MODERNIZING PROJECT MANAGEMENT SERVICES

MAXIMIZING THE AI JOURNEY THROUGH AUTOMATION AND SECURITY

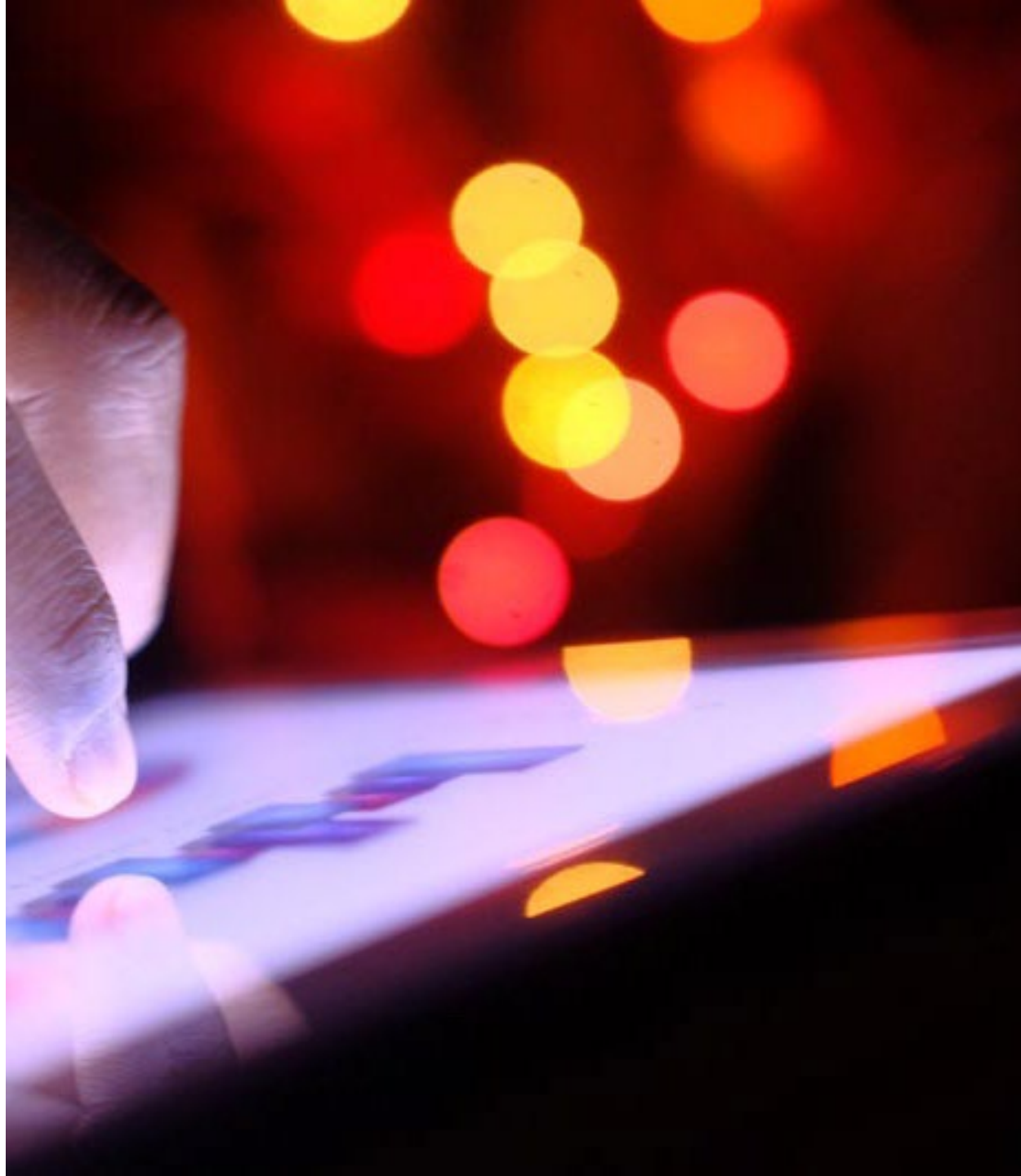
Today’s Agenda

Topics
Value of AI
Securing AI
Q&A

AI to ROI

JASON CIGAN

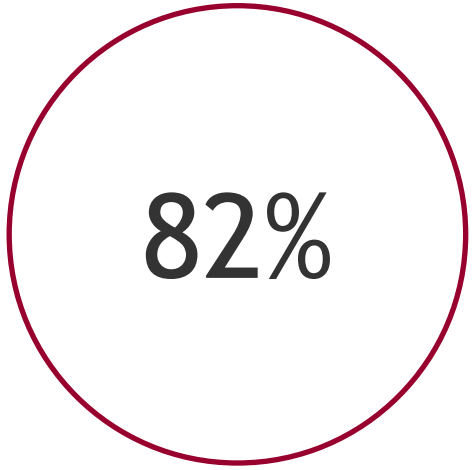
Partner, Technology Consulting
Modern Workplace, BDO Canada



2025 Microsoft Modern Work Trend Index Report

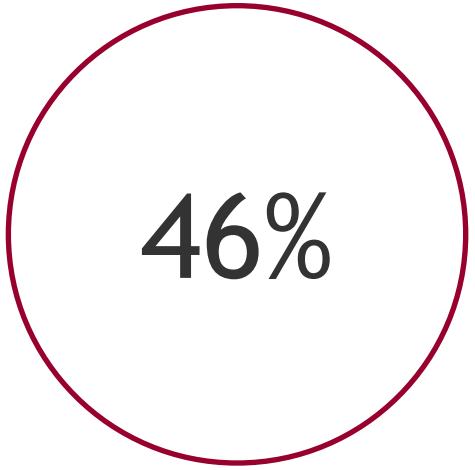
Intelligence on tap will rewire business. Every leader needs a new blueprint.

You can buy intelligence on tap



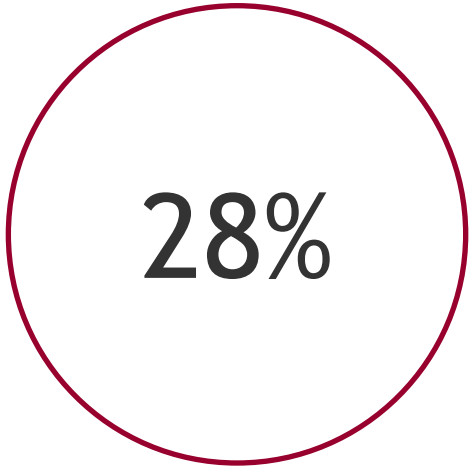
of leaders say they're confident that they'll use digital labor to expand workforce capacity in the next 12–18 months.

Human-Agents teams will upend the org chart



of leaders say their companies are using agents to fully automate workflows or processes

Every employee is an agent boss



of managers are considering hiring AI workforce managers to lead hybrid teams of people and agents

