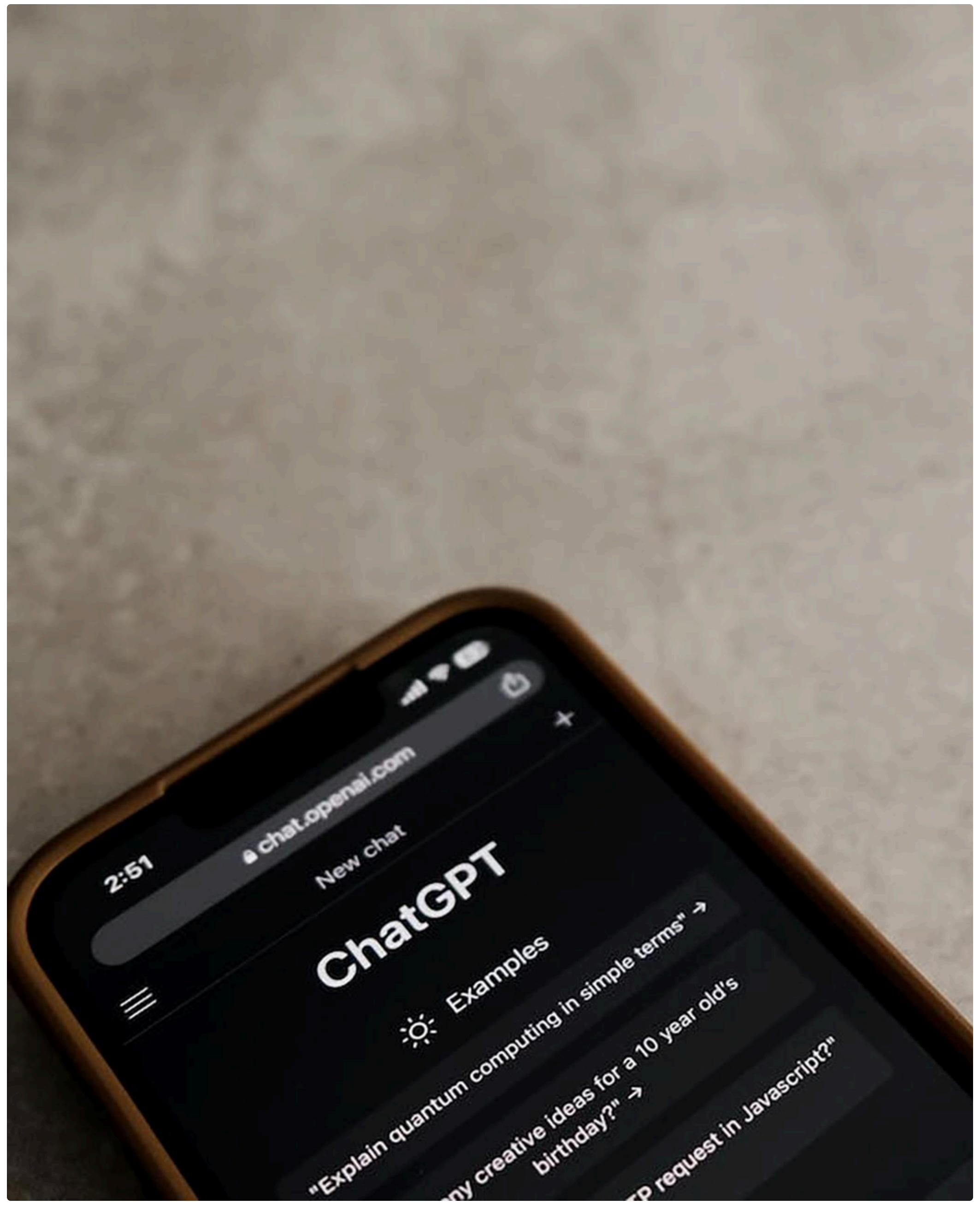
ideaBOX
THINK B4U CLICK


2:51
chat.openai.com
New chat
ChatGPT
Examples
"Explain quantum computing in simple terms" →
ny creative ideas for a 10 year old's birthday?" →
P request in Javascript?"

