



Bank Gains Control Over Sensitive Data with PKWARE DLP Enhancement

CASE STUDY



Uncontrolled encryption

One of the world's largest financial institutions discovered that well-intentioned employees were inadvertently creating a data security and compliance risk.

The bank lacked an enterprise-wide standard for data protection, leaving employees and departments to choose their own methods for securing sensitive information. The result was a patchwork of passphrase-based and certificate-based encryption, using a variety of user-selected tools, some of which provided inadequate protection.

The inconsistent approach to encryption created difficulties when users needed to share sensitive data internally. When users shared data outside the organization, the situation became even more problematic.

Ineffective DLP

The bank had invested significant resources in a data loss prevention (DLP) system in order to prevent unauthorized sharing of sensitive data. However, the DLP system was unable to inspect emails or attachments that were encrypted with user-selected tools.

With DLP unable to inspect encrypted email, the bank's security team was faced with two unacceptable options: route the messages for manual follow-up, or allow them to leave the company network without inspection. The first option was simply not feasible for such a large organization—with encrypted email accounting for 3% of total traffic, the DLP system was locked out of thousands of outgoing messages each month. Allowing these messages to bypass DLP, on the other hand, exposed the

Introduction

A global bank uses PKWARE technology to solve a complex data security challenge.

About PKWARE

PKWARE offers the only data discovery and protection solution that locates and secures sensitive data to minimize organizational risks and costs, regardless of device or environment. Our ultra-efficient, scalable software is simple to use on a broad range of data types and repositories, enabling precise, automated visibility and control of personal data, even in the fastest-moving, most complex IT environments. With more than 1,200 customers, including many of the world's largest financial institutions, retailers, healthcare organizations, and government agencies, PKWARE continues to innovate as an award-winning global leader in data discovery, security, and compliance. To learn more, visit PKWARE.com.

bank to multi-million dollar fines and other sanctions in the event that sensitive data was shared inappropriately.

DLP Enhancement from PKWARE

The bank needed a solution that could eliminate uncontrolled encryption and enable DLP inspection of encrypted files and messages. The solution needed to integrate with and enhance the bank's existing DLP technology, rather than replace it.

The bank evaluated PKWARE's DLP Enhancement technology and found that it provided a complete

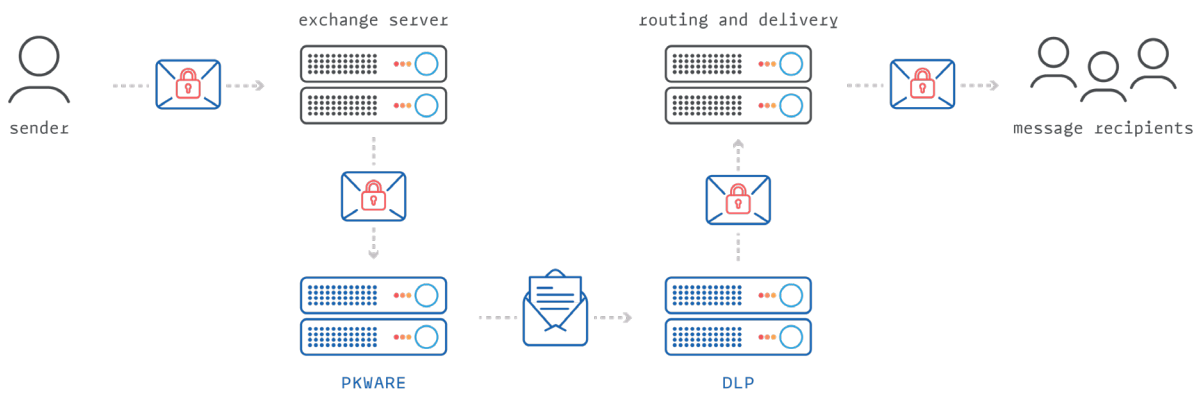
solution to the bank's DLP challenges:

- Encryption and decryption would now be handled by a single solution across the organization, with centralized control over key creation, exchange, and revocation.
- Every encryption operation would include a company-controlled "policy key" to ensure that the organization never lost access to its own data.
- Outgoing email messages would be decrypted prior to DLP inspection, using a policy key. If a message passed DLP inspection, the encrypted message would be allowed to proceed. Messages that violated the bank's policies could be blocked after inspection.

Decryption for DLP scanning:

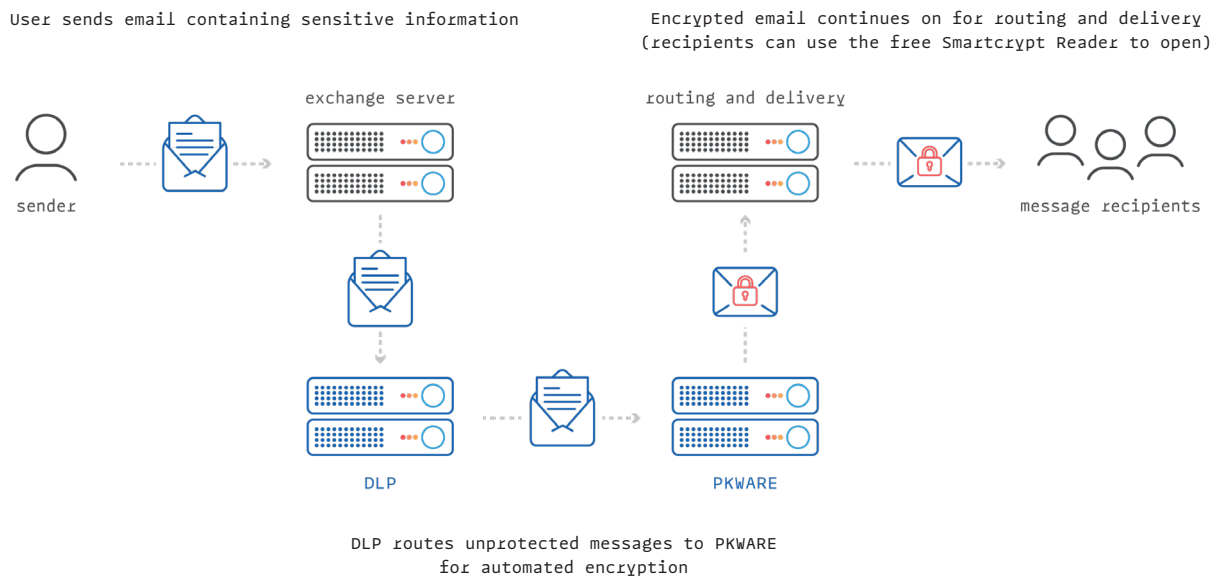
Outlook email is encrypted via PKWARE outlook add-in

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



PKWARE MTA decrypts message and provides plaintext copy for DLP inspection

Remediation of unprotected data:



From an end user perspective, the change was negligible, as email encryption and decryption are facilitated by PKWARE's Outlook integration. Authorized message recipients can decrypt and open encrypted messages using PKWARE's free Smartcrypt Reader.

Goals achieved

PKWARE's DLP Enhancement automated the bank's policy enforcement and eliminated the obstacles to proper DLP inspection. Despite the complexity of the challenge, PKWARE's solution was up and running quickly. As the bank's lead security architect said, "It was just a matter of weeks from proof of concept to implementation, once we saw how PKWARE's interoperable encryption fit in our process. Plus, we were able to scale up for the new Mac and Linux systems we were bringing online later in the year."