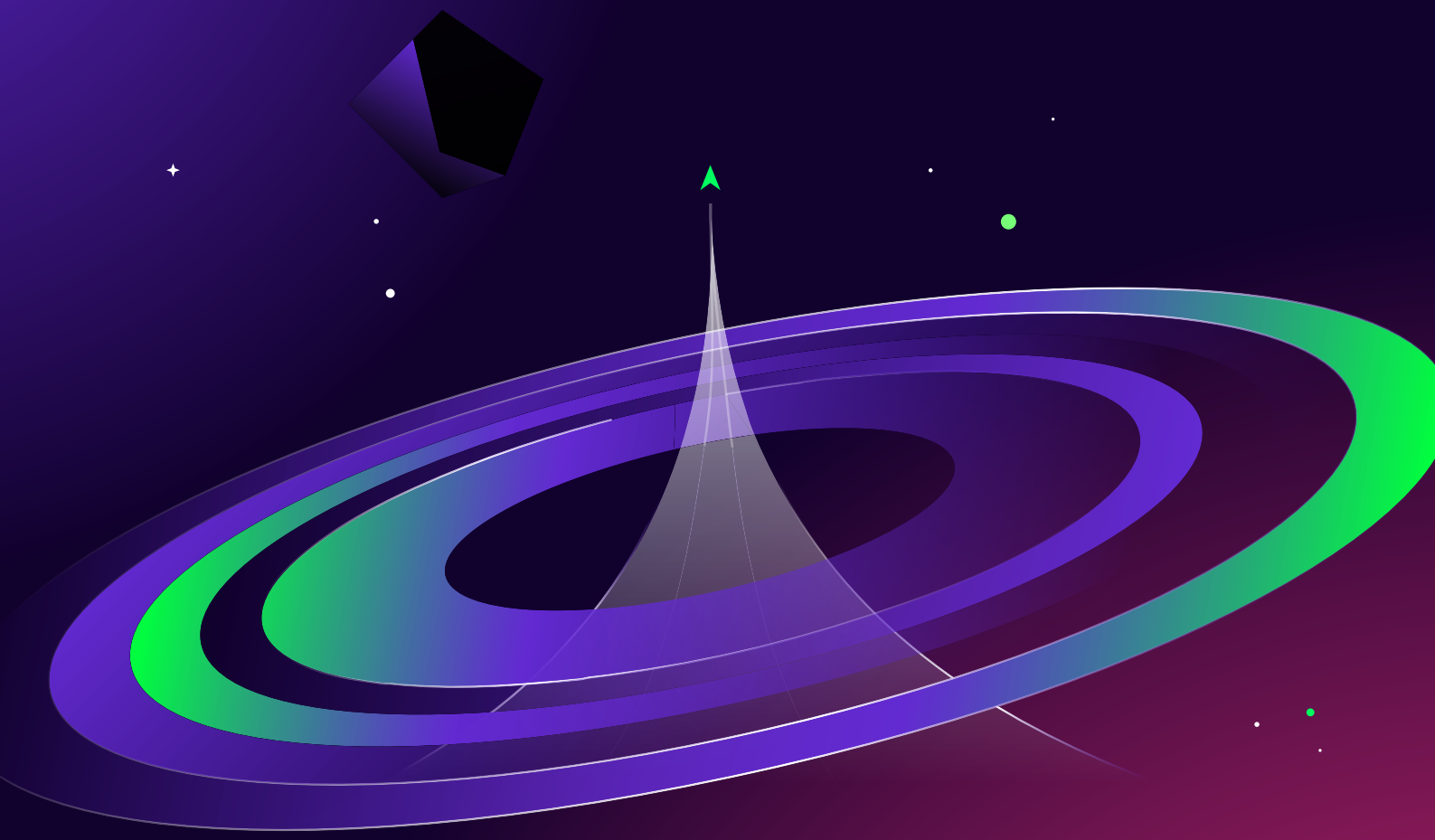
CYERA

GUIDE

Protecting Personal Data in Chile

How Cyera Supports Compliance with the PDPL

Table of Contents



Introduction

About the PDPL

The 2024 amendments to Chile's Personal Data Protection Law (PDPL) transformed the country's privacy framework into a modern, rights-based system aligned with the EU's GDPR. The reform broadened the law's scope to cover all entities—public and private—that process personal data and introduced extraterritorial reach for foreign data controllers targeting Chilean residents.