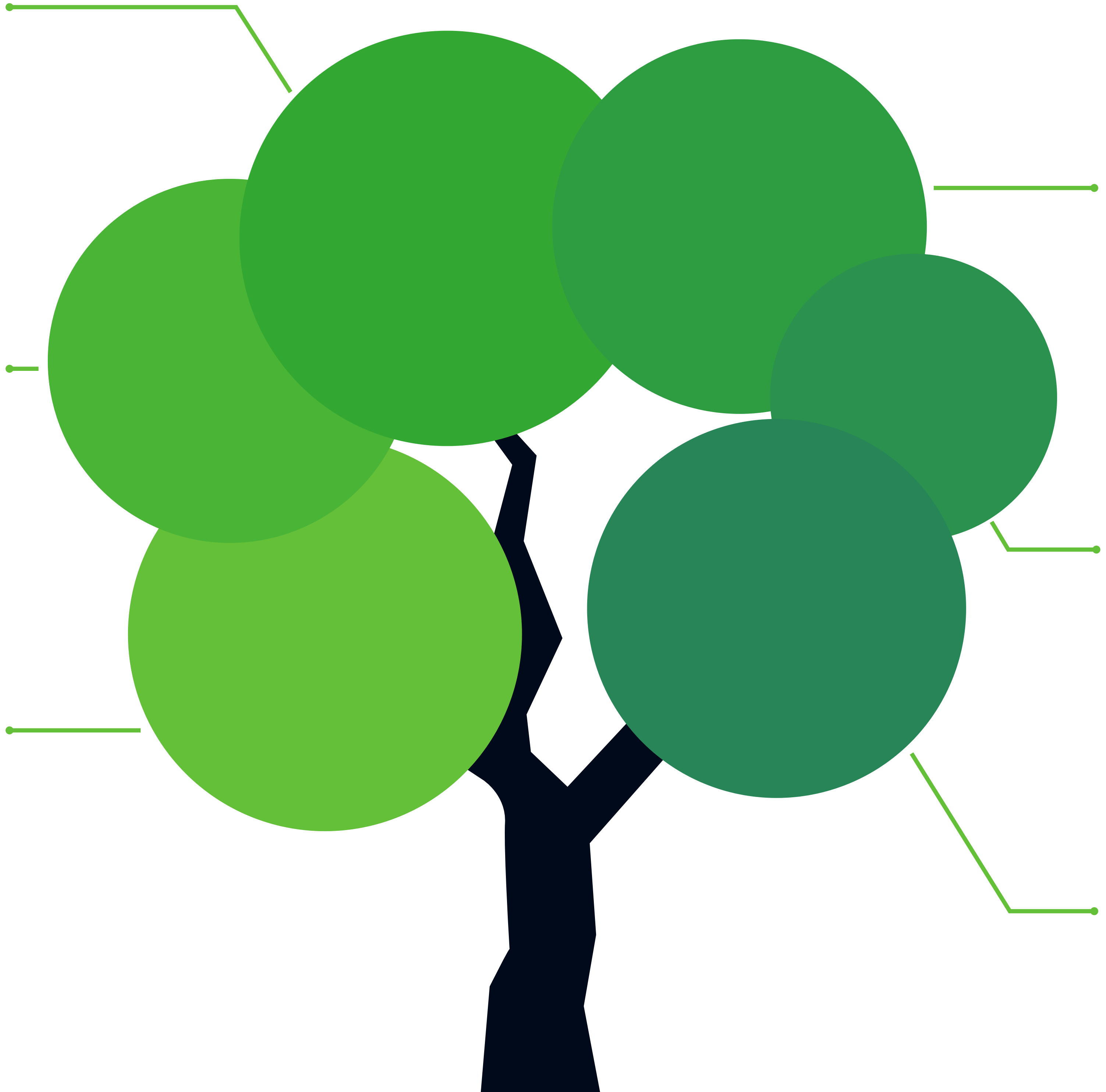
ENHANCING AI SECURITY IN ORGANIZATIONS WITH IDEABOX AND ACTIFILE

This presentation delves into how ideaBOX collaborates with Actifile to empower organizations in understanding and securing their AI tool usage, specifically focusing on ChatGPT, Microsoft Copilot, and Grok. It features a case study from the financial services sector, illustrating the challenges posed by sensitive data exposure, the innovative solutions implemented by ideaBOX, and the remarkable outcomes achieved.

James Oliverio

UNDERSTANDING CLIENT AI USAGE RISKS

Assessing AI tool risks in financial services to protect sensitive data



Challenge: Unmonitored AI tool use

Risk of exposing **sensitive client** and internal data.

Company Size: 1,000+ employees

Significant workforce managing sensitive data.

Industry: Financial Services

Focus area of the client company.

