PK Dynamic Masking

One of the most valuable assets an organization has is its data. But holding personal data comes with the responsibility of protecting it, both from external threats as well as internal threats. Some sensitive data access is necessary for particular job functions. Which means that blanket protection, while helpful for defending data, may actually inhibit the productivity of certain roles within the business.

PK Dynamic Masking is purpose built with technology that masks sensitive data as it is accessed based on user roles and policies, leaving the original database untouched.

Protect Privacy While Maximizing Data Value

Real-time data masking ensures users do not get access to sensitive data while also preventing physical changes to the original production data from taking place.

- Fine granulated masking control is directly tied to each user's granted access capabilities
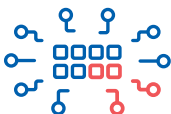
- Only the queried data is masked, leaving the rest of the data untouched and reducing necessary overall processing necessary for data protection

- Modify masking policies at any time and see immediate results

The Dynamic Masking Method

Unlike at-rest or static masking, dynamic masking does not impact any data in the data store, instead masking only sensitive data returned to selected users when they access the data store. Preset policies determine which data is accessible, which data is masked, and which users can receive masked versus unmasked data.
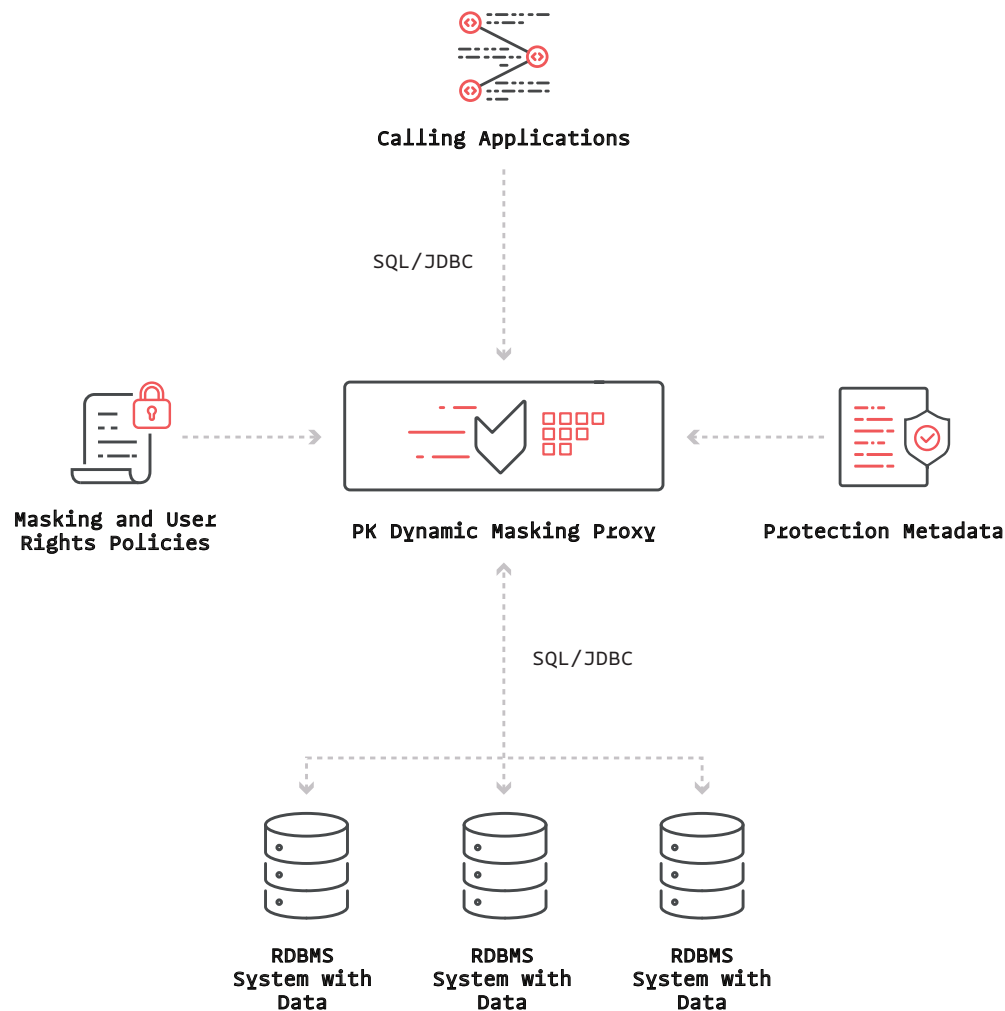
How It Works:

Applications call the database using existing standard SQL or JDBC queries. No code change is required for the calling applications.

PK Dynamic Masking receives the queries and executes the appropriate masking operations based on established polices and protection metadata. Protection metadata informs the program which columns contain sensitive data that must be protected.

PK Dynamic Masking then remediates selected sensitive items in the returned data based on the user executing the query. User and group information for these policies can be imported directly from directory systems such as Active Directory of LDAP.

PK Dynamic Masking limits the exposure of sensitive data, preventing users who should not have access to the data from viewing it.

Calling Applications

SQL/JDBC

Masking and User Rights Policies

PK Dynamic Masking Proxy

Protection Metadata

SQL/JDBC

RDBMS System with Data

RDBMS System with Data

RDBMS System with Data

Example of Use

In a bank that assigns account numbers to customers and uses Social Security numbers for identification, two groups of employees have access to customer records. The first group consists of tellers and other customer service people. They do not have authority to see the full SSN of any customer. Only the last four digits are visible, with the rest masked using an 'X' character when customer data is retrieved. These four digits are used as identifying information any time this group speaks to a customer.

The second group is the fraud handling team and has access to the full SSN as needed.

While both groups use applications that access the same customer data store, the applications access data via the PK Dynamic Masking proxy. Group one will receive masked SSN when retrieving customer records, while the second group will receive full SSN information from the same customer data store. The records in the data store itself are not masked; instead, masking is applied according to the query group's credentials. Other protections—including transparent data encryption and access controls—may be applied to the data store.

Supported Platforms

Current supported platforms for PK Dynamic Masking are: Hive, IBM DB2, MySQL, Oracle, Postgres, SAP HANA, SQL Server, Teradata

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

Technical Requirements

Technical Specifications Management Console:

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

Scanning and Redaction:

Operating Platforms
- Microsoft Windows
- macOS

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
- Z

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.com

PKWARE