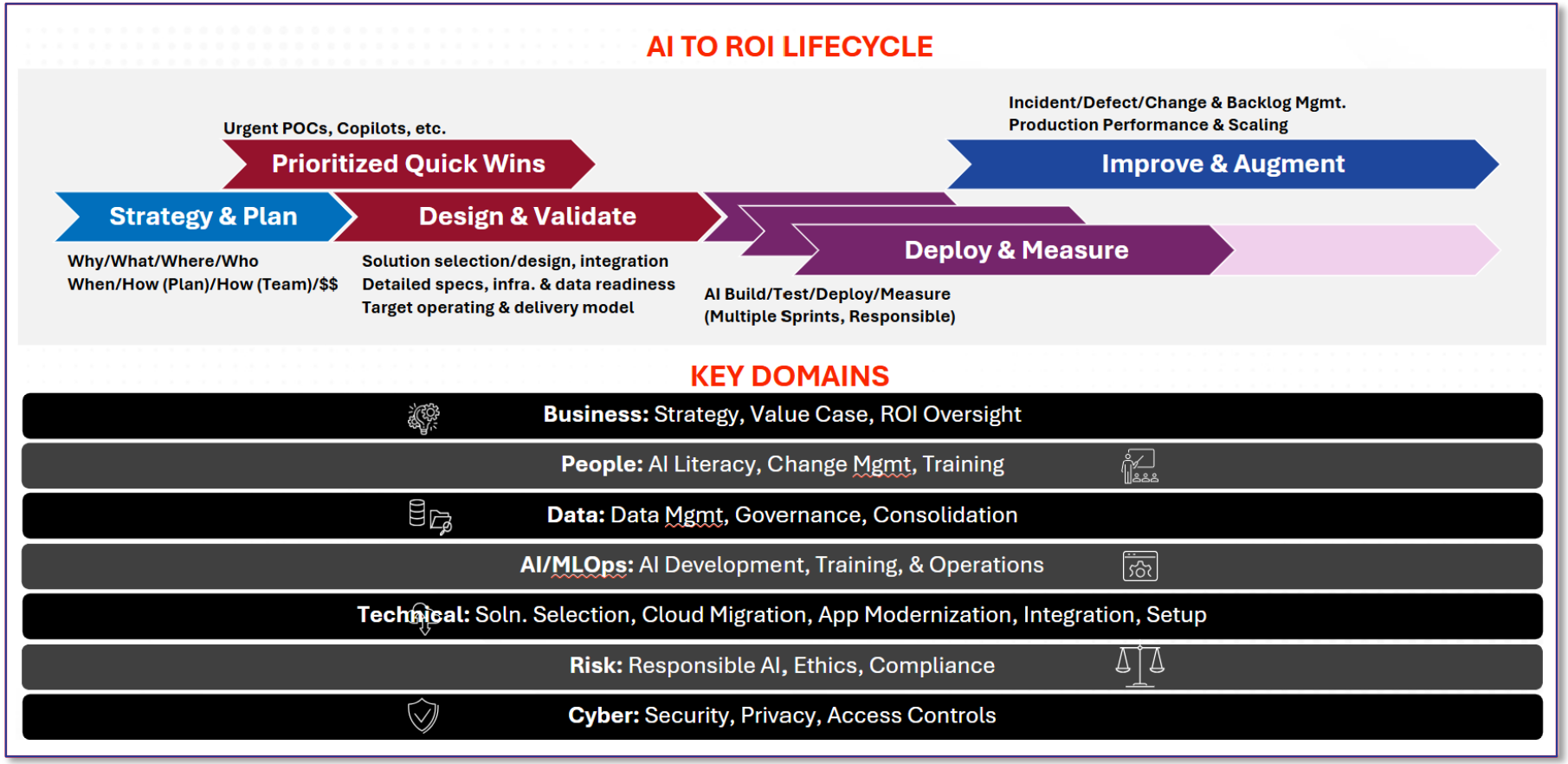
From global enterprises to small businesses, AI is the engine for scale.

2025 Microsoft Modern Work Trend Index Report

BDO's "AI to ROI" transformation methodology

Providing a holistic approach to enable a practical, business-first enablement of AI aligned to organizational objectives.

BDO'S PRACTICAL "AI TO ROI" METHODOLOGY



BUSINESS VALUE

- **Practical and trusted AI advice** to help guide from start to finish
- **Clarity and alignment** on why/what/where/who/when/how/$$ for data, automation and AI objectives
- **Establishment of target operating & delivery model to** drive AI related impact, at scale (e.g., factory model)
- **MS Partner of the Year recognition,** for our capabilities, brand, innovation
- **Factors in BDO's responsible AI framework** for ethics, governance and risk-mgmt.
- **Access to BDO's deep capabilities** in Data, Cloud, AI, Cyber, Risk, etc. for feasible solutions & delivery
- **Embedded change management** to ensure staff literacy and adoption

Unlocking Productivity

Optimize value at every phase of AI adoption

Agent Intelligence

Level 100

AI ASSISTED

Empower your teams to collaborate with AI tools to assist their workflows

Level 200

AI POWERED

Offload parts of end user and development workflows to AI bots that can independently deliver on repeatable tasks

Level 300

AI AUTONOMY

Leverage AI agents to independently complete end to end development workflows that are reviewed and validated by humans

- Setting your AI strategy
- Upskill users & track adoption
- Performance reporting & optimization
- AI use case ideation
- Workflow reimagination with AI
- AI agent design & implementation
- Tool iteration & improvement

M365 Copilot, Chat | Graph, | Fabric | SharePoint | Bing |

Copilot Studio agents

Azure AI Foundry, I Agents Services, |API Plugins

Semantic Kernel

BDO AI ACCELERATORS

Copilot Care+

Deploy Copilot, accelerate adoption through change management, and track ROI and adoption statistics

BOOST

Enable a secure AI interface to create persona-based bots fine-tuned for long form documents

Microsoft Copilot Studio Enablement

Enable task-based Copilot Studio agents connected to data stored in your MSFT environment

AutoDev

AI Agents that plan and independently undertake activities in an agile manner to support legacy code and app modernization efforts

What is Microsoft Copilot?