The updated PDPL is organized around eight core principles: lawfulness and fairness, purpose limitation, proportionality, quality, responsibility, security, transparency and information, and confidentiality. In addition to the traditional "ARCO" rights—access, rectification, deletion, and objection—individuals also gained the rights to portability, restriction of processing, and protection against automated decision-making.

The reform mandates data protection impact assessments, security breach notifications, and privacy-by-design obligations, modernizing Chile's privacy regime while strengthening citizens' control over personal information and bolstering cybersecurity.

About Cyera

Cyera is a unified, AI-native data security platform that empowers businesses to manage sensitive data across highly permissive and widely distributed environments with precision and efficiency.

The platform's non-invasive, automated data discovery provides a comprehensive view of sensitive data across structured and unstructured sources. This capability enables organizations to address critical challenges like data proliferation. Powered by AI-driven classification, Cyera goes beyond traditional methods by understanding context, intent, and nuance. This deep insight helps uncover ghost data, reveal data risks, reduce false positives, and mitigate threats like data breaches and ransomware — areas where conventional data loss prevention and data governance tools fall short.

By combining advanced technology with ease of use, Cyera empowers organizations to confidently secure personal data, support PDPL compliance, and safely enable AI use cases.

Principles for Processing Personal Data

Article 3 stipulates that data must be processed in accordance with the following eight principles:

- **Lawfulness and fairness:** data must be processed with the consent of the data subject, unless some other lawful exception applies; data may not be collected or processed deceptively or in a way that would harm the data subject or upset their reasonable expectations.
- **Purpose limitation:** data must be collected for specific, explicit, and lawful purposes, and processing of data must be limited to these purposes.
- **Proportionality (minimization):** only those personal data that are necessary, adequate, and relevant to the purposes of processing may be processed.
- **Quality:** personal data must be accurate, complete, current, and relevant in relation to their provenance and the purposes of processing.
- **Responsibility:** data controllers and data processors are legally responsible for complying with the PDPL's requirements.
- **Security:** data controllers must adopt adequate security safeguards. They must protect personal data from unauthorized or unlawful processing, loss, leakage, damage, or destruction. The security measures should be appropriate given the nature of the data and how it is to be processed.
- **Transparency and information:** data controllers must provide data subjects with clear and easily accessible information about how to exercise their rights under the law.
- **Confidentiality:** data controllers must put in place adequate safeguards to ensure the confidentiality of data subjects' personal data.

The cornerstone of lawful data collection and processing is consent. Cyera Privacy will soon be equipped with consent management, allowing your organization to manage user consent for cookies, tracking technologies, mobile software development kits (SDKs), and other processing activities.

