PKWARE

PK Protect

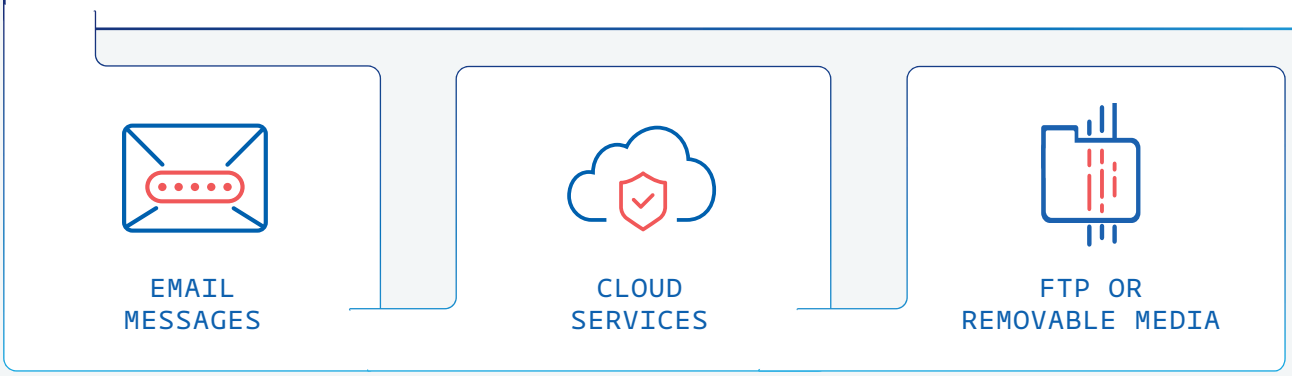
PK Protect

Solution Overview: Secure Data Sharing

Policy-Based Secure Data Sharing Solution

Sharing data with outside organizations is table stakes in conducting effective business today. Sensitive data requires adherence to enterprise-wide policies to assure its security and privacy as it is shared externally. As data volume and traffic continue to explode, sharing sensitive data becomes a greater necessity and presents an ever-growing risk.

Our persistent encryption remains with sensitive data and file in transit and at rest, preventing unauthorized access to sensitive data—both on-premises and cloud-based—no matter where the data is copied or shared. Organizations using PKWARE's PK Protect can securely employ an array of appropriate methods to protect sensitive data transfers, including:



Build customer confidence with simple, secure data exchange.

Add Security, Not Complexity

No matter which mechanism your organization uses in sharing encrypted information, one question always has to be answered: What is the corollary mechanism needed for authorized recipients to secure decryption keys required to access and use the sensitive shared data?

It's common to use methods that are not secure and difficult to standardize, such as sharing passphrases over email, phone, or messaging. Other options involve implementing complex public-key infrastructure for enterprise-wide implementation at scale, which can prove to be impractical.

PKWARE's persistent encryption keys, Smartkeys, take the difficulty out of key management. With Smartkeys, your organization can grant and revoke access to sensitive encrypted data quickly and easily. By supporting passphrase and certificate-based encryption, Smartkeys provide flexibility at scale that large enterprises need when regularly sharing sensitive data outside their controlled boundaries.

External recipients can go through a quick one-time set up and use our free Reader to readily access and use sensitive messages, data, and files that have been encrypted with a Smartkey and emailed, whether or not their organization even uses PKWARE software.

1. Open Reader application to enter address and create password.
2. PKWARE Reader automatically provides Smartkeys that the recipient has been granted access to.
3. Download and drag PKWARE encrypted message to Reader icon. If access was granted, the message or file opens, and sensitive data can be used as authorized.

Solution Summary

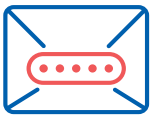
- PKWARE agents apply persistent encryption that remains with sensitive data while it's shared outside the organization.
- PKWARE delivers a single solution to secure sensitive data before it's shared whether by email, cloud services, FTP, or removable devices.
- Administrators can easily grant and revoke others' access to sensitive data even after it has left their organization.
- Free PKWARE Reader makes it secure and reliable for authorized recipients to access and use protected sensitive data.
- PKWARE agents integrate into Microsoft Outlook and Microsoft Office to enable users to easily protect sensitive data and files without any workflow disruption.

PK Protect Benefits

- Critical sensitive data protection against theft or misuse outside your organization.
- Full remediation of all sensitive data at scale before, during, and after it leaves your enterprise.
- Organization-wide control based on enforcement of over 100 out-of-the-box and custom-built sensitive data policies.
- Quick and easy normal workflows to share encrypted sensitive data.
- Encrypted files that contain protected, sensitive shared data compressed up to 90 percent.
- Authorized recipients readily using shared data as intended without even being PKWARE customers.

PK Protect Overcomes Typical Issues with Sharing Methods

Email



PK Protect is a simpler and better approach for sharing sensitive data over email with customers, partners, and other external parties.

Issue

- Secure email gateways create nearly as many problems as they solve. Multi-step processes required to open protected email together with forgotten passwords, password resets, and account lockouts create frustrations for senders and recipients.
- Frustrations can obstruct information flow that damages business relationships and outcomes.
- Recipients can be thwarted by email requirements their organizations don't support.

Solution

+ Rather than relying on a multi-setup model, PKWARE provides users drag and drop functionality eliminating complicated workflows and frustration.
+ Senders encrypt their message body and attachments using keys that only the intended recipient can use.
+ Recipients use free PKWARE Reader to decrypt and open attachments.
+ Administrators apply policies or create rules based on content and user permissions.
+ Sensitive data in outgoing messages is protected with strong AES-256 encryption meeting government regulations and industry mandates.

Cloud Services

PK Protect is a comprehensive and better approach for protecting sensitive data being shared with customers, partners, and other external parties from cloud data storage.

Issue

- When organizations rely on cloud-based storage systems as a mechanism for sharing sensitive data, they often lose control over where the data may travel in its route to the recipient.
- Cloud providers are generally responsible for maintaining the security of their infrastructure, whereas the organization whose sensitive data is being moved to or stored in the cloud is responsible to protect its data, including all sensitive or personal data.

Solution

- PK Protect can be configured to monitor folders that are synced with cloud services and automatically encrypt files or sensitive data in files before they are copied to the cloud.
- PK Protect maximizes sensitive data protection at motion and at rest, on premises and in the cloud.
- PK Protect Administrators can revoke access to encrypted files at any time, even if files have been copied from the cloud to another device.
- Administrators apply policies or create rules based on content and user permissions.

FTP or Removable Media

PK Protect provides a thorough and more secure approach for protecting sensitive data being shared with customers, partners, and other external parties using FTP or removable storage devices.

Issue

- FTP remains one of the most common mechanisms for data exchange between organizations. While secure FTP provides some protection for senders of sensitive data, once files are downloaded externally, the organization that owns the data loses control of how it's used. This puts them in legal peril.
- Removable media leaves vulnerable sensitive data exposed to theft or attack.

Solution

+ PK Protect gives organizations the ability to encrypt sensitive data or files before an FTP upload. PKWARE software can also define authorized recipients who are the only individuals able to access, decrypt, and use the sensitive data, and only for the purposes authorized.
+ PK Protect provides a policy-based approach to encryption. Customers retain control of sensitive data throughout its lifecycle, protecting it even when on removable storage.

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