AI Tools: ChatGPT, Grok, Microsoft Copilot

Examples of tools posing **data risks**.

Solution: ideaBOX’s AI Usage Risk Assessment

Utilizes **Actifile’s** observability and risk scoring.

Goal: Protect sensitive data

Ensuring client and internal data security.

UNDERSTANDING HIDDEN RISKS IN AI PRODUCTIVITY TOOLS

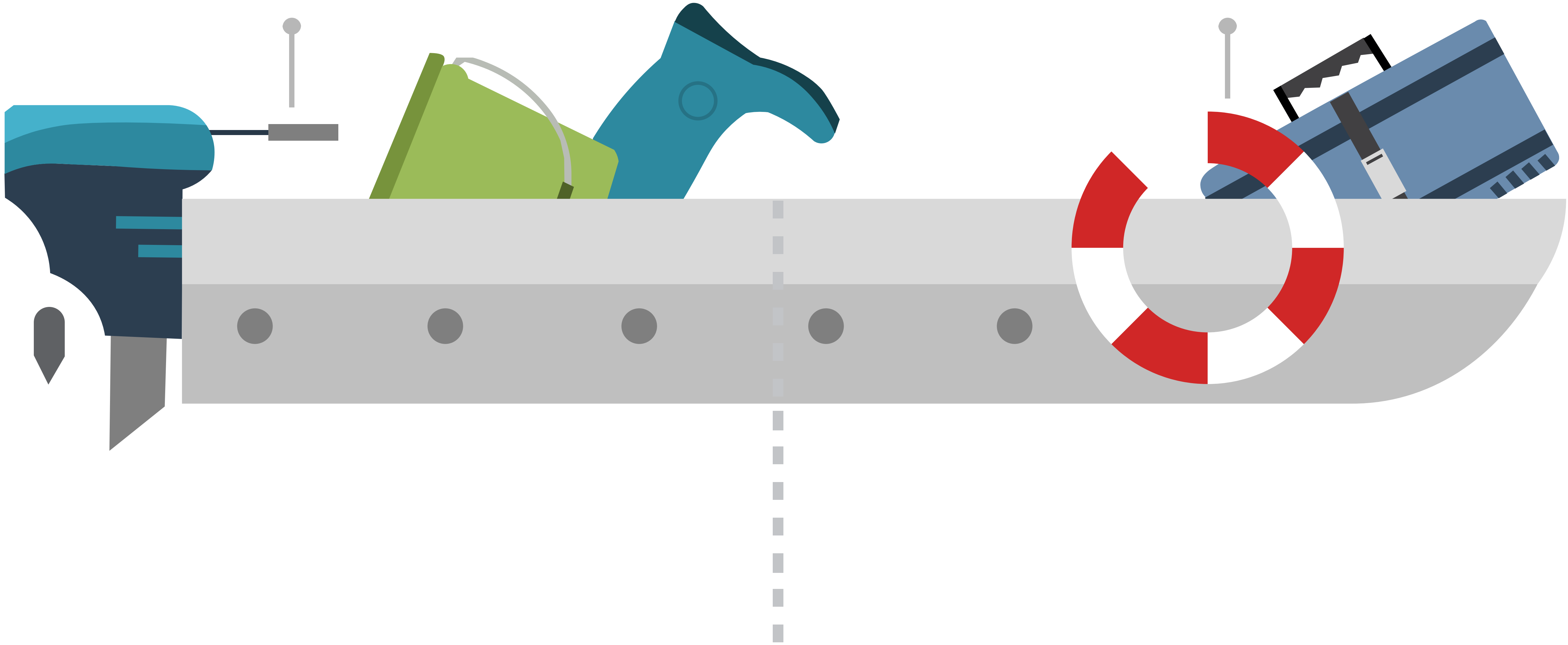
Navigating the complexities of AI usage and data governance in the workplace

