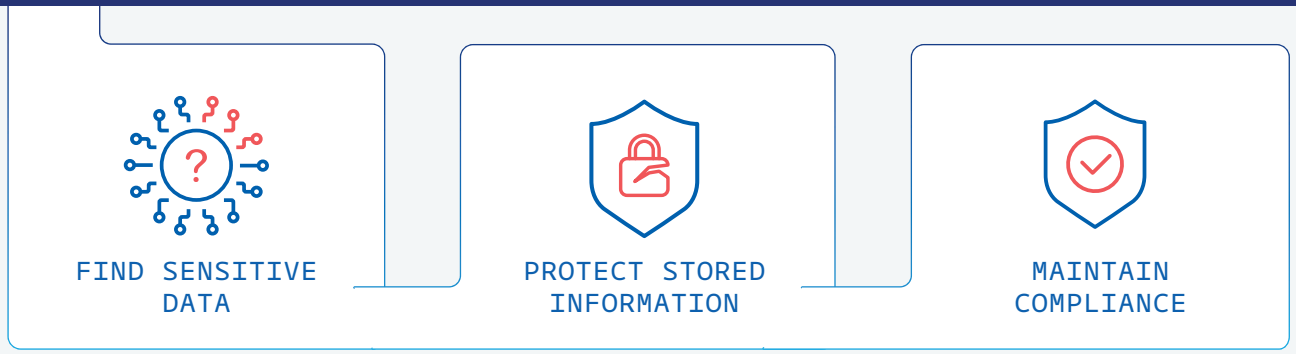
PKWARE

PK Protect

PK Protect

Achieving and Maintaining PCI DSS Compliance

Achieving and maintaining Payment Card Industry Data Security Standards (PCI DSS) compliance is a must for any organization that interacts in any way with payment cardholder data. PCI DSS compliance can be challenging. Organizations need proven data security solutions that are prepared for the future: the flexibility of cloud computing for reliable, competitive performance combined with a robust, ready solution for continuously protecting cardholder data. PK Protect is the best choice in securing cardholder data, providing sensitive data discovery and management for both achieving and sustaining compliance.



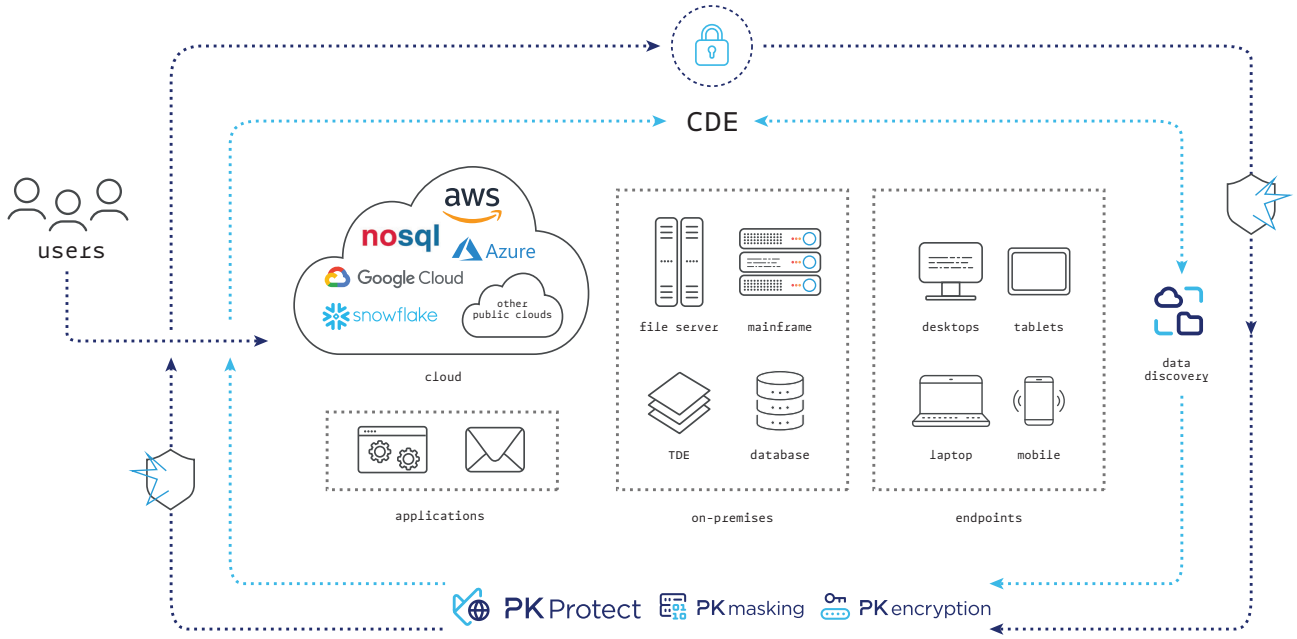
Meeting PCI DSS Requirements

Compliance in protecting cardholder data involves multiple requirements. PK Protect aids in compliance by directly addressing the need to:

