PKWARE

PK encryption

PK Encryption

Solution Overview: FIPS 140-Compliant Encryption

What Is FIPS 140?

The Federal Information Processing Standardization 140 (FIPS 140) publication, which specifies requirements for cryptography modules. The National Institute of Standards and Technology (NIST) issues the FIPS 140 series to define the requirements that United States government systems and IT products should meet.

FIPS 140 requires all federal government agencies and departments that use cryptographic-based security to meet specific standards related to encryption strength and capabilities.

PROTECT

CONTROL

AUTOMATE

3 out of 4 of PKWARE users choose to protect their data with encryption.

How Do FIPS 140 Standards Affect My Organization?

- FIPS 140 requirements apply to all government agencies that use encryption to protect sensitive data.
- In addition, organizations that do business with government agencies or departments must meet FIPS 140 security requirements when exchanging sensitive data.
- Many other organizations must now meet these same standards, as FIPS 140 compliance is becoming an accepted best practice outside of the government sector and outside of the United States.

How Can PK Encryption Help Organizations Meet FIPS 140 Standards?

PK Encryption fully addresses the standards outlined in FIPS 140 by strongly encrypting the data itself. PKWARE's own FIPS mode setting ensures only FIPS 140-validated cryptography is used and eliminates the need for disruptive operating system FIPS policy settings.

PK Encryption keeps data secure:

- At rest and in motion
- At its origin and destination

PK Encryption offers government agencies the ability to use validated cryptographic modules for protecting data when run in FIPS mode. Data remains protected even if placed on removable media that is lost or stolen during transit.

Persistent File and Email Encryption

Format-Preserving Encryption

Dynamic Data Encryption in Motion

Transparent Data Encryption

FIPS 140-Compliant Encryption and Beyond

In addition to meeting the security standards outlined in FIPS 140, PK Encryption helps solve several other data security issues that government agencies face today.

> “PKWARE has helped address our concern for protecting sensitive documents being sent by email. Attachments can be encrypted automatically, which not only saves time, but also ensures that users don’t forget to protect them.”
>
> Abdul Azeez Panambron
> IT Manager, Hidada

Extensive Encryption Capabilities and Protection Against Data Loss

- Automate policy-based, element-level encryption for sensitive data in TXT, AVRO, Sequence, RC, ORC, MSAON, XML file formats, and more.
- When an authorized sender attempts to transmit unencrypted sensitive information, PK Encryption automatically encrypts the message for the recipient using a public key or a unique Smartkey, limiting the opportunity for data loss or misuse.

PK Protect: Automate enterprise-wide location and monitoring of sensitive data, identity creation, data classification, and policy-based data protection techniques, ensuring complete privacy for individuals and protection of organizational personal data vulnerabilities.

PK discovery

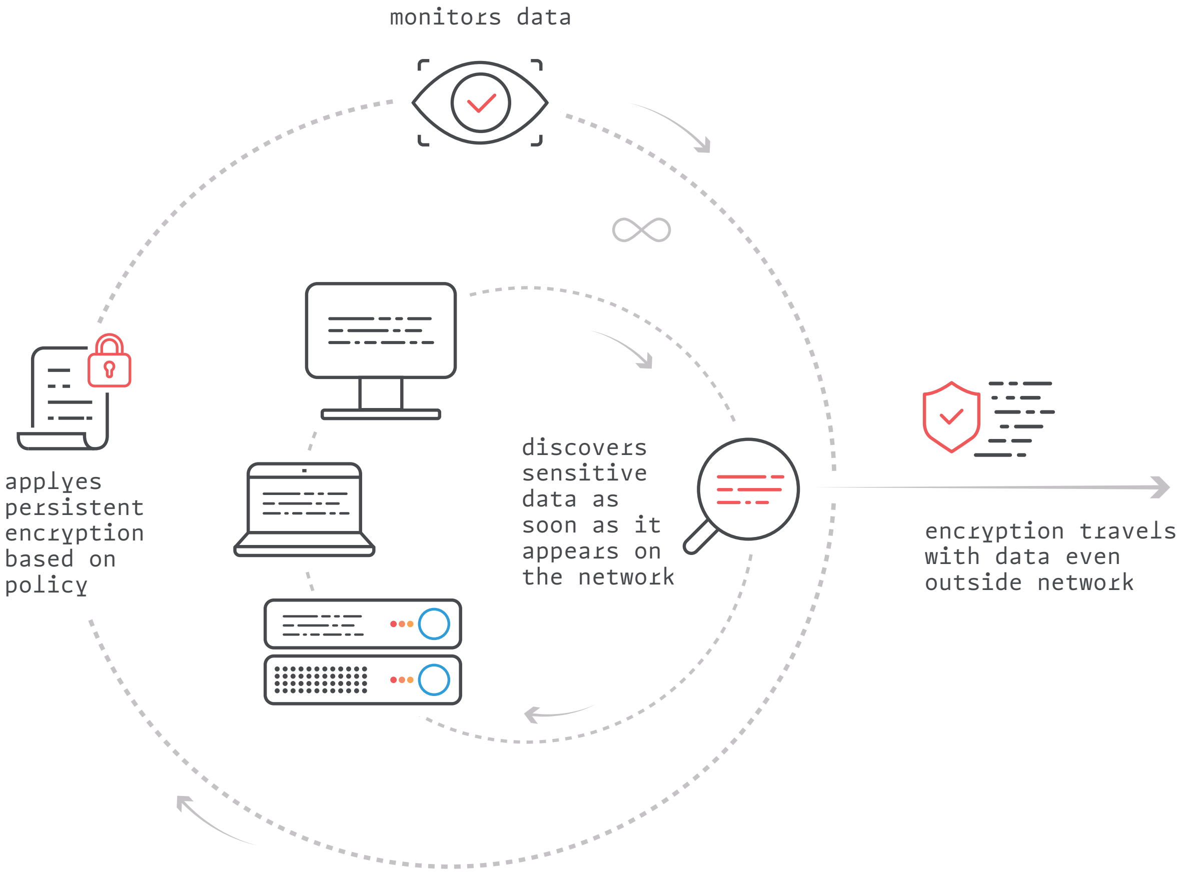
PK classification

PK masking

PK encryption

PK privacy

PK Encryption in Action



monitors data

applyes persistent encryption based on policy

discovers sensitive data as soon as it appears on the network

encryption travels with data even outside network

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

PKWARE