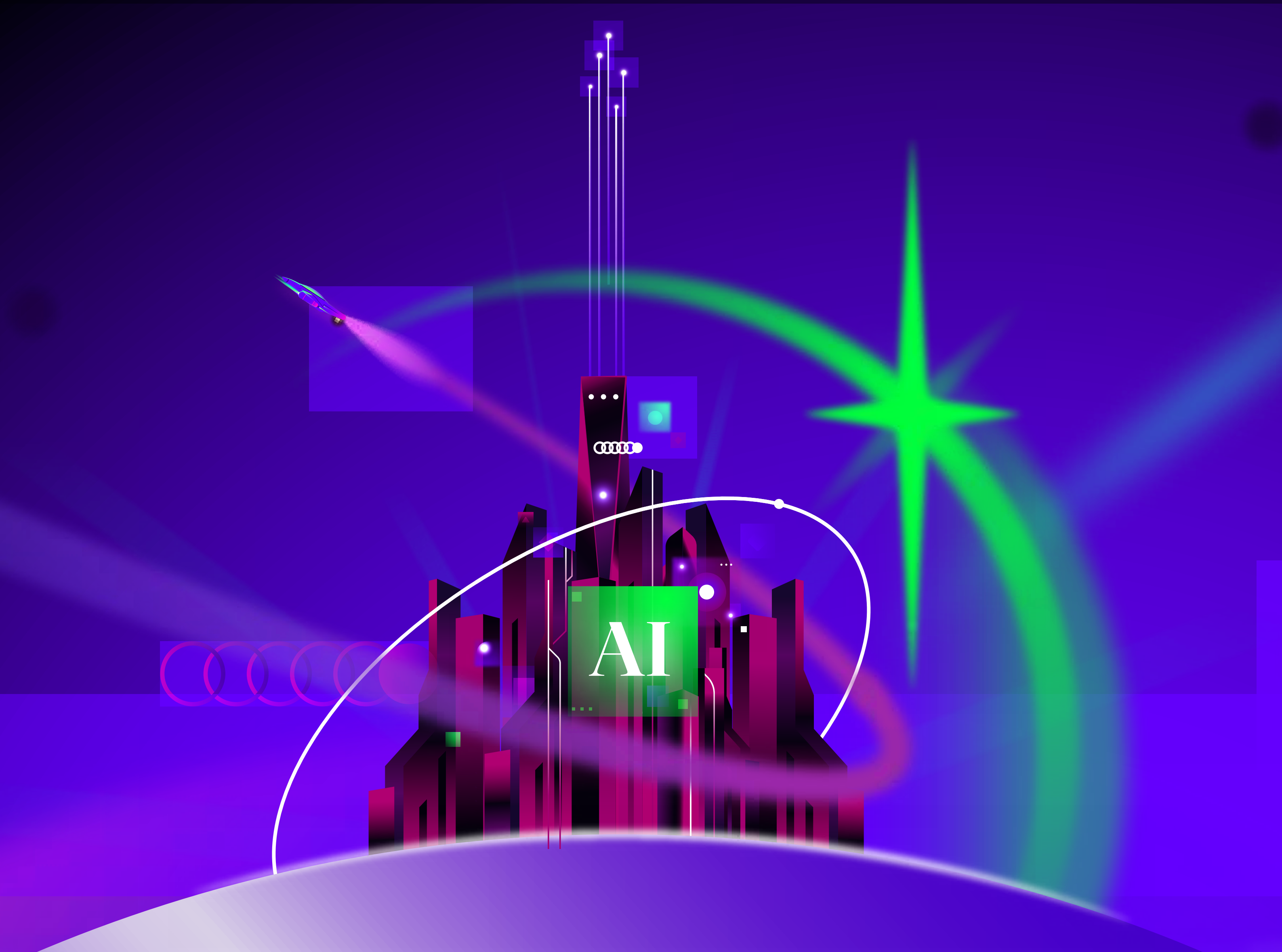
CYERA

Securing GenAI Adoption: A Data -Centric Executive Guide

How data security is aligning CISO, CDOs, and CIOs



While in the past the use of predictive AI has become commonplace, Generative Artificial Intelligence (GenAI), is a newer technology set making waves within the market. As GenAI quickly reshapes the business and technology landscape, the opportunity to drive innovation, efficiency, and competitive advantage is there for every business leader to seize. However, with that opportunity comes risk - especially when it comes to securing the data that fuels AI.