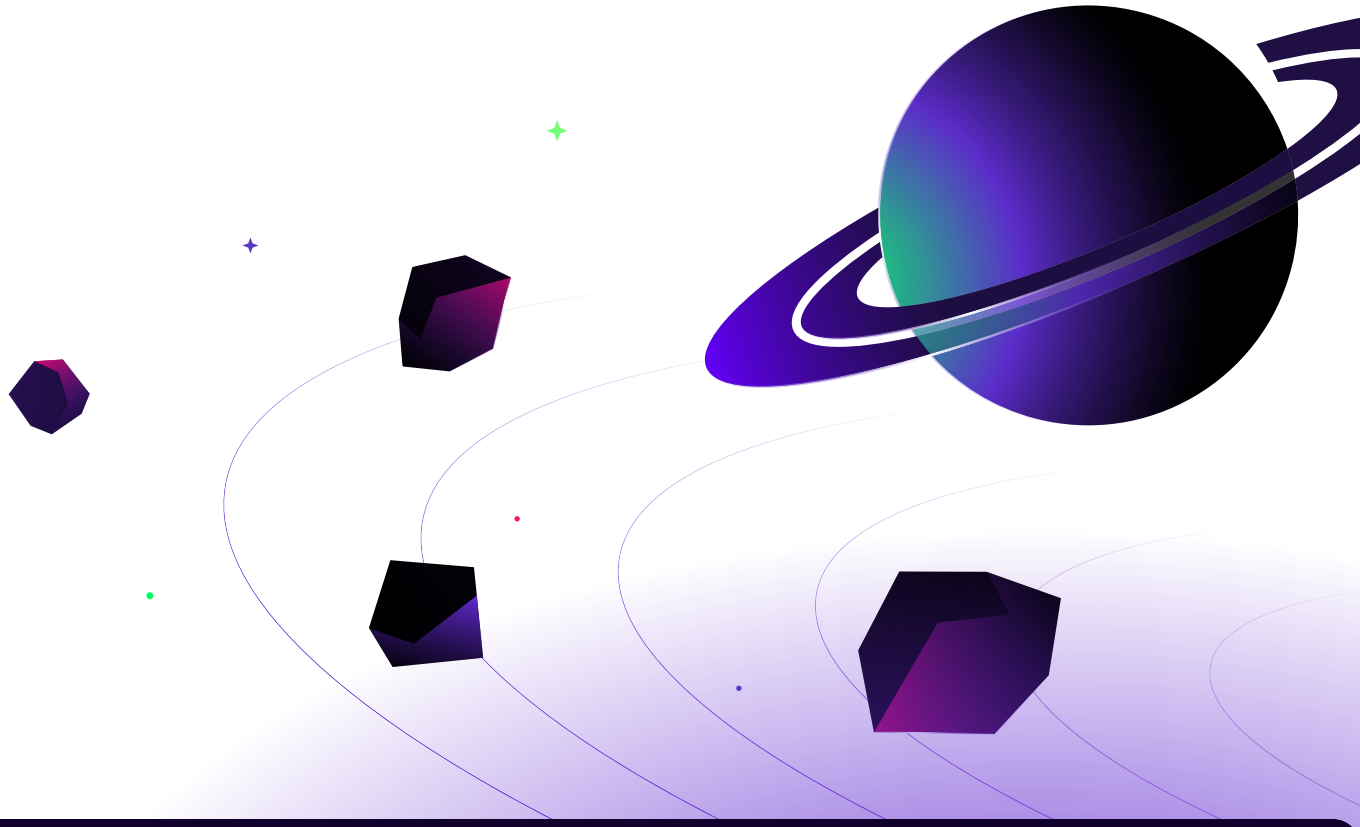
Cyera periodically scans your entire data estate, including cloud and on-prem resources, helping you build an up-to-date personal data inventory that ensures collection is specific, relevant, and current, supporting the requirements of purpose limitation, proportionality, and quality. Cyera also supports the proportionality and quality principles by identifying stale or ghost data stores that should be securely destroyed.

Cyera's Identity Access module integrates with identity providers like Okta to identify human and non-human entities with access to your data. Through these integrations, Cyera can identify stale identities who have either left the organization or changed roles, as well as surface identities that have not enabled multifactor authentication. These safeguards help support the security and confidentiality principles.

Data Subjects' Rights

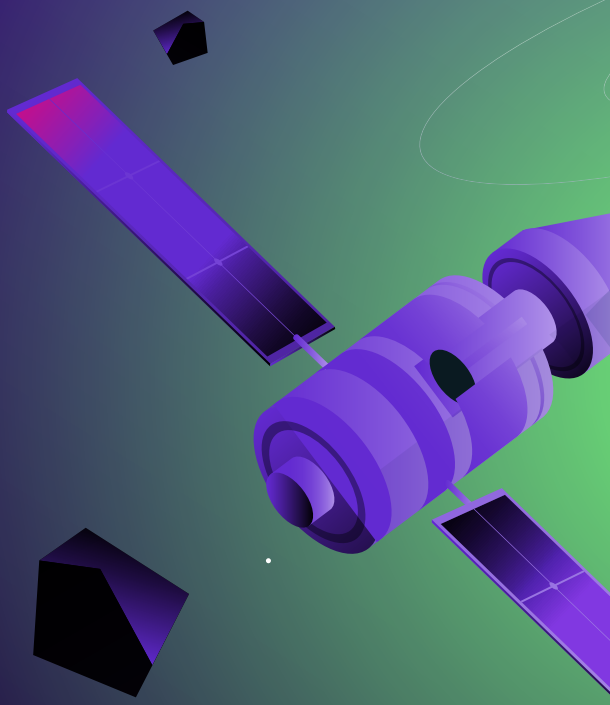
Articles 4 through 11 govern the rights of data subjects under the PDPL. These include the rights of:

