CYERA

INDUSTRY WHITEPAPER

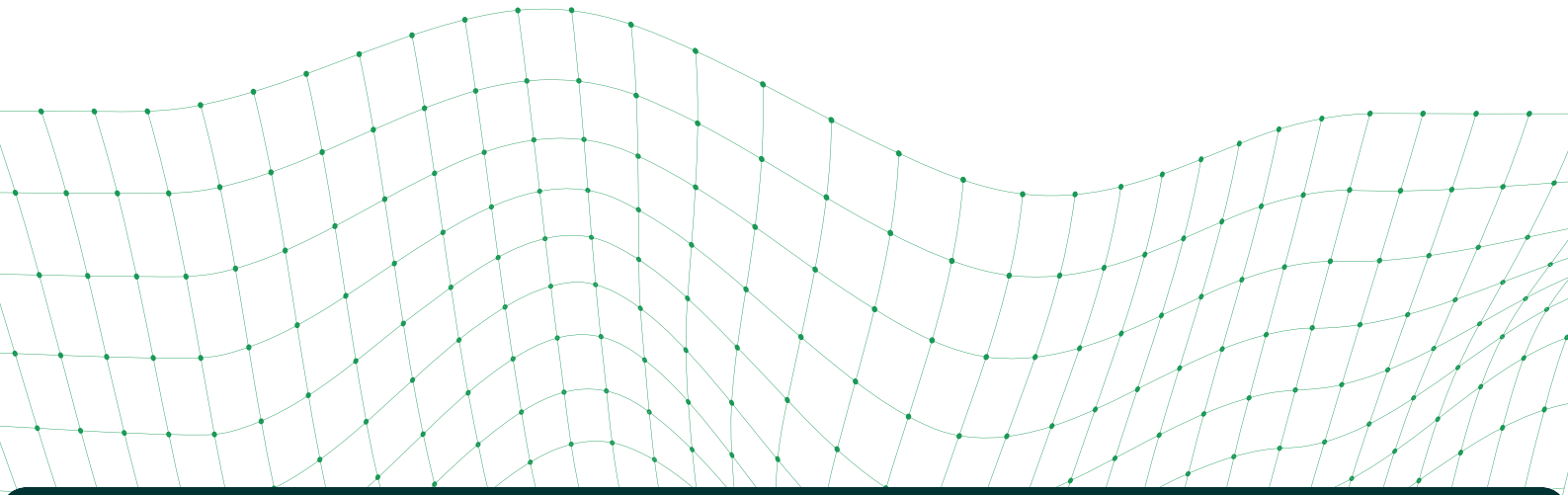
# Simplify Data Security During M&A and Divestitures with Cyera

# Executive Summary

Mergers, acquisitions, and divestitures are critical for enterprises. They provide new opportunities for growth by helping increase market share, integrate new technologies, and offer an opportunity for organizations to scale rapidly. A well-executed merger or acquisition will even lead to more synergies like cost savings, and better operational efficiency and customer brand loyalty. Divestitures help companies refocus resources on more profitable business units, and growth efficiently. When enterprises divest, they free up capital bandwidth to focus on innovations, invest in high-growth sectors, and position themselves more favorably within the market.

Secure and actionable data intelligence has become a critical aspect of due diligence during events such as these. This is because the complexity of data, sheer volume of known, and unknown data within an organization, coupled with the ever-growing threat landscape, demand a more sophisticated approach to assessing data security. This has led to the emergence of modern solutions like Data Security Posture Management (DSPM). These automated and frictionless services, often part of a larger Data Security platform, offer valuable data insights necessary to evaluate opportunities, while minimizing risk of owning unacceptable levels of risk post M&A. DSPM tools provide additional value during early M&A discussions as provide leverage for the “buyer” in the form of a highly accurate and timely “data risk assessment”.  During divestitures, both companies may have legal obligations to remove specific records from their environments. The continued storage of that data post divestiture, could introduce legal risk and fines, generally exposed during a subsequent audit or exposure.

Understanding data and context discovery, risk and access to material data,  plays a crucial role during mergers and acquisitions (M&A) or divestitures as these types of transactions almost always involve the transfer, consolidation, or separation of sensitive information.



