PKWARE

PK Protect

PK Protect

Make DLP Processes More Efficient and Effective

Data loss prevention (DLP) technology is an essential component of today's enterprise cybersecurity strategies, allowing organizations to detect data breaches and prevent unauthorized data transmission or exfiltration.

DETECT DATA BREACH

PREVENT DATA LEAKING

PREVENT EXFILTRATION

Data encryption, while also critically important for enterprise cybersecurity, often makes DLP less effective, especially when encryption is applied by end users without organizational control. When encrypted email messages or files are submitted for inspection, the encryption renders the data unreadable to DLP scanners. Administrators must choose between two undesirable options: allowing the encrypted data to proceed without inspection or redirecting it for time-consuming manual follow-up.

PK Protect Suite

PK discovery

PK classification

PK masking

PK reporting

PK privacy

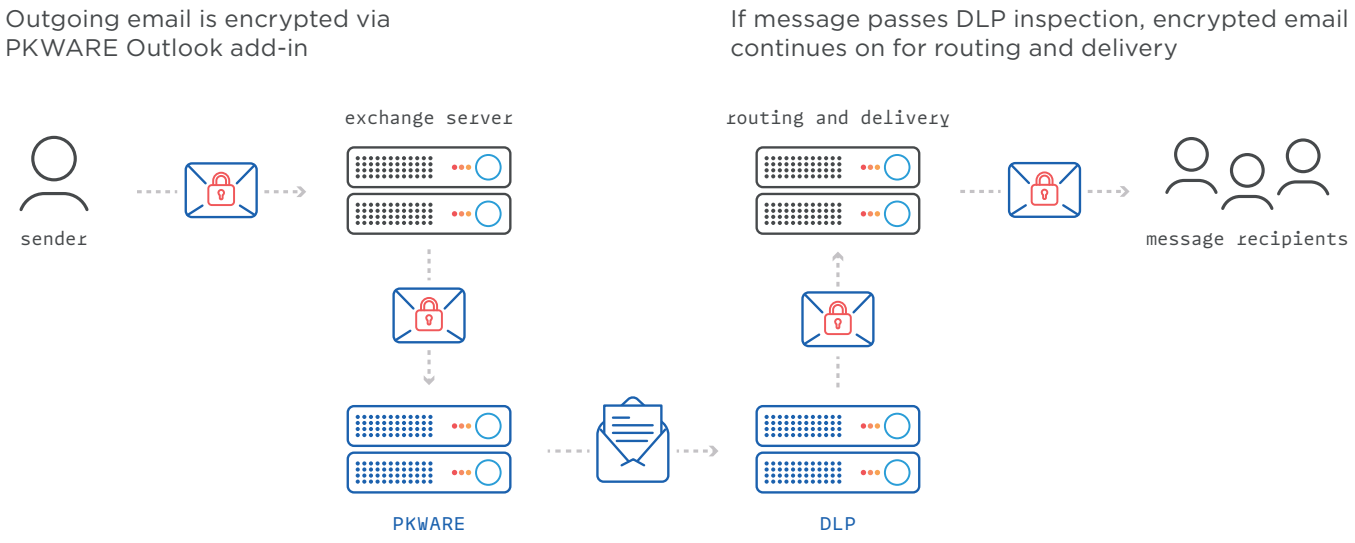
Policy-Based Encryption to Enhance Existing DLP

PKWARE's DLP enhancement capabilities integrate with your organization's existing DLP technology to facilitate scanning of encrypted data, as well as remediation of unprotected data.

PKWARE's PK Protect technology includes company-controlled keys in each encryption operation, enabling DLP scanners to decrypt content that has been encrypted elsewhere in the organization. PK Protect also allows the organization to encrypt data that was not protected prior to sending, eliminating the need to block transmissions that contain sensitive information.

Decryption for DLP Scanning

When a user initiates a transmission that requires DLP inspection and includes encrypted data, the message is routed for decryption and converted to plaintext using one of the organization's policy keys. The plaintext message is then submitted for DLP inspection. If the message is permitted to proceed by DLP, the original encrypted message continues on to the intended recipient.

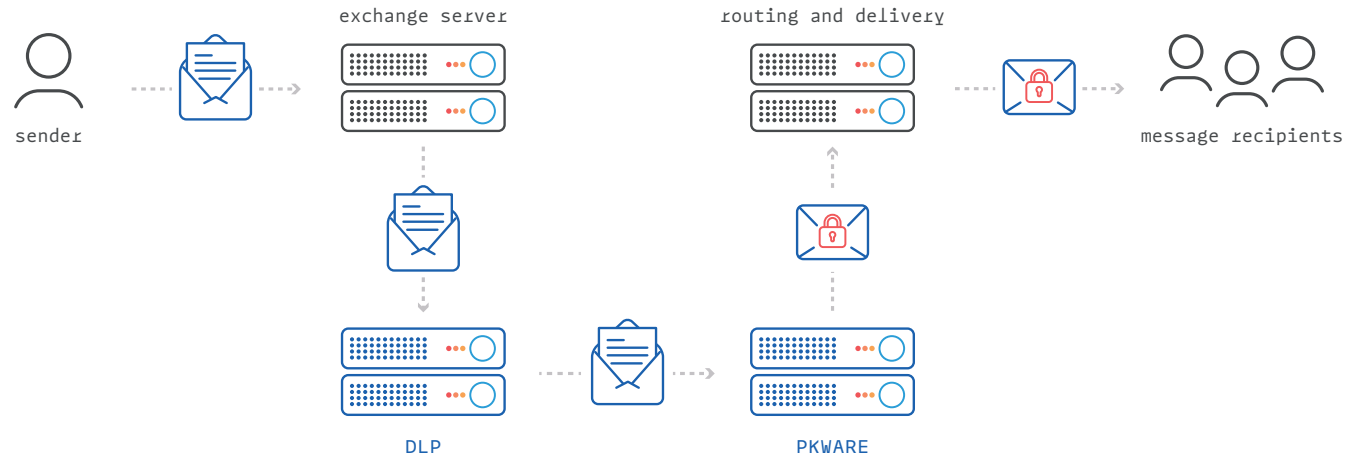


Remediation of Unprotected Data

In other situations, a user who is authorized to send sensitive information might have forgotten to encrypt the data before transmission. Rather than blocking the message or re-routing it for manual remediation, PK Protect can encrypt the sensitive data using a public key or unique Smartkey, after which the message can be permitted to continue.

User sends email containing sensitive information

Encrypted email continues on for routing and delivery (recipients can use the free PK Protect Reader to open)



DLP routes unprotected messages to PKWARE for automated encryption

Enhanced Security and Flexibility

PKWARE's protection travels with the encrypted files, ensuring they remain encrypted wherever they are transmitted or stored. Organizations can protect sensitive data using a variety of encryption key types, including passphrases, PGP keys, X509 digital certificates, or Smartkeys (PKWARE's embedded encryption key management system).

Regardless of which encryption system is used, administrators can use the PKWARE PK Protect Enterprise Manager to define policy keys to be transparently included in every encryption operation. This ensures that the organization never loses access to encrypted information.

Summary

PKWARE's DLP enhancement capabilities solve 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.

Supported Key Types

Smartkeys: PKWARE's embedded key management solution. Removes complexity from key generation, synchronization, exchange, or escrow. Smartkey technology also simplifies formerly challenging tasks such as re-encryption, key rotation, public key creation, or 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.

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