PKWARE

PK Protect

Automated Ongoing File Redaction for PCI DSS

Remove Credit Card Numbers From Unstructured Data

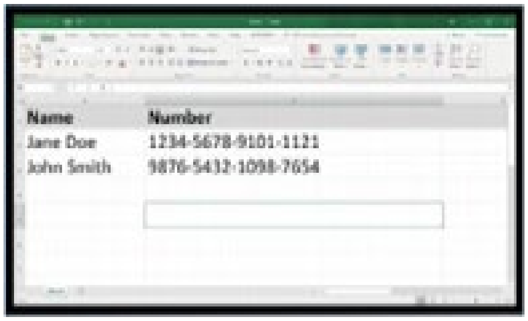
The Payment Card Industry Data Security Standard (PCI DSS) has provided a common framework of technical and operational requirements for protecting cardholder account data.

While not a set of laws or a regulation, PCI DSS does have costs. Companies that accept, process, or service credit card payments have to follow PCI DSS. Annual assessments for compliance are required, while non-compliance may result in penalty fines, increased transaction costs, and other consequences when a company fails an audit or experiences a high-risk data breach.

Wherever credit card numbers are stored—or extracted from a database and saved, even as as unstructured data in files on employee devices and file servers—they pose an obligation.

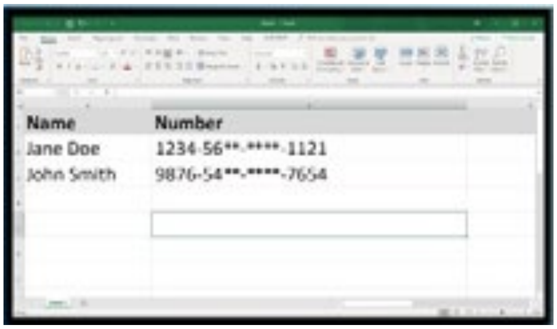
Real-Time Policy Enforcement

PKWARE's automated file redaction removes credit card numbers, leaving other file contents unchanged. Redaction takes files out of scope for PCI DSS requirements and ensures that cardholder data will not be exposed in the event of a computer theft or other security event.



Name	Number
Jane Doe	1234-5678-9101-1121
John Smith	9876-5432-1098-7654

FILE WITH UNREDACTED CARD DATA

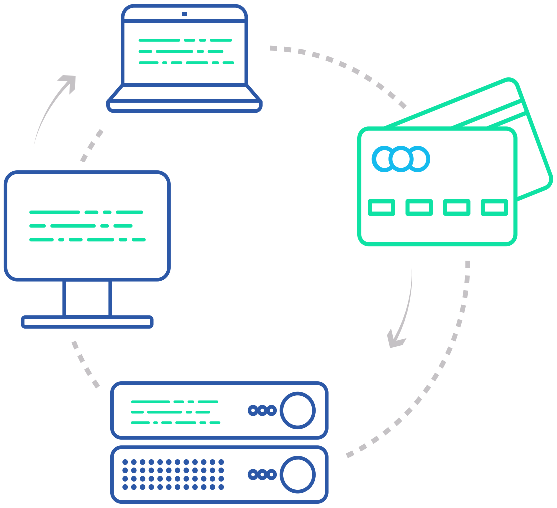


Name	Number
Jane Doe	1234-56**-****-1121
John Smith	9876-54**-****-7654

FILE AFTER AUTOMATED REDACTION

SOLUTION HIGHLIGHTS

- Automatically detects and redaction credit card numbers on Windows servers, laptops, desktops.
- Configurable workflow renders card numbers unusable in accordance with organizational policy.
- Unlike tokenization and similar technology, redactionis not reversible, allowing organizations to remove redacted data and files from the scope of PCI DSS requirements.
- Real-time file scanning ensures that card numbers are detected and remediated as soon as they appear.
- Removes card numbers from existing data.
- Helps reduce compliance risk and cybersecurity exposure.
- Industry-best achine learning-infused scanning technology minimizes false positives and reduces burden on IT resources.
- Web-based management console streamlines policy definition and administration.
- Detailed logging simplifies auditing and reporting.



Automated, Configurable Workflow

PKWARE's automated file redaction technology removes sensitive data from all supported file locations. It eliminates manual processes and surpasses other technologies that are often limited to specific types of data or environments, which can be costly and ultimately fail to comply with PCI DSS.

Organizations can remediate sensitive data as soon as it arrives, and can also remove credit card numbers from legacy data, taking terabytes or even petabytes of stored data out of PCI DSS scope.

STEP 1: FILE AND DATA SCANNING

PK Discovery searches file contents and all data at the element level for sequences of numbers that match algorithms published by all major credit card issuers. PK Discovery leverages machine learning and other heuristics to perform efficient, scalable scanning and discovery, whether at scheduled intervals, on demand, or in real time.

Each time the system finds a file that contains credit card data, it automatically remediates the file based on company policy, redacting and storing data in ways that prevent reconstruction of the original sensitive PCI data and ensure compliance.

STEP 2: COPY AND QUARANTINE (OPTIONAL)

If an organization wishes to preserve a copy of the original data prior to redacting, PK Protect can create a duplicate file in a quarantined location, and protect the unredacted version with PCI-compliant transparent or persistent encryption. This may be desirable for companies when the value of the data is needed in test or analytics.

STEP 3: POLICY-BASED CLASSIFICATION AND REDACTION

PKWARE's file redaction protects account data so that it will be of no use or value to unauthorized users who gain access to it. Apply persistent classification to files, data, and repositories across the enterprise as they are created, moved, shared, duplicated, or saved. Classify sensitive data automatically or apply labels manually to files and data, including email messages Files and data not covered by PCI DSS remain unchanged. Each company can define custom policies or use our out-of-the-box PCI DSS policies for compliance and secure PCI redaction.

STEP 4: CONTINUOUS MONITORING

PK Protect monitors file activity on servers, desktops, and laptops. Every time a file is created or modified, the system initiates a scan for credit card data. All scanning and remediation activity is recorded in immutable logs, allowing the organization to monitor and report on data protection across the enterprise.

TECHNICAL SPECIFICATIONS

Management Console:

- Hardware appliance
- Virtual appliance
- Software-based (Windows Server)

Scanning and Redaction:

Operating Platforms

- Microsoft Windows

Credit Card Number Patterns

- VISA
- MasterCard
- American Express
- Discover
- Diners
- JCB

... And More

File Types

- DOC/DOCX
- XLS/XLSX
- PPT/PPTX
- VSD/VSDX
- XML/OOXML
- PDF
- TXT
- CSV
- MDB
- ACCDB
- MSG
- RTF
- LOG
- JSON
- ZIP

PK Protect Suite

PK discovery

PK classification

PK masking

PK encryption

PK privacy

Ready To See It Live? Contact Us!

pkware.com/demo

201 E. Pittsburgh Ave.
Suite 400
Milwaukee, WI 53204

866-583-1795

Follow Us

/company/PKWARE

facebook.com/PKWARE

@PKWARE

PKWARE.com

NASSCOM

ISO 27001

ISO 9001

Silver Microsoft Partner

PKWARE