An AI-powered assistant integrated into the apps that you use every day, working alongside you to unleash your creativity and help you perform tasks faster.

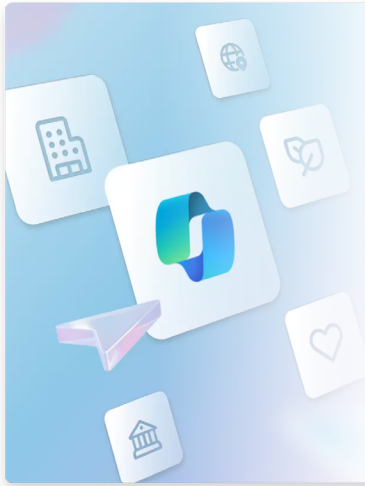
New agents in Microsoft 365

Microsoft

COPILOT CARE +

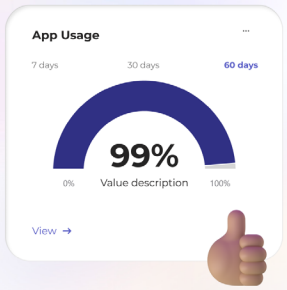
No matter where you are in your Copilot journey, BDO has the support you need

AI Strategy + Advisory

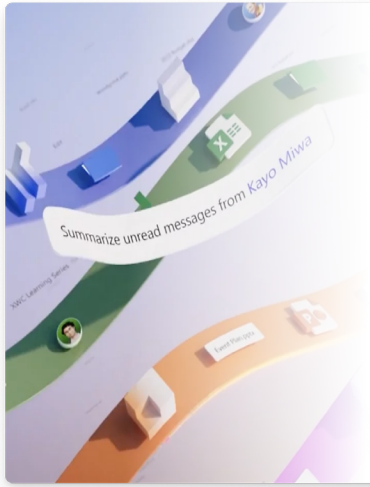


Get Started with Copilot POC

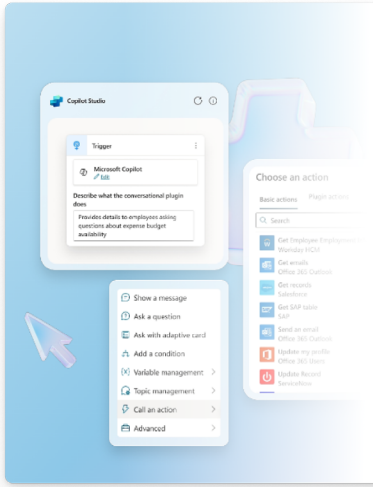
Data Security + Privacy



Adoption + Change Management



Care+ Support



Expand + Elevate

Due to the evolving nature of Microsoft 365 Copilot, offerings are subject to change.