As of early 2025, approximately 65% of enterprises report regularly using generative AI (GenAI) technologies, a significant increase from previous years. This surge reflects a growing recognition of GenAI's potential to transform business operations. Projections indicate that by 2026, up to 80% of enterprises will have incorporated GenAI into their workflows. Yet, 71% of AI tools fall into the "high or critical risk" categories, 39.5% of these tools inadvertently expose user data, and nearly 35% of data being input into AI tools is sensitive. This trend underscores the rapid adoption and integration of GenAI across various industries.

It is for this reason why the most effective leaders will recognize that data is the foundation of AI, thus making data discovery, and data sensitivity, the most important factor in AI adoption.

This guide outlines why a data-led approach is critical to enabling the safe adoption of AI, and discusses how this new approach empowers CISOs, CDOs, and CIOs to fulfill their mandates while aligning toward a common goal: driving innovation without compromising trust. Within this guide, we also provide a recommended journey that IT leaders can learn, implement, and benefit from as they look to safely roll out GenAI solutions within their environment.

The Growing Complexity of AI Risk Revolves Around Data

AI adoption accelerates digital transformation, but it also introduces new complexities around data governance, privacy, and security. Traditional risk models fall short when AI systems are built on massive, dynamic datasets that include sensitive, unstructured, structured, regulated, and or proprietary data. As a result, data becomes the primary attack surface, compliance burden, and ethical risk vector in AI-motivated organizations.

Some common data-centric risks of AI:

- **Data Privacy and Confidentiality -** AI systems often require large datasets, which may include sensitive personal or corporate information. The infusion of un-santized, sensitive data, or mishandling of this data, can lead to privacy breaches and regulatory non-compliance.
- **Data Loss:** AI can introduce data loss risks through prompt inputs, generated responses, and chatbot interactions. Sensitive data may be exposed if prompts or outputs aren't properly monitored. Prompt and response analysis help catch confidential info before it's processed or leaked, while chatbot monitoring detects misuse or unintentional disclosure in real time.
- **Overprovisioned access:** AI systems often operate with broad data access, increasing the risk of overprovisioned permissions and unintended exposure of sensitive files. Without proper controls, AI may access more data than necessary for its task, violating least privilege principles. To reduce this risk, organizations need robust AI file access control, comprehensive auditing of data interactions, and strong governance to ensure AI only uses data it's authorized to see.
- **Model Inaccuracy and Reliability -** AI models may produce inaccurate or unreliable outputs, especially when trained on biased or incomplete data. Such inaccuracies can lead to erroneous decisions and undermine trust in AI systems. A survey indicated that 44% of organizations experienced issues related to AI inaccuracy, underscoring the importance of rigorous validation and monitoring.

To safely and effectively harness AI, it's essential for teams to take a data-led approach. This means starting by first identifying, classifying, and securing sensitive data wherever it resides. Then, understanding the AI systems within your organization, and how data is being used by those AI systems. Lastly implementing controls that scale with AI adoption, monitoring for issues, and taking action when absolutely necessary.

Three Reasons Why a Data-Led Approach Matters

A data-led approach puts data at the center of AI strategy, aligning security, governance, and innovation. It provides:

01 | Visibility:
Understand what data you have, where it lives, who can access it, and how it is used.

02 | Control:
Apply consistent policies and controls to protect sensitive data, regardless of where it flows.

03 | Accountability:
Track how Gen AI tools and AI models access and use data to ensure compliance and ethical use.