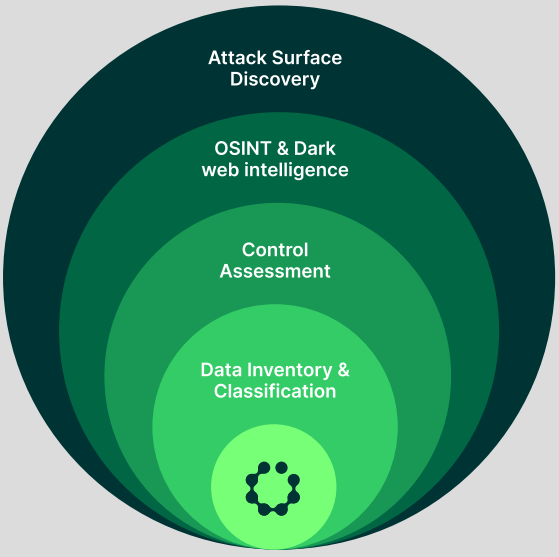
# Ensure due diligence and assess risk as part of a transaction

As part of an M&A or divestiture both the buyer and seller parties will need to identify and assess the types of data that's involved. This will often include sensitive data like intellectual property (IP), personally identifiable information (PII), as well as other proprietary business data.

Discovering and classifying data is often the first Cyera use case. The platform discovers any data type, and then classifies that data with deep data context. Once the data is discovered and classified, each party can use the data insights to inform the transaction processes. For example, perhaps there's sensitive data that each company was unaware of, and requires additional means of protection. Identifying locations, volume and access to unique business and intellectual property is extremely valuable during such negotiations.

Assessing risk is another key step. Cyera can determine if there are potential data security risks related to either of the company's data, which also includes any existing or ongoing vulnerabilities, breaches, or non-compliance regulations. Cyera  verifies whether or not sensitive data is encrypted, masked or tokenized, and shines light on data masking misconfigurations that could indicate over-privileged access to critical and sensitive data.

Cyera's Data Risk Assessment is a critical starting point for organizations. Once deployed, the risk assessment service determines the overall risk posture of the acquired or divested company, based on the data that is discovered, classified and accessible by sanctioned and unsanctioned entities by Cyera. Customers are provided with key actionable insights starting with Cyera's "data materiality" analysis combined with over 30 risk factors  to develop a custom risk assessment for review prior to the M&A or divestiture transaction.




## Risk Assessment Strategy

**Attack Surface Discovery**

Leveraging attack surface discovery and mapping resources to identify the public digital footprint of your organization

**OSINT & Dark Web Intelligence**

Discovery exercise on previous data breaches, leaks & other OSINT intelligence to identify compromised credentials and other details related to the in-scope organization.

**Control Assessment**

A vCISO led evaluation of 31 critical controls derived from established frameworks

**Data Inventory & Classification**

Leveraging Cyera's Data Security Platform to target a predefined number of customer Data Stores to execute Data inventory and automated classification.

After the DRA is provided, Cyera can deliver data detection and response capabilities to continuously monitor and alert data owners and SOC teams of any potential data security risks derived from human and non-human access with your most critical data. For example, sensitive data that's publicly accessible, or sensitive data stored in a terminated employee's OneDrive, or sensitive data not backed up. Cyera can then pass along these data insights to the enterprise's SIEM, security service edge (SSE), email security, workflow automation, and other key security services deployed within the environment to take further remediative action.

These insights can have a massive impact on the valuation of the overall transaction. If an acquired company has been subjected to a data incident, or is shown to lack the proper data protection controls, the value of the deal can be reduced. Providing buyers and sellers with insights prior to the merger's "ink drying" allows for leverage and higher confidence during negotiations.

## Zero trust data access and control

During the evaluative process, sensitive information is required to be shared across parties - and it's not limited to just the employees of each party.  If third-party service providers or vendors are involved, it's essential to assess their security measures as part of the overall process. It's important to remember that weak links in vendor relationships can compromise the security of the transaction. This sharing can introduce risk to the organizations if not handled properly. Security, and controlled access of sensitive data will be required in order to prevent leaks or any unauthorized access.