- Protect stored cardholder data (Requirement 3)
- Encrypt transmissions of cardholder data across open, public networks (Requirement 4)
- Restrict access to cardholder data by business need-to-know (Requirement 7)
- Maintain a policy that addresses information security for employees and contractors (Requirement 12)

- Focusing on implementing continuous, sustainable solutions can help organizations meet evolving compliance requirements. PK Protect averts risk while meeting key challenges in processing cardholder data with a continuous three-step process:
- Assess: Identify sensitive data, classify, take an inventory of IT assets and business processes, then analyze for vulnerabilities.
- Remediate: Fix vulnerabilities and eliminate the storage of all unnecessary sensitive data.
- Report: Compile and submit required reports to the appropriate teams and management.
- Leveraging this process empowers organizations to avoid potential fees and fines due to PCI DSS non-compliance.

PK Protect Credit Card Data Boundary Protection



PK Protect's core focus areas for PCI are:

- CDE Scoping and Discovery
- CDE Boundary Protection
- Protection of data at rest (Requirement 3)
- PCI Endpoint protection (Requirement 4)
- Restrict PCI Access to those with need to know (Requirement 7)

PK Protect also addresses Requirement 12 when protecting personal data of all business roles: contractors, partners, and employees.

Minimize Risk and Reduce Cost

The PK Protect data protection platform minimizes risks and reduces costs by allowing businesses automatically and accurately to discover, classify, remediate, and protect personal and proprietary data companies hold, whether in structured, unstructured, semi-structured or free-form formats, regardless of device or environment. PK Protect addresses PCI DSS requirements in Scoping, Discovery, Protection, Alerts, and Reporting, all reliably and continuously.

ASSESS

PK Discovery automatically digs deep to find every place that cardholder data is stored, whether that's a file system, database, cloud repository, or an endpoint. PK Discovery operates across all major platforms, from on-premises to cloud, on structured, semi-structured, and unstructured data. PK Discovery is reliable at scale, incorporating AI and ML technologies appropriately to clearly identify cardholder data, even when formats are wildly varied by application or region. The solution leverages machine learning to eliminate both false-positives and false-negatives.

When PCI data is found in locations outside a company's cardholder data environment (CDE), PK Discovery flags it and asks which remediation is required, then performs automated remediation based on the company's policies. PK Discovery also readily identifies PINs and CVVs beyond their storage time boundaries and flags them for automated remediation.

REMEDIATE

PK Encryption includes multiple options for precise data protection to promote meeting PCI requirements while maximizing the business value of IT assets. Encryption options include file, email, element-level, format preserving, and transparent data encryption with all operations audited and reported to a central location, ensuring compliance. Apply PK Protect persistent file level encryption, protecting cardholder data at rest, in transit, and in use. Set PK Encryption up to be on-demand and real-time, according to the data protection policies, to strengthen Assessment outcomes.

Remove all sensitive personal data while still preserving the value of the original cardholder data with **PK Masking**. Extensive data masking protection options include character-level, custom value, format-preserving, redaction, and others including customization options. These masking techniques protect cardholder data across multiple disparate data stores, including permanently removing credit card numbers and other sensitive data from files and emails while leaving other contents unchanged.

PK Masking can also create production-quality DBMS copies so that entire data sets can be leveraged for accurate and meaningful insight without compromising cardholder data. With no linkage between original and masked data, there's no retrieval of the original data. Businesses may also choose to automate masking of sensitive cardholder data in production data sets to allow development, test, and analysis to leverage the same realistic-looking values in non-production applications.

The PK Protect suite follows company policies in designating and controlling the CDE boundaries—what roles have access to what cardholder data—restricting access to PCI data. Apply access control to roles within the company and to third party roles including technology partners, supply chain, resellers, and data processors.

REPORT

Receive continuous, automated alerts from PK Discovery whenever PCI data is discovered, and automate remediation.

PK Protect continuously assures correct mapping and scoping of your CDE, discovery of cardholder data, and desired remediation of any cardholder data that is out of CDE boundaries for both achieving and maintaining PCI DSS compliance.

Sustainable Compliance Support for the Future

As a premiere PCI DSS solution provider, PKWARE supports enterprise customers both in compliance with current requirements and in meeting future standards and objectives, such as the updated PCI DSS 4.0

Overarching Objectives of PCI DSS 4.0

1. Ensure the standard continues to meet the security needs of the payments industry
2. Add flexibility and support of additional methodologies to achieve security
3. Promote security as a continuous process
4. Enhance validation methods and procedures

PKWARE's suite of PK Protect technologies is designed with flexibility and breadth to cover all of PCI DSS future requirements including scope and boundaries of CDE, continuous protection of data at rest, endpoint protection, and restriction of PCI access. Organizations can reliably engage PK Protect solutions to readily comply with PCI DSS today and tomorrow.

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