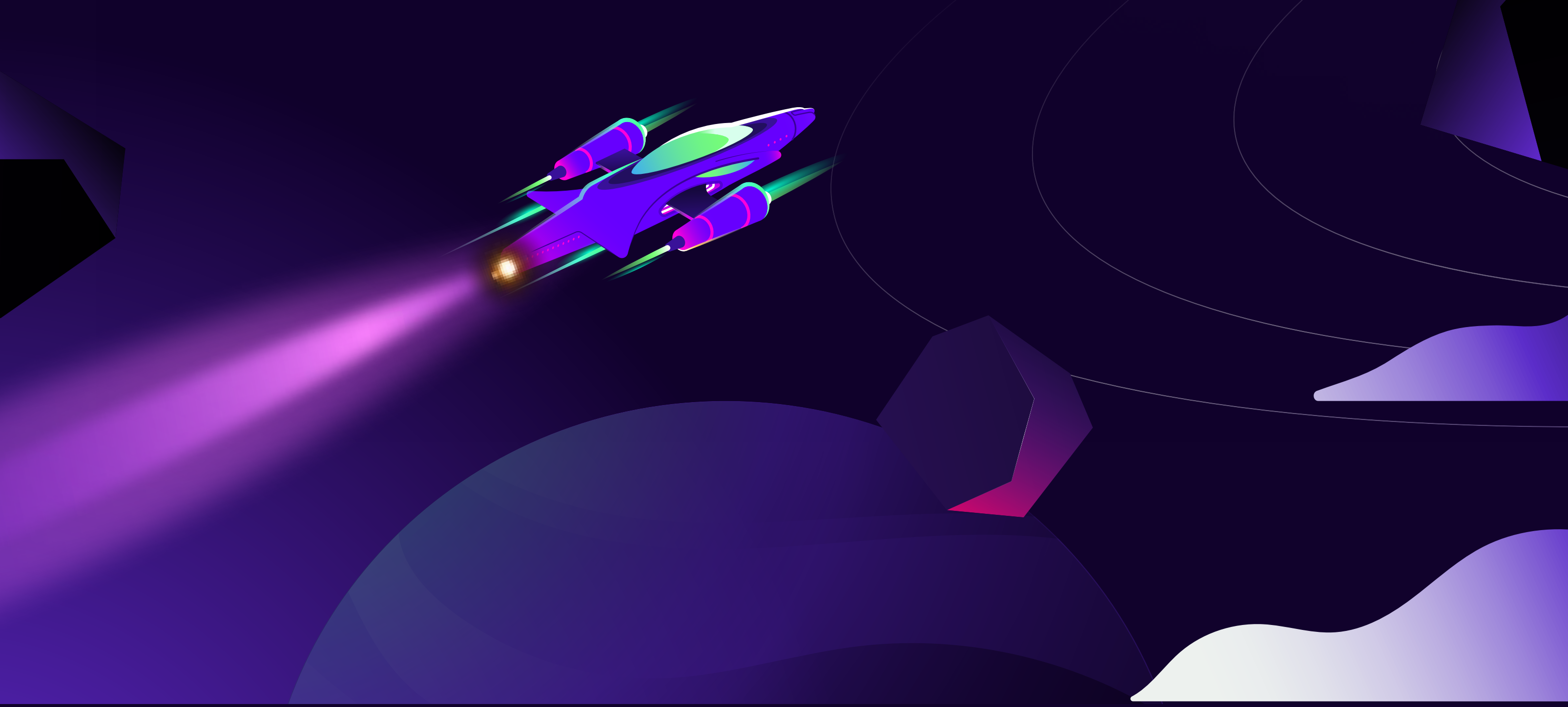
The Modern Enterprise *AI* Journey

The below image outlines the journey that Fortune 500 IT leaders are taking when looking to adopt GenAI to boost their company's productivity. We suggest IT leaders follow the steps within this journey to give themselves the greatest probability of succeeding in their mission.

Securely Accelerate Business Use of AI

1	2	3	4	5	6
Know Your Data	**Define AI Use Cases**	**Embrace AI Tools**	**Scale AI Tech Stack**	**Build AI Culture**	**Monitor, Optimize, Innovate**
✦ Identify data sources	✦ Align with strategic goals	✦ Choose the right AI approach	✦ Adopt AI Infra (Cloud, GPUs etc.)	✦ Develop company's AI Literacy	✦ Track metrics & expand use

> "80% of unauthorized AI transactions will be caused by internal violations of enterprise policies concerning information oversharing, unacceptable use or misguided AI behavior" - *Gartner*



How C-Level IT Leaders Can Seize The AI Opportunity

Let's discuss the benefits of this approach for each individual leader.

What a data-led approach means for the CISO

For the Chief Information Security Officer, AI presents both a challenge and an opportunity. A data-led approach allows the CISO to:

- **Reduce the organization's AI risk profile** by securing sensitive data used in training, and knowing what sensitive data is accessible by GenAI tools
- **Data DNA** that serves as a persistent identity for data elements and is comprised of metadata like type, role, identifiability, sensitive, security posture, and residency helps with consistent enforcement of security policies across cloud, on-prem, and hybrid environments
- **Demonstrate to industry regulators** and stakeholders that data security is embedded in the AI lifecycle.

