PKWARE ®

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.
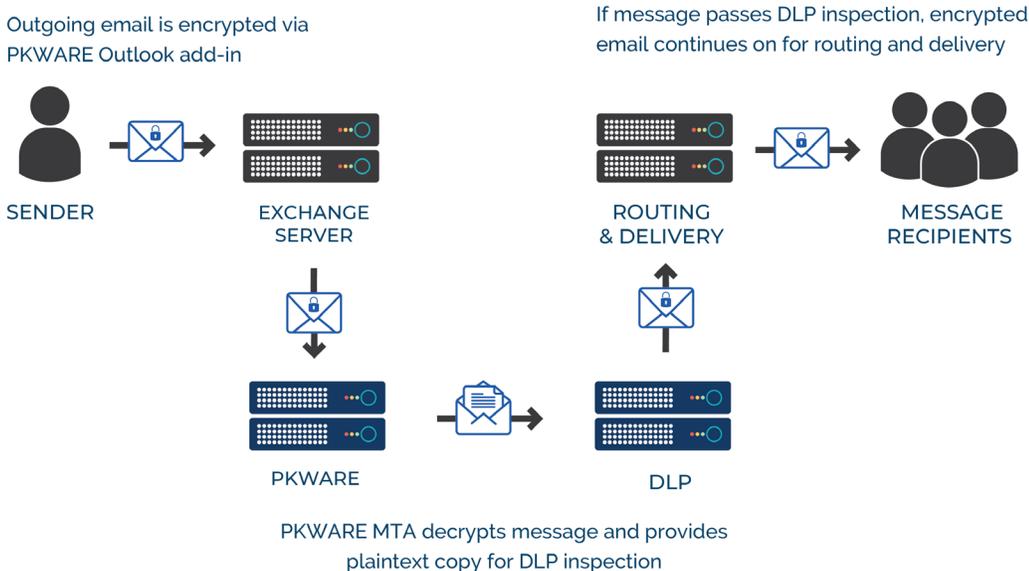
Data encryption, while also critically important for enterprise cybersecurity, often makes DLP less effective, especially when encryption is applied by end users without organizational control. When encrypted email messages or files are submitted for inspection, the encryption renders the data unreadable 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. .
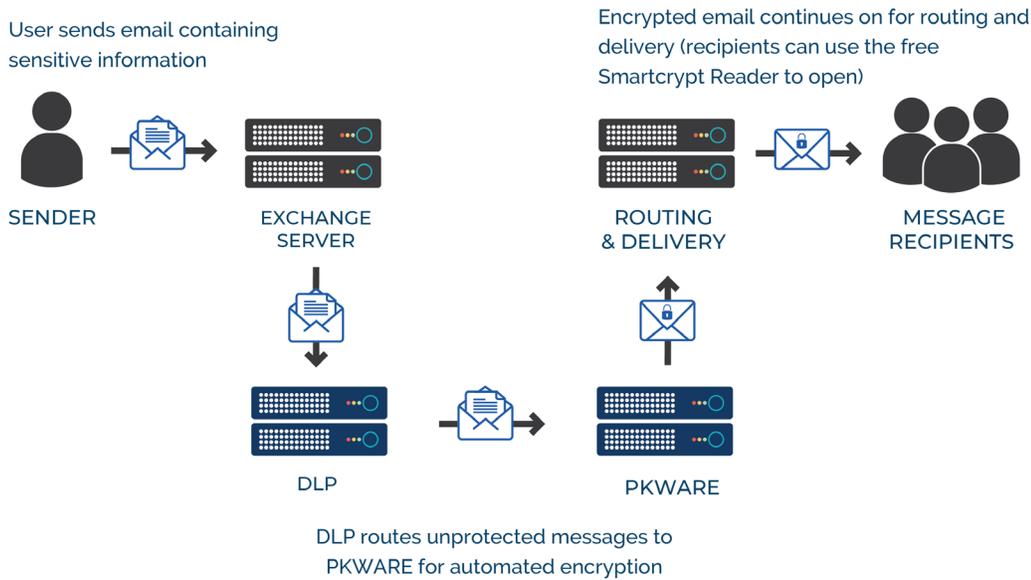
POLICY-BASED ENCRYPTION TO ENHANCE EXISTING DLP

PKWARE's DLP Enhancement solution integrates with your organization's existing DLP technology to facilitate scanning of encrypted data, as well as remediation of unprotected data.

PKWARE's Smartcrypt technology includes company-controlled keys in each encryption operation, enabling DLP scanners to decrypt content that has been encrypted elsewhere in the organization. Smartcrypt 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.

Outgoing email is encrypted via PKWARE Outlook add-in

If message passes DLP inspection, encrypted email continues on for routing and delivery

SENDER   EXCHANGE SERVER   ROUTING & DELIVERY   MESSAGE RECIPIENTS

PKWARE   DLP

PKWARE MTA decrypts message and provides plaintext copy for DLP inspection

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, Smartcrypt 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
Smartcrypt Reader to open)

SENDER

EXCHANGE
SERVER

ROUTING
& DELIVERY

MESSAGE
RECIPIENTS

DLP

PKWARE

DLP routes unprotected messages to
PKWARE for automated encryption

ENHANCED SECURITY & FLEXIBILITY

Smartcrypt 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 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 DLP Enhancement 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.

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.