PKWARE
ENCRYPTION WITHOUT COMPROMISE

SMARTCRYPT

# SMARTER ENCRYPTION FOR ENTERPRISE EMAIL

Email is an inherently insecure form of communication, yet it remains the most common form of business communication.

Though few email users give it a thought, messages typically pass through unsecured systems on the way from sender to recipient, creating multiple opportunities for sensitive information to be compromised in the process.

User error is just as much of a concern-- a simple mistake when adding message recipients can send sensitive data into the wrong hands, with potentially catastrophic results. Each time a sensitive email is responded to, forwarded, or copied, the risk of a security breach grows larger.

## Find and encrypt sensitive data

PKWARE's Smartcrypt is the only enterprise encryption solution that applies persistent protection to email messages, keeping sensitive data safe from unauthorized access no matter where it is shared or stored.

Smartcrypt provides a streamlined, intuitive workflow for encrypting and decrypting emails. The Smartcrypt Outlook add-in encrypts and compresses outgoing messages with a minimum of user involvement.

Authorized message recipients can use Smartcrypt or PKWARE's free ZIP Reader to decrypt and open encrypted messages. Encrypted files cannot be read by unauthorized users, even when they are copied or saved outside the organization's network.

**Smartcrypt can be integrated with existing data loss prevention workflows, allowing DLP scanners to access and evaluate encrypted emails.**

### SOLUTION SUMMARY

- Smartcrypt agent automatically detects and encrypts sensitive information in email body or attachments
- Outlook integration allows users to maintain current workflows
- Strong encryption prevents access by unauthorized users if email is copied or forwarded inappropriately
- Data Security Intelligence tools provide detailed reporting on discovery and encryption activity

### BENEFITS

- Protects critical data from theft or misuse
- Eliminates the negative consequences of a data breach, whether the breach occurs on the mainframe or elsewhere
- Facilitates compliance with industry and governmental mandates for data protection
- Provides visibility into types and amounts of sensitive information stored on company assets

PKWARE
ENCRYPTION WITHOUT COMPROMISE

SMARTCRYPT

| Email Security Challenges | Smartcrypt Solutions |
| --- | --- |
| **External network vulnerabilities**<br><br>Email sent to users outside the organization's own network can pass through dozens of different networks, any one of which could be compromised without the sender or recipient's knowledge. | Smartcrypt applies strong persistent encryption to email messages and attachments. Data intercepted via network sniffers or other means will remain unreadable and unusable. |
| **Messages sent or shared inappropriately**<br><br>Email communication creates multiple opportunities for messages to be sent to unauthorized parties, either through sender error or through the actions of a message's intended recipients. | Encrypted messages cannot be read by users without the correct decryption key. If a message is sent to the wrong address or forwarded inappropriately, the unauthorized recipient will be unable to read it. |
| **Uncontrolled encryption**<br><br>Without an organization-wide encryption solution in place, well-intentioned employees may use a variety of encryption tools to protect sensitive data. This uncontrolled encryption prevents scanning by DLP technology and can cause the organization to permanently lose access to the encrypted data. | Administrators can configure Smartcrypt to include one or more policy keys in each encryption operation. These policy keys can be used to facilitate access by DLP scanners before a message leaves the company network. Policy keys also ensure that the organization will always be able to decrypt its own files. |
| **Disrupted user workflows**<br><br>Many email encryption products require process changes and multiple steps by end users, increasing the chances that employees will attempt to circumvent the company's encryption policy. | With Smartcrypt, administrators or users can select a default process and encryption key, greatly reducing the burden on end users.<br><br>When Smartcrypt Data Discovery is enabled, the Smartcrypt agent automatically identifies and encrypts sensitive data based on the organization's policies, making the entire process automatic from the user's perspective. |

PKWARE®
www.pkware.com

**CORPORATE HEADQUARTERS**
201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

**+ 1 866 583 1795**

**EMEA HEADQUARTERS**
79 College Road
Suite 221
Harrow HA1 1BD

**+ 44 (0) 203 367 2249**