PKWARE®

Automated Redaction For PCI Data

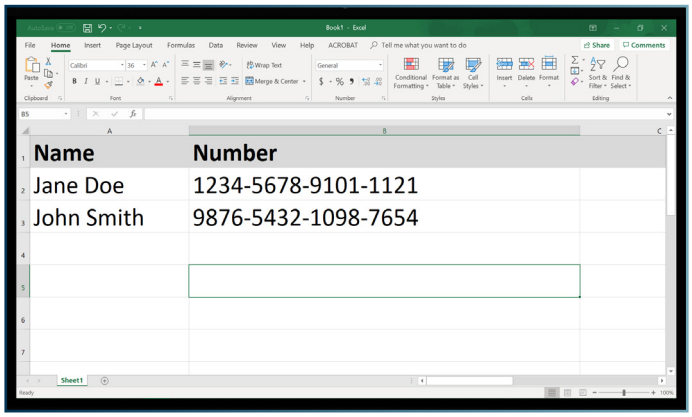
REMOVE CREDIT CARD NUMBERS FROM UNSTRUCTURED DATA

One of the biggest challenges to PCI DSS compliance is sensitive information that exists outside the organization's controlled database environment. When credit card numbers are extracted from a database and stored as unstructured data—in files on employee devices and file servers—they pose a significant threat.

REAL-TIME POLICY ENFORCEMENT

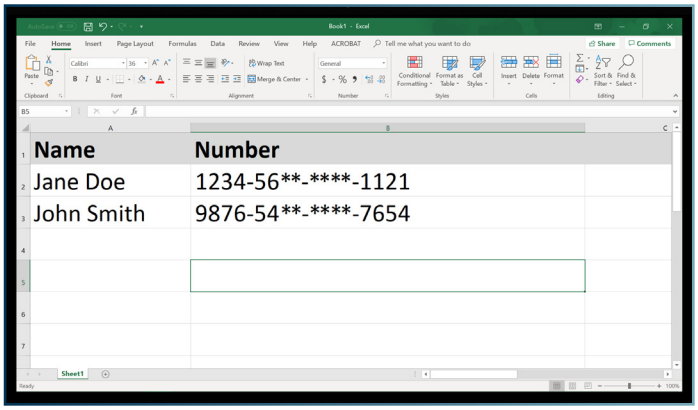
PKWARE's automated data redaction technology removes credit card numbers and other sensitive data from files, leaving other file contents unchanged. Redaction takes files out of scope for PCI requirements, and ensures that cardholder data will not be exposed in the event of a computer theft or other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

File with unredacted card data



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

File after automated data redaction



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

SOLUTION HIGHLIGHTS

Automatically detects and redacts credit card numbers on Windows servers, laptops, and desktops

Configurable workflow renders card numbers unusable in accordance with organizational policy

Unlike tokenization and similar technology, redaction is not reversible, allowing organizations to remove redacted 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 file 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 technology removes sensitive data from inappropriate locations, and eliminates manual processes that can expose an organization to compliance failures and other risks.

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

STEP 1: FILE SCANNING

PKWARE's file scanning technology searches file contents for sequences of numbers that match algorithms published by major credit card issuers. PKWARE can identify valid credit card numbers while ignoring similar sequences that do not pass the Luhn test or other applicable algorithms.

Each time the system finds a file that contains credit card data, it automatically remediates the file based on company policy.

STEP 2: COPY AND QUARANTINE (OPTIONAL)

If an organization wishes to preserve a copy of the original data prior to redaction, PKWARE can create a duplicate file in a quarantined location, and protect the unredacted version with PCI-compliant transparent or persistent encryption.

STEP 3: POLICY-BASED REDACTION

PKWARE automatically redacts a portion of each credit card number within a file, rendering the numbers unreadable in the event that a file is stolen or shared inappropriately. Other file contents remain unchanged.

STEP 4: CONTINUOUS MONITORING

PKWARE 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.

SPECIFICATIONS

Management Console:

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

Scanning and Redaction:

OPERATING PLATFORMS

- Microsoft Windows (Vista or later)

CREDIT CARD NUMBER PATTERNS

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

FILE TYPES

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