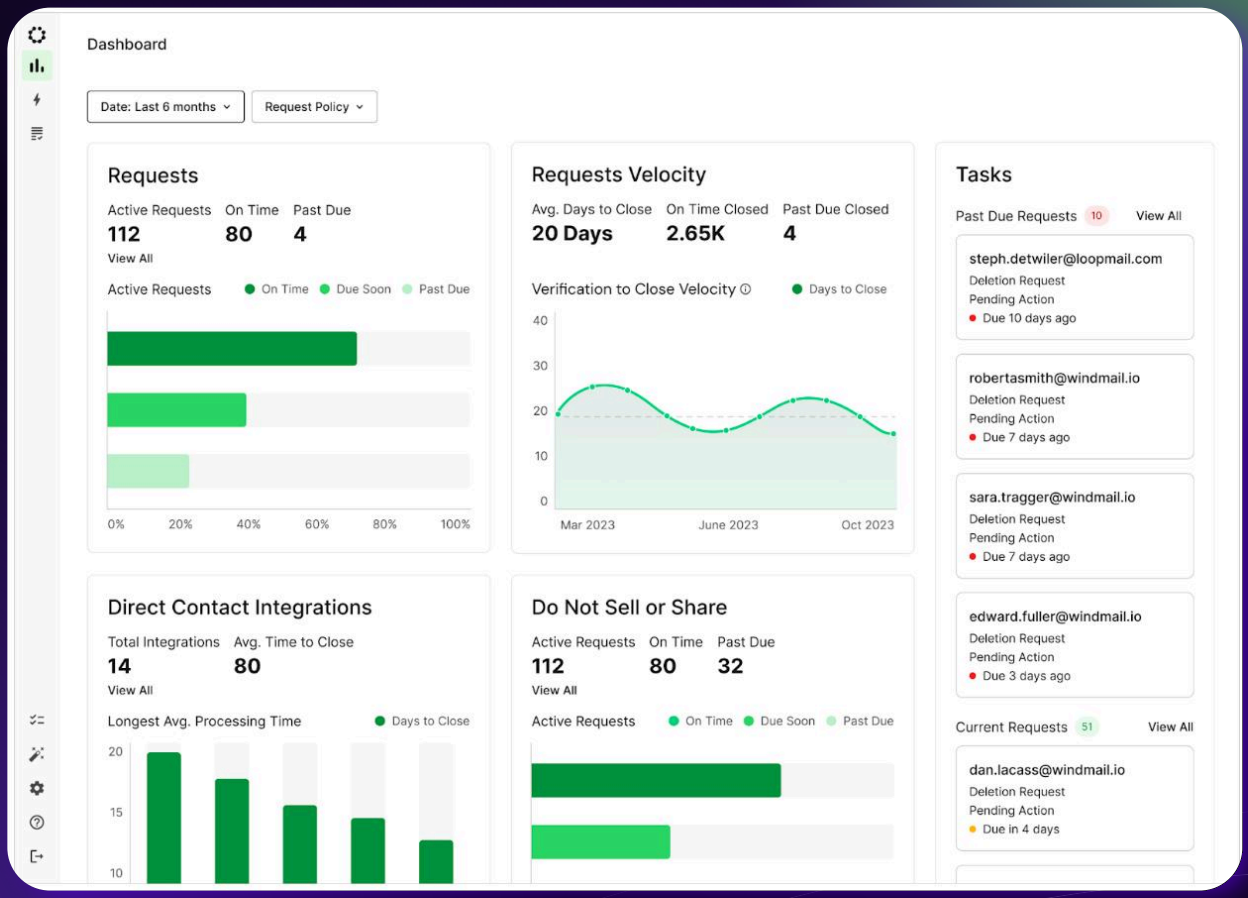
- **Access:** data subjects have a right to know what data controllers have collected/processed, its origin, the purpose(s) for which it was processed, how long it will be retained, and any third parties to whom it has been transferred.
- **Rectification:** data subjects have the right to request correction of inaccurate, incomplete, or outdated data.
- **Deletion:** data subjects have the right to request deletion of data in certain circumstances, such as when the data are outdated, when they are not necessary to fulfill the purpose for which they were collected, or when the data subject has revoked consent.
- **Opposition:** data subjects have the right to object to the processing of their personal data in certain circumstances, such as when the data was gathered from a public source, or is processed solely for the purposes of direct marketing.
- **Objection to automated decisionmaking:** data subjects have the right not to be subject to decisions based on the automated processing of their data where those decisions produce significant legal consequences.
- **Suspension of processing:** data subjects have the right to request the temporary suspension of processing of their personal data when making a request for rectification, deletion, or opposition.
- **Portability:** data subjects have the right to receive a copy of their personal data in a structured, generic, and commonly used format that permits them to transfer their data to another controller.