Impact on the business: The CISO gains a proactive security posture that reduces the risk of breaches, data leaks, and compliance failures.

What a data-led approach means for the CDO

For the Chief Data Officer, success depends on enabling data-driven innovation while maintaining control and compliance. A data-led approach helps the CDO to:

- **Streamline data discovery,** classification, and governance across silos.
- **Enable safe data sharing** and AI experimentation by de-risking sensitive data.
- **Ensure the quality,** lineage, and compliance of data used in AI pipelines.

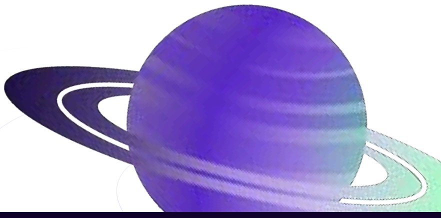
Impact on the business: The CDO can accelerate AI initiatives without sacrificing governance, making data a trusted asset rather than a liability.

What a data-led approach means for the CIO

For the Chief Information Officer, the focus is on enabling innovation and scaling technology responsibly. A data-led approach supports the CIO by:

- **Providing the foundation for secure** and scalable AI infrastructure.
- **Aligning IT** and data governance teams around a shared set of data controls.
- **Minimizing redundant, obsolete, and trivial data** to reduce costs, and other operational friction between innovation and risk management functions.

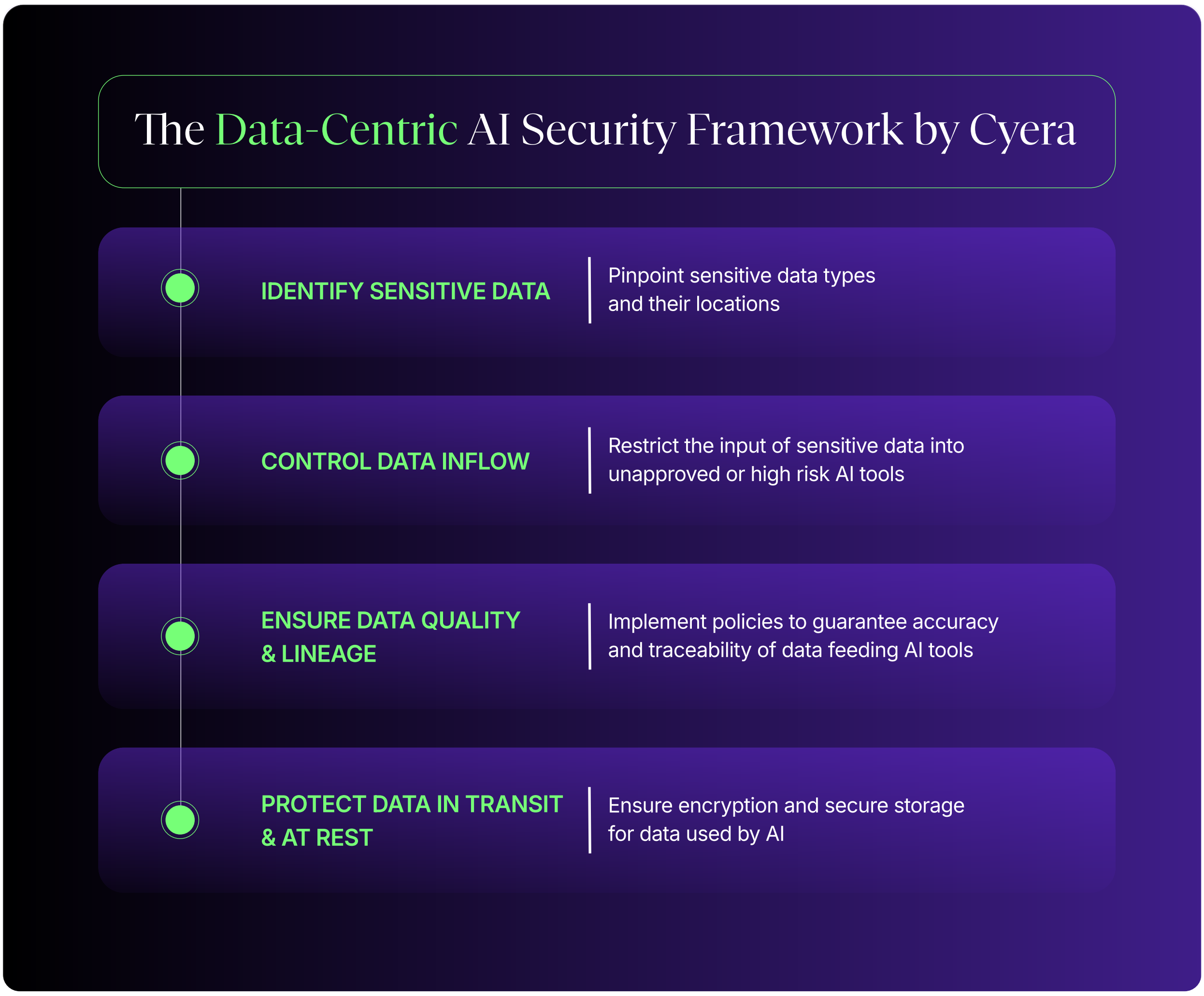
Impact on the business: The CIO gains a clear path to scale AI adoption while maintaining operational integrity and regulatory compliance.