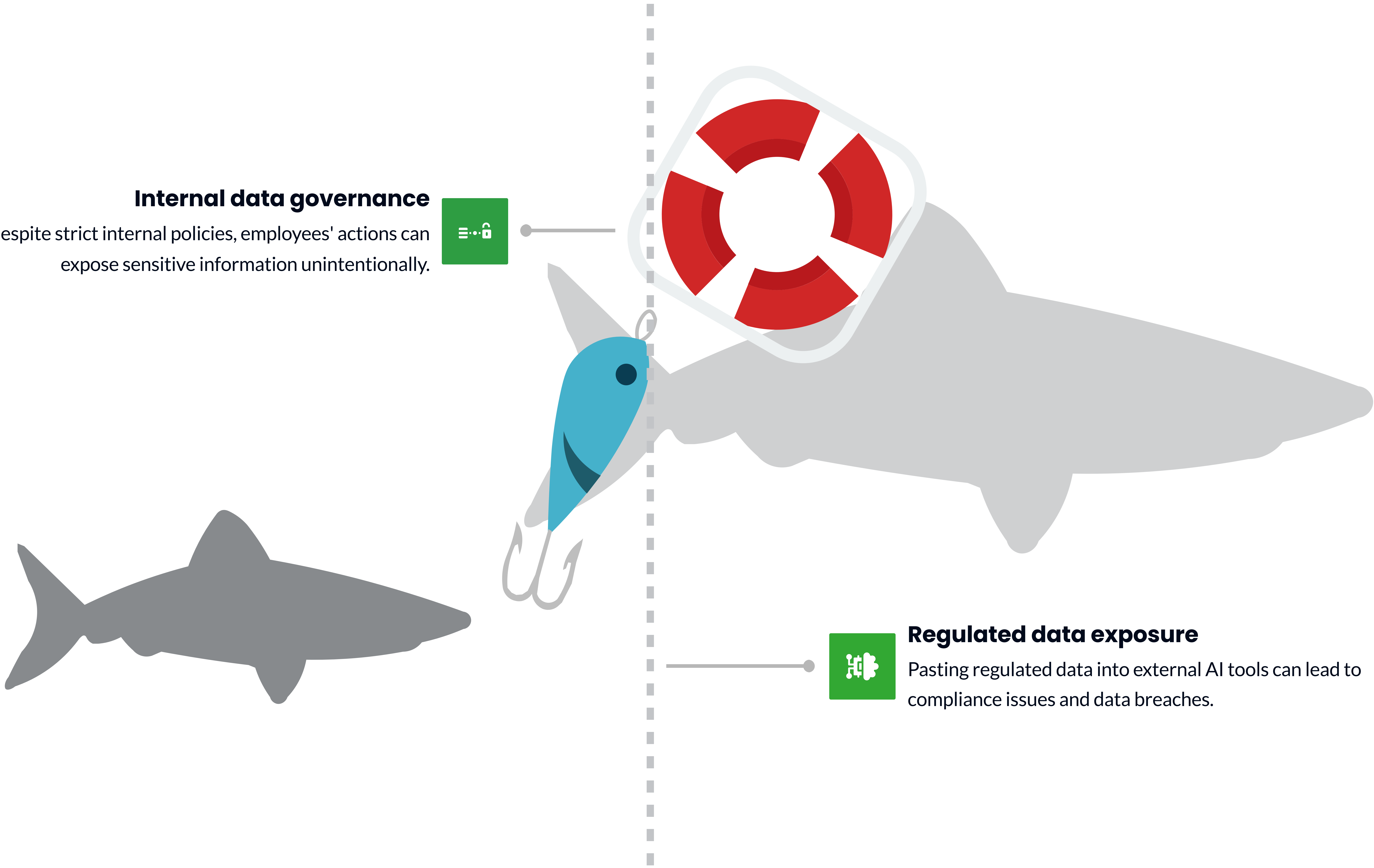
Employees often paste sensitive data into AI tools without realizing the associated risks.

Employee data handling

The adoption of AI tools like ChatGPT and Microsoft Copilot has surged among employees for task automation.