Cyera can help your organization streamline the process of fulfilling data subject requests (DSRs). Cyera enables granular discovery of all data belonging to a subject and classifies data by residency or source.

Cyera's unified DSR intake and fulfillment automates the handling of access, correction, erasure, objection, and portability requests (see image below). Cyera validates requester identity, executes secure data retrieval, deletion, or reduction actions, and maintains audit trails to demonstrate timely and complete fulfillment.





Data Security and Protection Measures

The PDPL requires organizations to implement technical and organizational measures tailored to the sensitivity, scope, and risk of data. These measures include:

- **Pseudonimization and encryption** of personal data
- The ability to ensure the **confidentiality, integrity, availability,** and **resilience** of information processing systems.
- The ability to **restore availability and access** to personal data quickly in the event of an incident.
- **Regular assessments** of the effectiveness of these measures.

Cyera's AI and data security platform can identify unencrypted personal data at rest or in motion, and apply policies to obfuscate unencrypted data and alert data owners to take remedial actions.

Cyera integrates with identity providers like Okta to create a catalog of identities with access to your data estate, including internal and external users. Cyera can identify stale or ghost identities that should no longer have access, and can see which entities have disabled multifactor authentication.

Cyera's AI Guardian (including AI Security Posture Management and AI Protect) can identify embedded AI apps, homegrown AI tools, and public AI apps in use in your organization, and enforce policies to prevent AI from ingesting sensitive data, as well as blocking sensitive data from leaking through AI outputs.

Through its integration with Cohesity, Cyera enhances your cyber resilience by helping you prioritize your backup policies based on the sensitivity and criticality of your data.

Finally, Cyera offers various professional services - including its Data Risk Assessment and AI Readiness Assessment - that can help you evaluate the effectiveness of the technical and organizational measures you have implemented for data security.

Data Breach Notification

Violations of security measures resulting in risk to data subjects must be reported to the Personal Data Protection Agency “without undue delay.” Where the breach concerns sensitive data, financial data, or data pertaining to children, notification must also be provided to data subjects in clear language.

Notifications must include the nature of the incident, its effects, the categories of data that were exposed, which data subjects were affected, remedial actions taken by the data controller, and any measures the controller has put in place to prevent future breaches.

Cyera’s data security platform helps your organization simplify breach response by quickly identifying all impacted personal data - including unstructured personal data - generating reports and determining the materiality of a breach.

Transfers of Personal Data and Supervision of Third Parties

Unless some other legal basis for making the transfer exists, data controllers must obtain the consent of data subjects before transferring their data to a third party or third country. Controllers must disclose the destination and purpose of the transfer.

Data controllers must utilize contract terms to bind third party data processors, ensuring that they provide the same quality of security and governance controls over transferred data.

Cyera’s DSPM enables filtering by data subject residency, allowing you to build an inventory specifically of Chilean data subjects. It also enables you to monitor which third parties are accessing personal data, and set policies to flag non-Chilean vendors accessing Chilean data subjects’ data.

Cyera helps you protect data integrity and supervise third party processors by giving you visibility into which identities are accessing your data and what actions they have taken.