Cyera's AI-powered classification delivers 95% precision and enriches valuable business and environment-specific context such as sensitive data masking, encryption state (plain text, hashed, tokenized, encrypted, etc), residency of the data data owner and data owner subject (employee, customer, vendor, patient, client, borrorower). These insights are combined with Cyera's Identity module. The identity module discovers human and non-human identities within the enterprise's environment, assigns a trust level to each identity, MFA posture, and most importantly, correlates those identities to what sensitive data they have potential access to. Cyera ensures controlled sharing of sensitive data, and protects against over-sharing of sensitive data as part of the M&A or divestiture. By overlaying identity and data materiality, Cyera lays the underlying foundation for zero trust access. What's more impressive,these insights can be passed along the enterprise's DLP service, security service edge (SSE) and extended detection & response (XDR) services, further reducing any lingering over-privileged access to the sensitive data that Cyera discovers.

## Lessen the compliance burden

Anyone who has gone through an M&A or divestiture will tell you that the data compliance burden is significant. This is due to the fact that both entities involved must ensure that they adhere to various legal, regulatory, and industry-specific standards throughout the process. This is especially pertinent when dealing with sensitive data like customer or employee personally identifiable information (PII),financial data,  intellectual property (IP), or other regulated information. Data privacy laws like GDPR are often top of the list of regulations because any companies operating in or dealing with data from the EU, which is the majority of most large organizations, must comply or face hefty penalties. It's also important to note that both the acquiring and selling companies must ensure compliance regarding any cross-border data transfers (which can involve significant changes in how data is handled post-transaction).

Any international M&As involve transferring data between multiple jurisdictions, which can trigger compliance within cross-border data transfer regulations. GDPR is a prime example due to its strict rules surrounding data transfers outside the EU, Standard Contractual Clauses (SCCs) and binding corporate rules (BCRs). Data processing, and data subject rights are additional factors that must be considered.

There are also industry-specific compliance requirements that are worthy of mention;. (1) HIPAA, which focuses on the handling of protected health information (PHI)(2) GLBA/ SOX within the Financial Industry, which governs the protection and disclosure of financial data. Industries such as energy, retail, telecommunications, and defense have their own data compliance requirements as well. All of these compliance mandates must be verified and maintained during M&A and divestitures.

From an internal perspective, data zoning is another factor to consider. Data zoning ensures that data storage respects the organization's policies around data sovereignty.

Cyera comes with out of the box policies mapped to the most critical compliance frameworks. Combined with Cyera's speed, scale and frictionless approach to data classification, such policies  accelerate the identification of gaps  Within GDPR, HIPAA, CCPA, and so many other critical regulations. Cyera's classification engine has been enhanced with industry-specific large language models (LLMs) and semantic classifiers. This allows for super high precision classification of sensitive data. Furthermore, by integrating industry-specific knowledge, our models grasp the nuances of specialized terminologies unique to sectors like Technology, Manufacturing, Healthcare, Food & Beverage, Real Estate and all other industries. This specialization leads to our models outperforming general purpose models, delivering results in days to weeks versus months to years.

**Healthcare example:** Healthcare providers manage a vast array of sensitive medical data, including patient assessments, test results, and drug information. Cyera's healthcare LLM precisely identifies and classifies each document type and the sensitive data they contain. Imagine a large healthcare organization that owns ten hospitals in different countries, some in the United States, some in Australia, and some in Canada. These hospitals process patient data, including health information releases and patient medical records. However, these documents are vastly different in terms of content, structure, and potentially even file type. Since the Cyera platform trained on healthcare-specific data, Cyera discovers, identified and classify these documents with high precision, even the weakest pattern

Cyera is also designed to help support data zoning requirements. In addition to the classification context provided in the platform, which includes data residency, Cyera monitors for data drift. For example, if EU citizen data is drifting to the US or if production data is drifting to the enterprise's development environment.

# Streamline data management processes

When it comes to data management, M&A and divestiture transactions can be quite different. In the case of M&A data from both entities must be integrated into a single system. Knowing what data exists, its level of sensitivity, and the context around that data is invaluable.

