PKWARE
DATA PROTECTION WITHOUT COMPROMISE

SMARTCRYPT

SECURE DATA EXCHANGE WITH POLICY-BASED ENCRYPTION

Every organization needs to share sensitive information with external companies and individuals. As data volumes and data traffic continue to increase, data exchange becomes a greater necessity and a greater risk each year.

PKWARE's Smartcrypt applies persistent encryption that remains with files in transit and at rest, preventing unauthorized access no matter where data is copied or shared. Organizations use Smartcrypt to protect data transferred via a variety of methods, including email, FTP, cloud services, and removable media.

Added security without added complexity

No matter which mechanism an organization uses to exchange encrypted information, one question must always be answered: how will authorized recipients get the decryption keys they need in order to access the data? Common approaches such as sharing passphrases via email, phone, or instant message are insecure and difficult to standardize, while public-key infrastructure has proven too complex for enterprise-scale implementation.

PKWARE's Smartkey technology takes the difficulty out of key management, allowing organizations to grant and revoke access to encrypted data quickly and easily. Smartcrypt also supports passphrase-based and certificate-based encryption, providing the flexibility large organizations need in order to exchange sensitive information with multiple external organizations.

Recipients can use the free Smartcrypt Reader to access files that have been encrypted using Smartkeys, even if their own organization does not use Smartcrypt.

SOLUTION SUMMARY

- Smartcrypt agents apply persistent encryption that remains with data when shared outside the organization.
- Single solution for securing data before exchange via email, cloud, FTP, or removable media
- Integrations with Outlook and Office allow users to protect files without disrupting workflows
- Free Smartcrypt Reader allows any authorized recipient to access protected data
- Administrators can grant or revoke access to sensitive data even after files leave the organization

BENEFITS

- Protects critical data from theft or misuse
- Automates the discovery and remediation of unencrypted sensitive data
- Enables organization-wide control and consistent policy enforcement
- Encrypted files are as much as 90 percent smaller than the unencrypted data

PKWARE

ENCRYPTION WITHOUT **COMPROMISE**

SMARTCRYPT

Data Protection Challenges	Smartcrypt Solutions
Email 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 integrates with Microsoft Outlook, allowing organizations to secure sensitive data in message bodies and attachments without disrupting the user experience. Smartcrypt can be configured to scan and protect emails automatically, or to provide a manual workflow for users who need to specify different encryption keys and authorized users for different outgoing messages.
Cloud Many organizations use cloud-based storage services as a mechanism for sharing data. However, once data leaves an organization's network for the cloud, the organization has limited control over where the data might travel next. Cloud services that provide data protection capabilities typically leave data in the clear while in transit, or leave encryption keys (and ultimately, control over the data) in the hands of the cloud provider.	Smartcrypt can be configured to monitor folders that are synced with cloud services and automatically encrypt files containing sensitive data before they are copied to the cloud. Administrators can revoke access to encrypted files at any time, even if the files have been copied from a cloud location to another device.
FTP FTP remains one of the most common mechanisms for data exchange between organizations. While secure FTP provides some measure of protection for data in transit and while it resides on the server, the organization that owns the data cannot control what happens once files are downloaded by a partner, vendor, or customer.	Smartcrypt gives organizations the ability to encrypt files before an FTP upload, ensuring that only authorized users will be able to decrypt and access the data, even in the event that files are moved or shared inappropriately after download.
Removable media Users have many options for encrypting flash drives and other forms of removable media. However, weak passphrases can leave sensitive data vulnerable to attack, while lost or forgotten passphrases can permanently lock an organization out of its own data	With Smartcrypt, organizations can take a policy-based approach to encryption, protecting files on removable storage while retaining control over sensitive information throughout the data lifecycle.

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