Aligning Around Data to Power Safe AI Adoption

Safely adopting AI through a data security-led approach is ideal for CISOs, as well as their CDO, and CIO counterparts. This is because it ensures that AI initiatives are both innovative and secure. By prioritizing data security from the outset, leaders can build trust in AI-driven processes while maintaining regulatory compliance and protecting sensitive information.

This framework below serves as guidance for how to take a data-centric approach to AI Security.



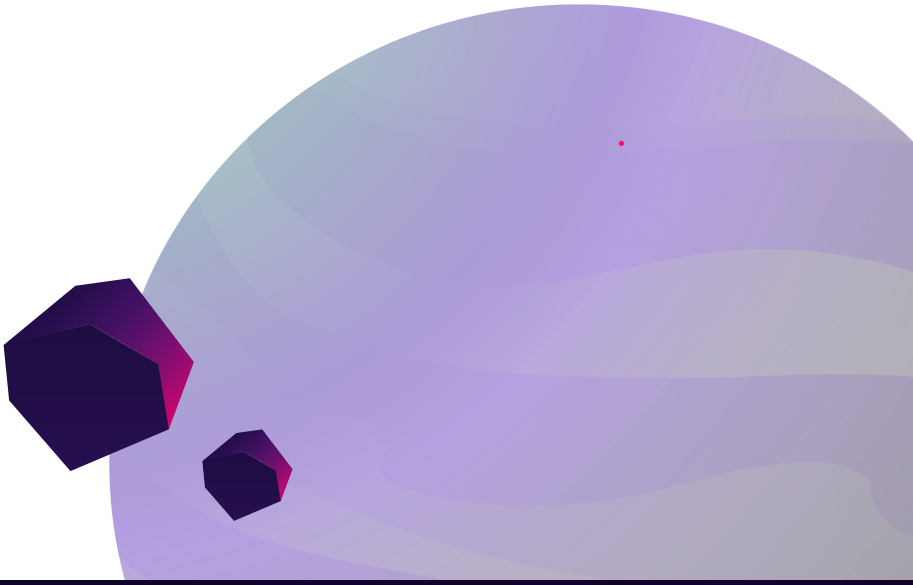
The Data-Centric AI Security Framework by Cyera

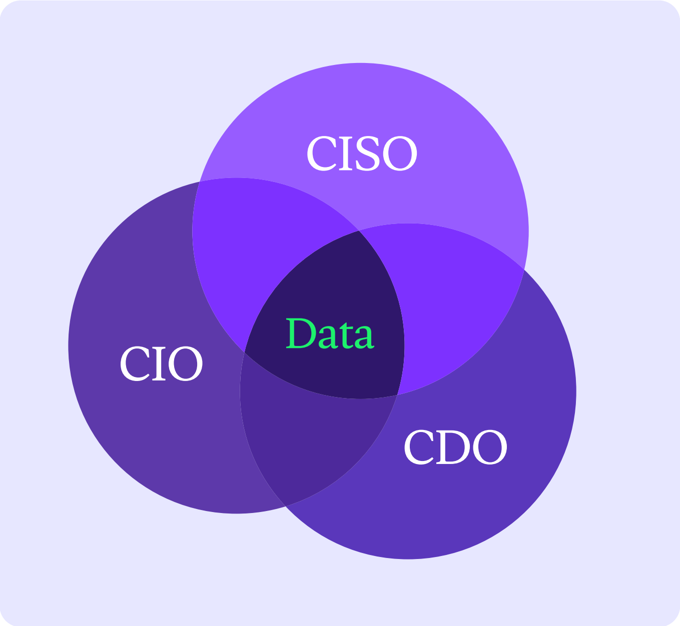
IDENTIFY SENSITIVE DATA — Pinpoint sensitive data types and their locations

