# PK Protect

## Safeguarding Data During Cloud Migration

## The Standard in Data Protection

The cloud promises countless ways to realize operational and bottom-line benefits when an organization migrates physically hosted IT operations to a virtual environment. Although data is safe once inside the cloud, large-scale data movement can incur risk of exposure for sensitive data.



FIND SENSITIVE DATA
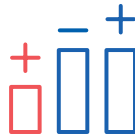
VALUABLE DATA INSIGHT

REPORT SCAN

Mitigating risks requires users to take extra care when transferring and storing highly sensitive data. While cloud service providers guarantee data will be safe once in the cloud, organizations are responsible for ensuring data is protected in transit. PK Protect plays a vital role in cloud strategy by automatically scanning and acting on all migrations to keep data safe.

## PK Protect Suite

PK discovery

PK classification

PK masking

PK encryption

PK privacy

Cloud is essential to many business strategies. Adding PK Protect to uphold the cloud shared security model can minimize disruption and increase security during cloud migration, preventing delays and ensuring compliance by supporting the following:

**1. Know what data you have:** Knowing what data you have before you move it ensures that only the necessary data in the intended format is moved. Types of data moving into the cloud should be reviewed for the level of required user access and if the data can even reside in the cloud. Determine if there are data and applications that are no longer needed; this both helps the bottom line and lessens security risks.

**2. Understand compliance and regulatory requirements:** Decide which data elements should be moved to the cloud and which shouldn't, and diligently adhere to those decisions. Controlling the migration of data should be done any time personal information is introduced to a new environment. Important legal and internal guidelines companies should develop include:

- Clear naming of data elements in database tables or a central index

- Clear mapping of the data elements in the new environment

- Recognition when data elements come together to represent a higher degree of sensitivity

**3. Access control:** Security considerations during migration should include traffic into and within the cloud, and users should be granted the minimum level of access necessary to perform their assigned function. PK Protect supports continuously verifying least privilege to meet regulatory and industry compliance objectives and assesses existing security measures and limitations in the new environment for a comprehensive understanding of new access and entitlement conditions.

**4. Protect data before it's migrated:** Mask or encrypt sensitive data before it travels to the cloud. Masking and encryption can be applied to data sets before they're migrated to the cloud to ensure the following of strict standards of regulatory and compliance rules. With data living in the cloud, masking and encryption can utilized for protecting data in use and/or at rest.

# Strategy, Security, Privacy, and Compliance

PK Protect's data security and privacy platform automatically scans and acts on all migrations. Security, privacy, and compliance are achievable with flexible deployment, including fully hosted, embedded library, or a hosted API gateway for serverless architecture.

### Pre-Migration Scans
PK Protect identifies data before it is moved to ensure that the right data can be migrated and what data, if any, needs to be protected.

### Pre-Migration Protection
PK Protect applies required protection measures for data sets that must be masked and/or encrypted before they can be migrated to the cloud.

### Post-Migration Scans
Once data has been moved, PK Protect accurately identifies where everything is in the new environment for added audit protection.

### Scale to the Data
PK Protect scales to the amount of data, both structured and unstructured, during the migration process.

### Data Modernization
PK Protect supports on-premises moves from one repository to another as part of data modernization for infrastructure needs.

### Ongoing Scans
Scan and move files on-demand or as part of a constant pipeline.

### Data Visibility
Track who is accessing what data, how much of that data vendors can see, and when to revoke access to it.

Whether preparing for a move to the cloud, already in the cloud, or expanding to multiple cloud platforms, it's important to have a true assessment of risk and understand how to manage sensitive data in the cloud with confidence.

PKWARE delivers solutions that keep data safe while moving to and from the cloud without breaking business processes or disrupting the user experience. PK Protect provides optics into data sensitivity by scanning through legacy data sources and creating actionable insights to calculate risk of migration, then enforcing controls and remediation to mitigate risk prior to moving data.

## 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