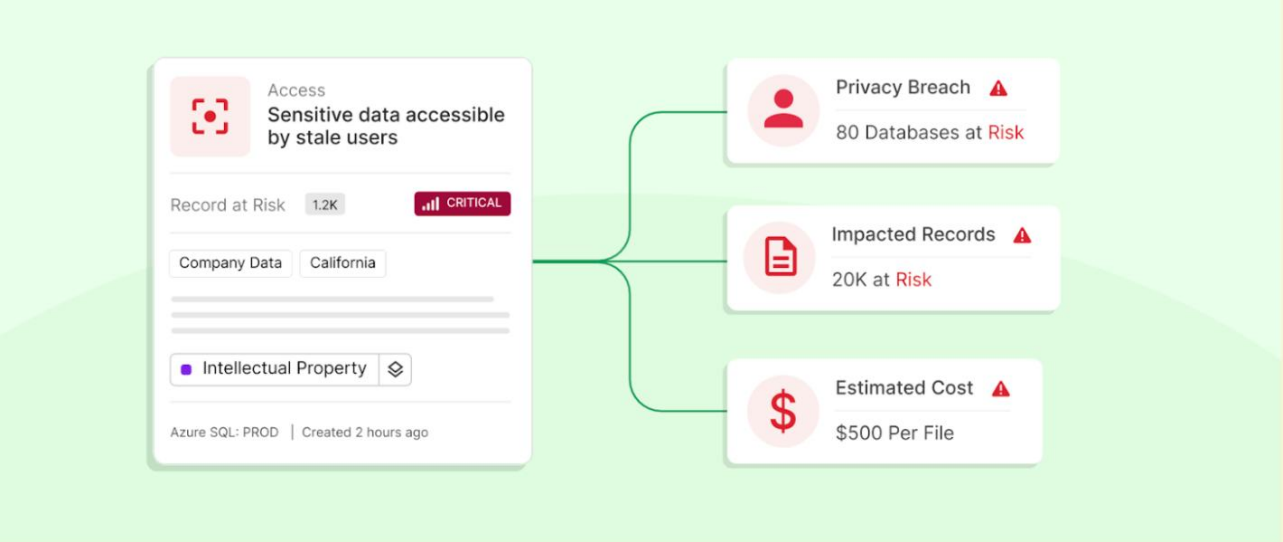
In a divestiture, separating data without compromising its security, or breaching confidentiality is the challenge. It requires careful planning to ensure that the divested entity takes only the data it needs, and nothing more. Knowing what data exists, areas of existing exposure, and areas of potential exposure are necessary. These are the insights that Cyera provides.

Cyera also improves data lifecycle management. Using context from its classification capability, Cyera identifies whether the acquired company is properly managing data retention and deletion policies - especially in the case of sensitive and regulated data. This also extends to shadow data as well (defined as data stored outside of an officially recognizes or “know” data store).

## Traditional Data Lifecycle

# Continuously monitor, detect, and respond to data incidents

After the M&A or divestiture is completed, the job of the data security team is not over. Data security during M&As and divestitures is not only about protecting information; it's also about ensuring the long-term success of the transaction, preventing reputational damage, and avoiding legal or regulatory repercussions. In order to do this, they must have an easy way to continuously monitor the data's integrity and security. It's no secret that these transactions are often an opportunity for purposeful or accidental exploitation. Threat actors may see the transition period as a time of vulnerability to exploit security gaps. Internal stakeholders may have access to sensitive data.




Given this hyper-level of attention, and constantly changing breach notification requirements, all parties involved must be prepared to handle any data breaches or security incidents. New SEC regulations, as well as existing regulations like GDPR and CCPA mandate reporting breaches within a given time frame, and any lapse in reporting could result in significant financial penalties and loss of brand reputation.

Cyera's Data Incident Response service provides both proactive, and re-active, guidance to develop a data incident recovery plan, understand the blast radius, accelerate recovery, and determine the materiality of a data incident. This service has proven invaluable in the case of M&A and divestiture activities both pre-transaction, and post-transaction.

With Cyera, security leaders can feel confident that as they look to accelerate M&A and divestitures for their business, that they have a data security platform in place that helps make the process simple, and secure.

To request a demo of Cyera for your team visit https://www.cyera.io/demo

## About Cyera

Cyera is reinventing data security. Companies choose Cyera to improve their data security and cyber-resilience, maintain privacy and regulatory compliance, and gain control over their most valuable asset: data. Cyera instantly provides companies with a holistic view of their sensitive data and their security exposure, and delivers automated remediation to reduce their attack surface.

Learn more at **www.cyera.io**, or follow Cyera on **LinkedIn.**

**Trusted by:**

SKECHERS · PELOTON · CHIPOTLE · AT&T · BlueCross BlueShield · Takeda · Constellation Brands · DELTA DENTAL · Rockwell Automation · Tyson Foods