Duties of Controllers and Processors

The PDPL requires controllers to appoint a data protection officer and maintain a record of data processing activities. They must also perform data protection impact assessments for high-risk processing activities. These include:

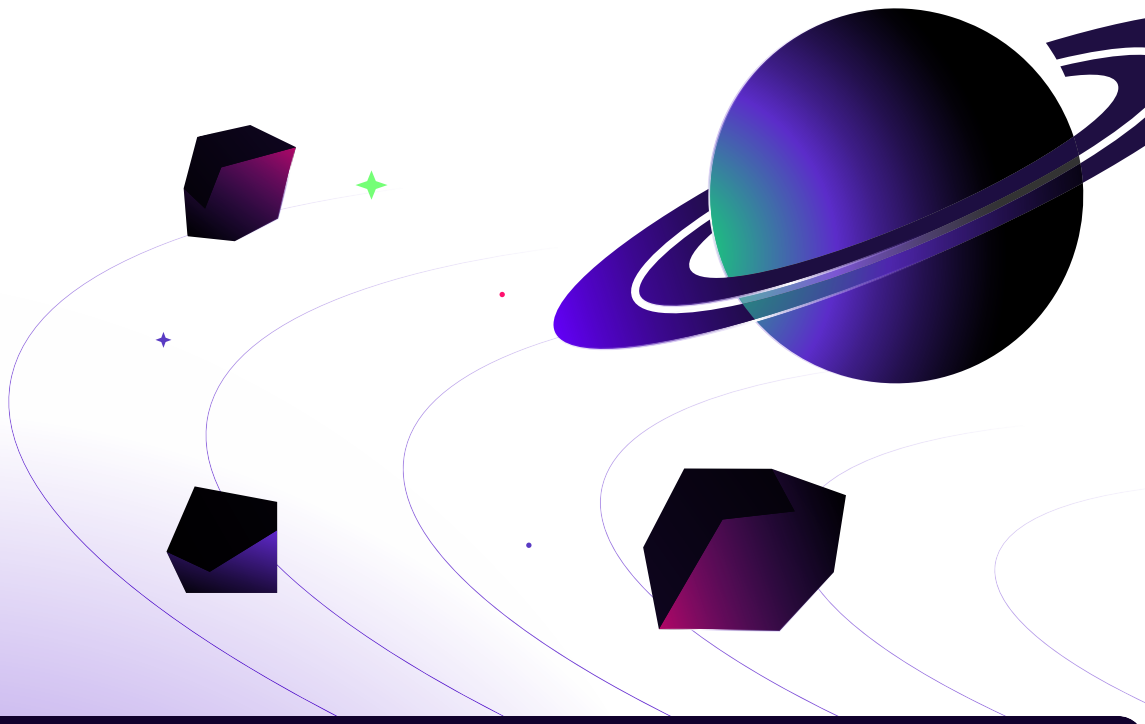
- Processing activities that involve **profiling** or **automated decisionmaking.**
- **Large-scale** data processing.
- **Systematic monitoring** of public areas.
- Processing of **sensitive** or **specially protected data.**
- **Storage Limitation:** Data controllers may not retain data subjects' personal data longer than authorized by law. The retention period is terminated when the purpose for the data's collection has been achieved, at the end of the stipulated processing period, when the data subject revokes consent, or when determined by the relevant authorities.

While it is each organization's responsibility to appoint a DPO or other responsible person for data protection, Cyera can provide services - such as its Data Risk Assessment or AI Readiness Assessment - to help those persons better understand the organization's data security posture and develop a plan for improving your data security posture going forward, including timelines and milestones.

By pre-filling the data-focused sections of a Record of Processing Activity (RoPA) - including things like categories of personal data, categories of data subjects, categories of recipients, data transfers, and technical security measures in place - Cyera accelerates the process of completing RoPAs.

Cyera can help inform the process of performing Data Protection Impact Assessments by creating an inventory of your organization's personal data and analyzing the impact of security configuration changes on sensitive data.

Cyera's Data Risk Assessment and AI Readiness Assessment services can also help surface data security risks - in particular those associated with AI deployments - and recommend strategies for mitigating risk, including timelines and milestones.




CYERA