Types:

- **Smartkeys:** PKWARE's embedded key management solution. Removes complexity from key generation, synchronization, exchange, and escrow. Smartkeys technology also simplifies challenging tasks such as re-encryption, key rotation, public key creation, and key distribution.
- **PGP Public Keys:** Any OpenPGP (GPG/PGP) RSA 2048-bit+ public key can be added into endpoint encryption operations.
- **X.509 Public Keys:** Any X.509 formatted public key—including third-party rooted and self-signed keys—can be added into endpoint encryption operations.

Extend DLP Protection with PKWARE

PK Protect solves problems resulting from uncontrolled encryption, providing the visibility organizations require in order to fully address security, audit, and compliance requirements while providing persistent protection for their data wherever it is used, shared, or stored.

With PK Protect, organizations can enforce organizational security policies, maintain control of data, and ensure data visibility.

Ready To See It Live? Contact Us!

pkware.com/demo

866-583-1795

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

Follow Us

/company/PKWARE

facebook.com/PKWARE

@PKWARE