Rise of AI productivity tools





Internal data governance

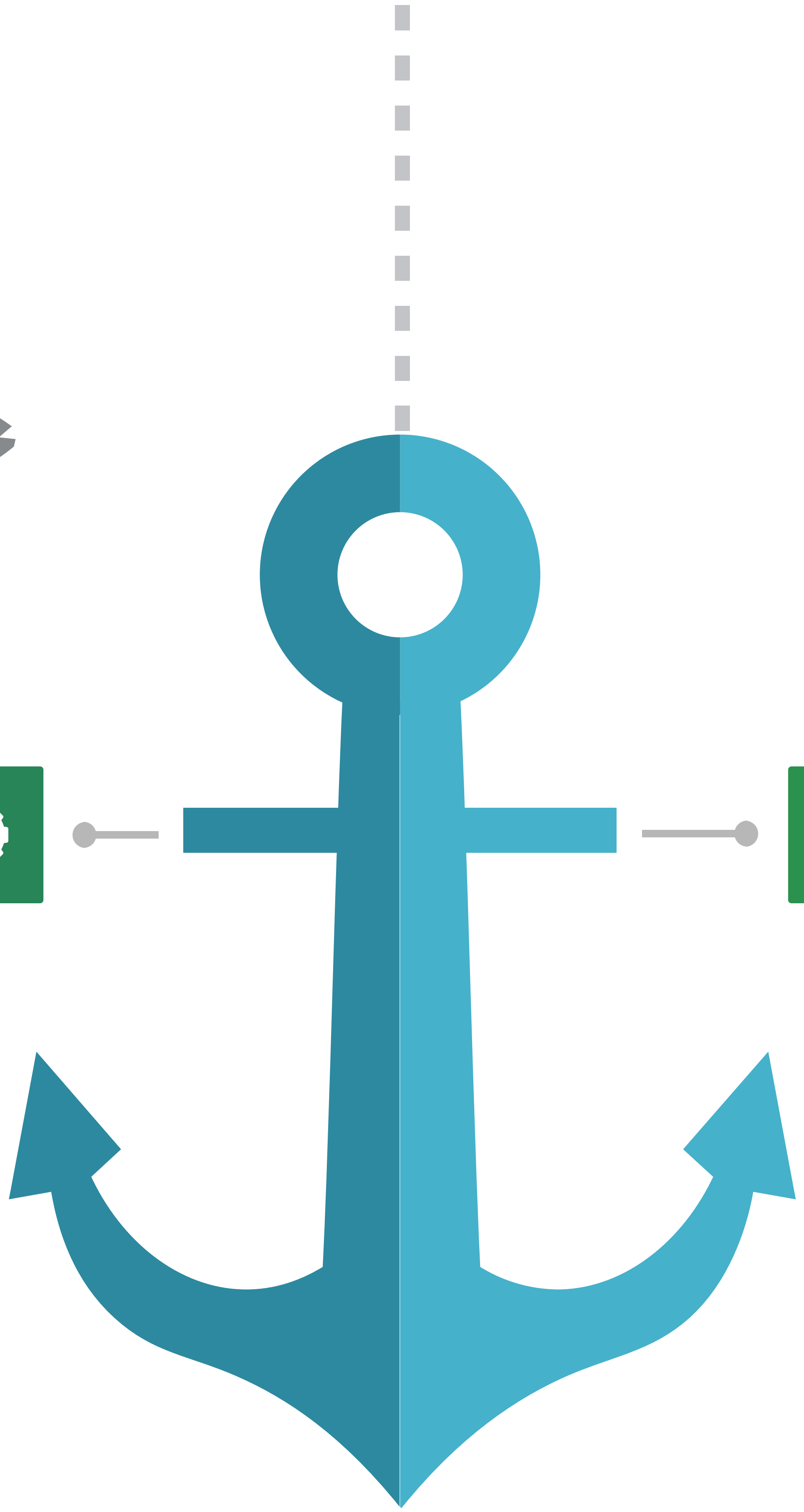
Despite strict internal policies, employees' actions can expose sensitive information unintentionally.

Regulated data exposure

Pasting regulated data into external AI tools can lead to compliance issues and data breaches.

Need for awareness and training

Organizations must educate employees about the risks to protect sensitive data while using AI tools.

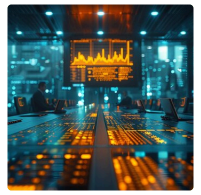


Hidden risks of AI tools

The convenience of AI tools masks significant hidden risks related to data security and privacy.

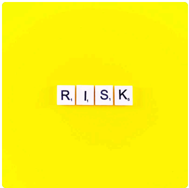
THE THREE-PHASE APPROACH OF IDEABOX FOR AI SAFETY

Safeguarding companies' data privacy while embracing AI through a structured process.



Phase 1: Discovery with Actifile

Utilized the **Actifile** agentless scanning engine to identify user interactions and potential data exposure risks.



Phase 2: Risk Quantification

Mapped incidents to an **AI Data Risk Score** to quantify exposure frequency, sensitive data types, and potential compliance costs.

Phase 3: Automated Prevention

Implemented **data-aware AI controls** including real-time encryption and shadow AI detection to enhance data security.

INSIGHTS FROM ACTIFILE'S DISCOVERY PHASE

Analyzing employee interaction with AI tools and data security risks

23%

+256.1

Significant AI tool usage by employees

A notable proportion of employees used AI tools recently.