CONTROL DATA INFLOW — Restrict the input of sensitive data into unapproved or high risk AI tools

ENSURE DATA QUALITY & LINEAGE — Implement policies to guarantee accuracy and traceability of data feeding AI tools

PROTECT DATA IN TRANSIT & AT REST — Ensure encryption and secure storage for data used by AI





There is an even greater benefit that comes from this alignment though. This approach fosters stronger collaboration between CISOs, who focus on security risks, CDOs, who manage data integrity and analysis, and CIOs, who drive technological innovation for the business. By dropping data into the center of this C-level triangle, these leaders will easily create a unified strategy that enables AI adoption without compromising security, ensuring AI delivers business value while remaining resilient against cyber threats.

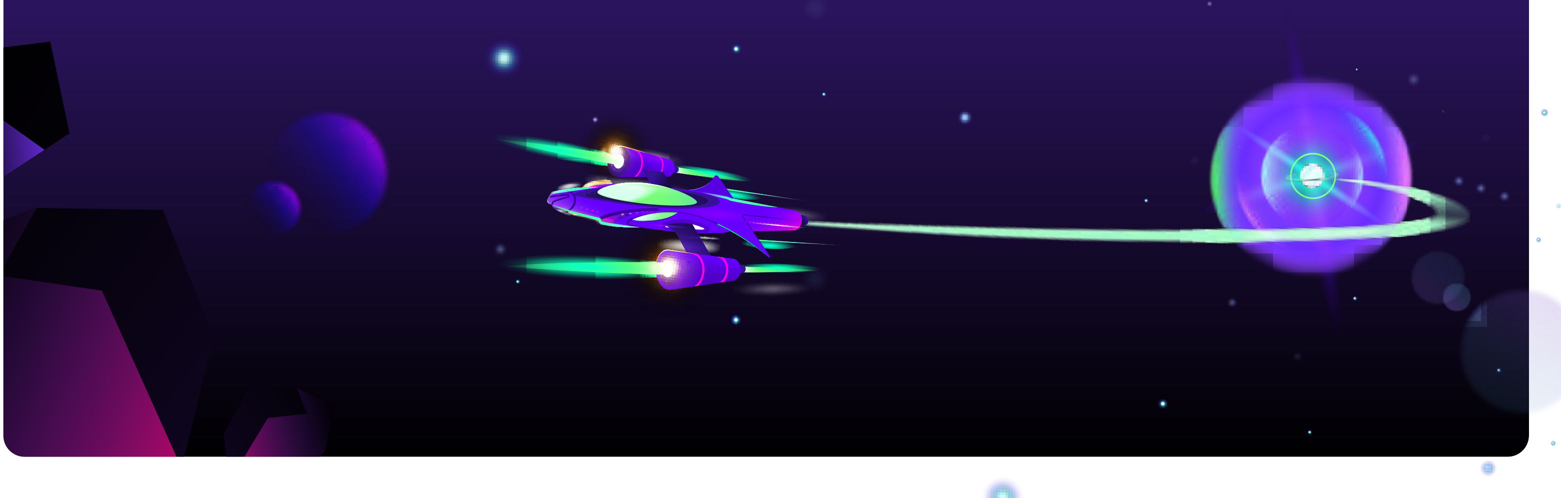
Expected Benefits

- Cross-functional coordination in managing data risks in AI initiatives.
- Reduced friction between innovation and compliance teams.
- Faster, safer deployment of AI models in production environments.

AI is only as secure, compliant, and ethical as the data that powers it. By making data the control plane for AI adoption, organizations can enable innovation at speed and scale without compromising on trust. A data-led approach unites the goals of leadership—making it the key to enabling safe, responsible, and transformative AI.

This strengthened partnership will pay dividends beyond just AI adoption, but for future business initiatives in the future as well.

Let us walk you through the Safe AI Adoption Journey.
Meet with our team here at Cyera https://www.cyera.com/demo



CYERA

CYERA.IO