# PK Protect

De-Risk Acquired Data and Ensure Compliance of Merged Platforms: Enabling Data Security and Privacy in Mergers and Acquisitions

The global market today is markedly characterized by consolidation and convergence; after a brief slowdown in 2020, companies are again looking at mergers and acquisitions for business growth. Beyond bringing people, technology, and business processes together, data is every company's biggest asset and largest liability. The convergence of data requires deliberation and insights, especially in light of the growing number of privacy and security compliance requirements.

FIND SENSITIVE DATA

CONTROL DATA USAGE

VALUABLE DATA INSIGHT
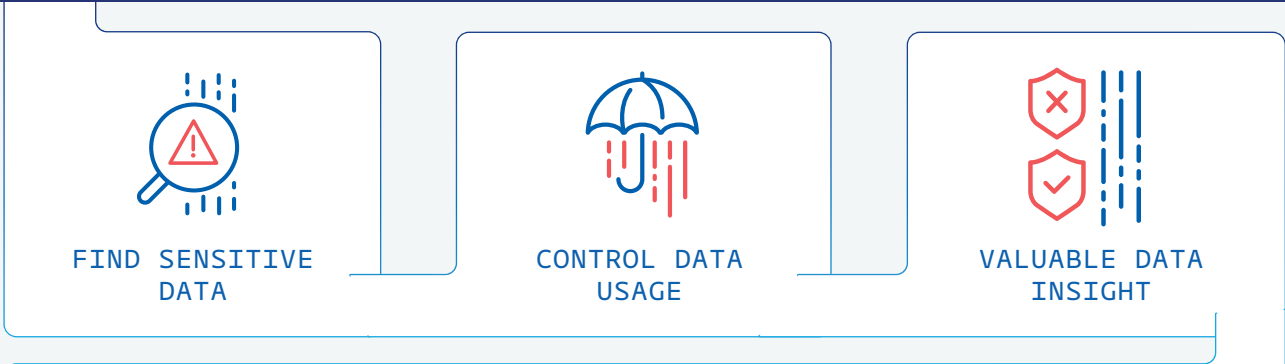
The sophistication of today's breaches tends to exploit badly designed environments and poorly implemented protocols, further increasing the need for convergence.

PK Protect Suite

PK discovery

PK classification

PK masking

PK encryption

PK privacy

The fundamental problem is that the company acquiring the new business is also acquiring all their data assets, and with that, the liability of safeguarding them. Fortunately, PKWARE's data solutions are purpose-built to de-risk data that is part of M&A and due diligence processes, addressing associated business challenges such as:

AUDIT / COMPLIANCE

Every company that acquires new data assets needs to know exactly what kind of information is contained in them. Without proper optics, any subsequent audit (internal or external) can result in monetary or legal repercussions.

NEW BUSINESS PROCESSES

When two companies come together, business processes of both companies tend to exert some influence. The way data will be used in the new business process must be done in accordance with security and privacy standards, which may or may not be the same across the two individual enterprises. In either case, the sensitivity of the data determines the processes needed to meet the standards. Knowing the data's sensitivity allows secure business processes to be established.

REMEDIATION

After a successful M&A, groups within businesses typically get access to data they never had before, such as data from different environments or geographical regions flowing into each other. Before sharing data can be enabled, it's necessary to implement appropriate controls.

PK Protect, PKWARE's end-to-end data discovery and protection suite, is purpose-built to mitigate many of M&A's toughest data challenges.

1. Data Discovery: Use PK Discovery to scan and inventory all data assets (structured, unstructured, semi-structured). Repository types are scanned differently—networks can be scanned for all databases, while all files in Hadoop or Cloud Stores (S3, ADLS, GCS) or File Shares can be cataloged in a report—and endpoints can be scanned as well. This end-to-end discovery provides a starting point for gathering deeper insights into all data assets.

2. Sensitive and Personal Data Detection: Once all the repositories have been inventoried, a comprehensive and deep scan of data provides optics into the exact type, quantity, and location of sensitive and personal data in the acquired assets. In-depth reports provide granular information such as the exact file or column location of sensitive or personal data, while high level dashboards provide an overview of the entire environment's sensitivity.

3. Identity Information and Compliance Obligation: PK Discovery can also scan for identities, finding the exact pieces of data that belong to specific individuals. Knowing information about customers enables the business to understand what compliance obligations it has. For example, if a business does not have offices, employees, or customers in the state of California, it may be exempt from the CCPA. However, if they gain California customers during M&A, they are now obligated to comply with the CCPA. Without understanding such information, a business might be completely unaware of all their compliance obligations.

4. Data Masking / Data Encryption: PK Masking and PK Encryption provide element-level remediation of data via masking (a non-production use case) for analytics and dev/test environments, or encryption/decryption (a production use case).

5.ITAR Compliance: PK Protect can detect any data that is governmentally restricted if a company is purchased by a foreign entity and therefore not legally able to transfer any of those ITAR items to the new company, nor allowed to create a US-based subsidiary to hold those assets.

6.Cross Border Transfers: PK Protect has the critical ability to track cross border transfers. When new data assets are acquired, they might be located in different geographical areas, opening the business to new compliance requirements. In addition, users in some regions may not be allowed to access data from other geographical regions. Knowing what cross border data transfers are happening within an organization is crucial. Under such circumstances, remediation techniques like masking and encryption can ensure users across different regions are able to share valuable data for utility and insights without compromising its security and privacy.

PK Protect is perfectly positioned to execute these features during M&A activity because it holds important technical advantages such as:

SCALE

PK Protect is capable of scanning huge volumes of data. M&As can typically involve multiple terabytes or petabytes of data. Because of its robust technology, PK Protect can easily scale up to this level.

PERFORMANCE

M&As are typically time sensitive, and although the scale of data at hand can be extraordinarily large, the amount of time available to do due diligence can be extremely small. Expertise in big data technology coupled with distributed multi-threaded architecture means that PK Protect can scan large amounts of data at astoundingly fast speeds.

PLATFORM BREADTH

PK Protect can scan and remediate data both on-premises and in the cloud. Beyond this, PK Protect can scan databases, Hadoop, cloud stores, file shares, various cloud-based applications, and even endpoints. This is critical, as enterprises have highly diverse data assets and can have multiple and varied data repositories, all of which need to be scanned and often remediated during M&A activity.

ACCURACY

Because of multi-structured and extremely heterogonous data assets, enterprises often contain a lot of semantically ambiguous data. PK Protect uses state-of-the-art technology that leverages context aware detection along with machine learning to provide accurate insights no matter how complex or ambiguous the data might be.

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