11%

+245.8

Interactions with sensitive data

A concerning percentage of interactions involved classified data.

N/A

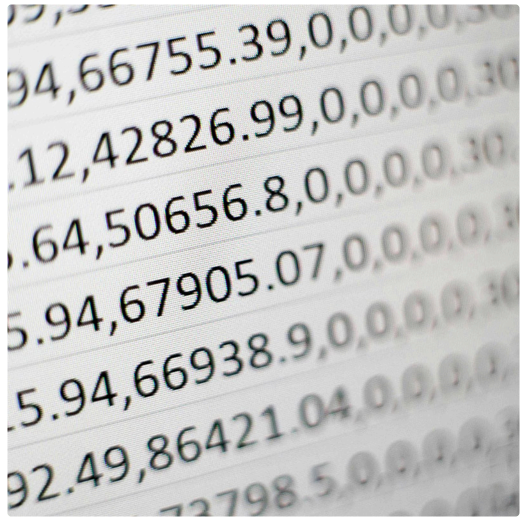
+286.1

Data security risk identified

Data from secure areas was improperly shared.

PHASE 2: INSIGHTS ON RISK QUANTIFICATION

Understanding data exposure, sensitive files, and compliance impacts



Frequency of data exposure

Insights on exposure rates per department/user.

Types and volume of sensitive files

Overview of files at risk.

Financial impact of compliance violations

Estimates for GDPR, HIPAA, DFARS risks.

Return on Mitigation (ROM)

Benefits of investing in AI governance and DLP controls.

ENHANCING SECURITY WITH AUTOMATED PREVENTION TECHNIQUES

Leveraging Actifile for Real-Time Data Protection and AI Tool Monitoring

1 Real-time encryption

Utilizes **real-time encryption** of sensitive data to prevent unauthorized uploads to LLMs, ensuring data integrity.

2 Shadow AI detection

Implements **shadow AI detection** to alert IT departments when unauthorized AI tools are in use, enhancing security protocols.

3 End-user guidance

Provides **end-user guidance** to flag risky behaviors, allowing users to maintain productivity while adhering to security measures.

4 Data protection focus

Focuses on protecting sensitive data through proactive measures, minimizing risks associated with AI tool usage.

5 Proactive security measures

Establishes a framework of **proactive security measures** that align with company policies to safeguard against data breaches.

★★★★☆

"WE DIDN'T KNOW HOW FAST AI TOOLS WERE INFILTRATING THE WAY WE WORK—UNTIL IDEABOX SHOWED US THE BLIND SPOTS. NOW WE CAN ADOPT AI WITH CONFIDENCE."

CIO

Financial Institution

MITIGATING RISKS IN AI USAGE WITH IDEABOX

Harnessing AI tools safely while protecting organizational data

- **Identify risky AI use.**

  Recognize and highlight instances of potential misuse of AI technologies within the organization to mitigate risks.

- **Quantify potential data exposure.**

  Measure and evaluate the extent of data that may be exposed due to unsafe AI practices, informing better decisions.

- **Enforce smart, real-time protections.**

  Implement adaptive security measures that respond instantly to threats, ensuring data integrity and compliance.

- **Boost productivity with AI.**

  Utilize AI capabilities to enhance organizational efficiency while maintaining a strong security posture.

- **Minimally invasive security solutions.**

  Adopt security measures that do not hinder productivity, allowing teams to work efficiently without interruptions.

- **Empower organizations with data control.**

  Enable firms to maintain authority over their data, ensuring it is used responsibly and securely across AI applications.

IMPACT OF IDEABOX ON DATA SECURITY METRICS

Comparative analysis of metrics before and after implementing ideaBOX

Metric	Before ideaBOX	After ideaBOX
LLM sessions w/ sensitive data	98 in 30 days	3 in 30 days
Risk-weighted data exposure	$4.2M	<$50K
Awareness of AI data risks	Low	High, with actionable dashboards
Productivity impact	Neutral	Neutral – no workflow disruption

CONNECT WITH IDEABOX TODAY TO TRANSFORM YOUR AI STRATEGY

Explore the potential of a partnership with ideaBOX to establish comprehensive AI usage governance. This initiative will safeguard sensitive data while maximizing the advantages of AI tools in your organization.

For more information
Contact US:
Main: 914.222.1995
Email: info@ideaBOX.com