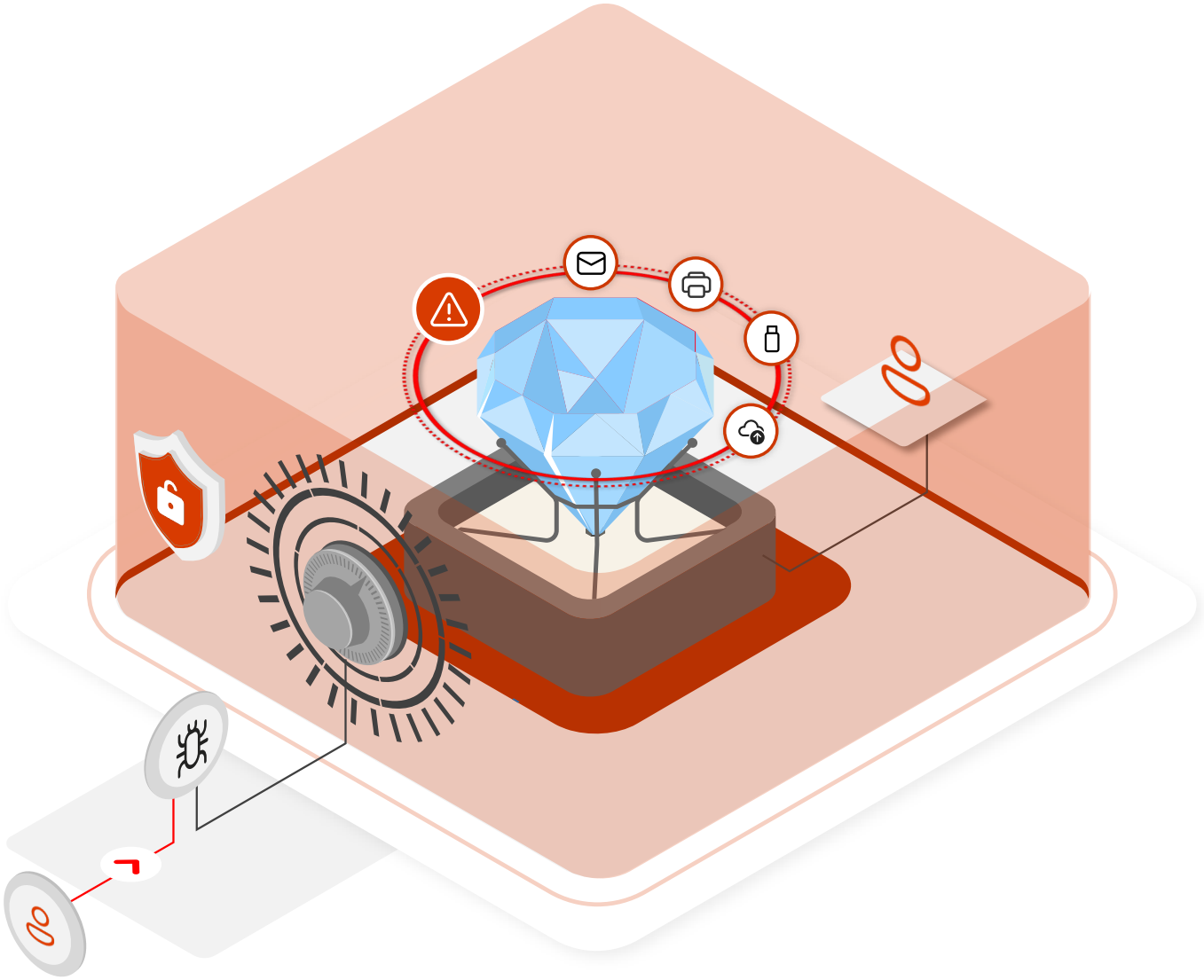
SECURING AI

KARAN PREET SINGH

Sr. Consultant – Cybersecurity,
BDO Canada

Data Security Challenges

- **Discover sensitive data**, whether structured or unstructured, on-premises or in the clouds
- **Secure configuration** to prevent sophisticated attacks
- Detect how users are interacting with data and **identify insider risks**
- Ensure your data remains **secure** from **data leakage** and **data exfiltration** activities

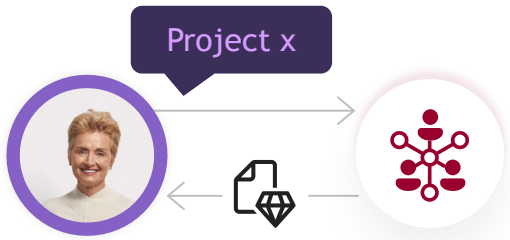


Security concerns associated with AI usage

Insufficient visibility into the usage of AI applications can result in security and compliance challenges.

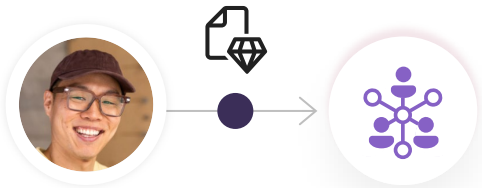
1

Data oversharing:
Users may access sensitive data via AI apps they're not authorized to view or edit



2

Data leak:
Users may inadvertently leak sensitive data to AI apps



3

Non-compliance usage:
Users use AI apps to generate unethical or other high-risk content

Securing AI with Data Protection

Safeguarding AI systems and data through comprehensive security measures to mitigate risks and ensure responsible AI adoption.

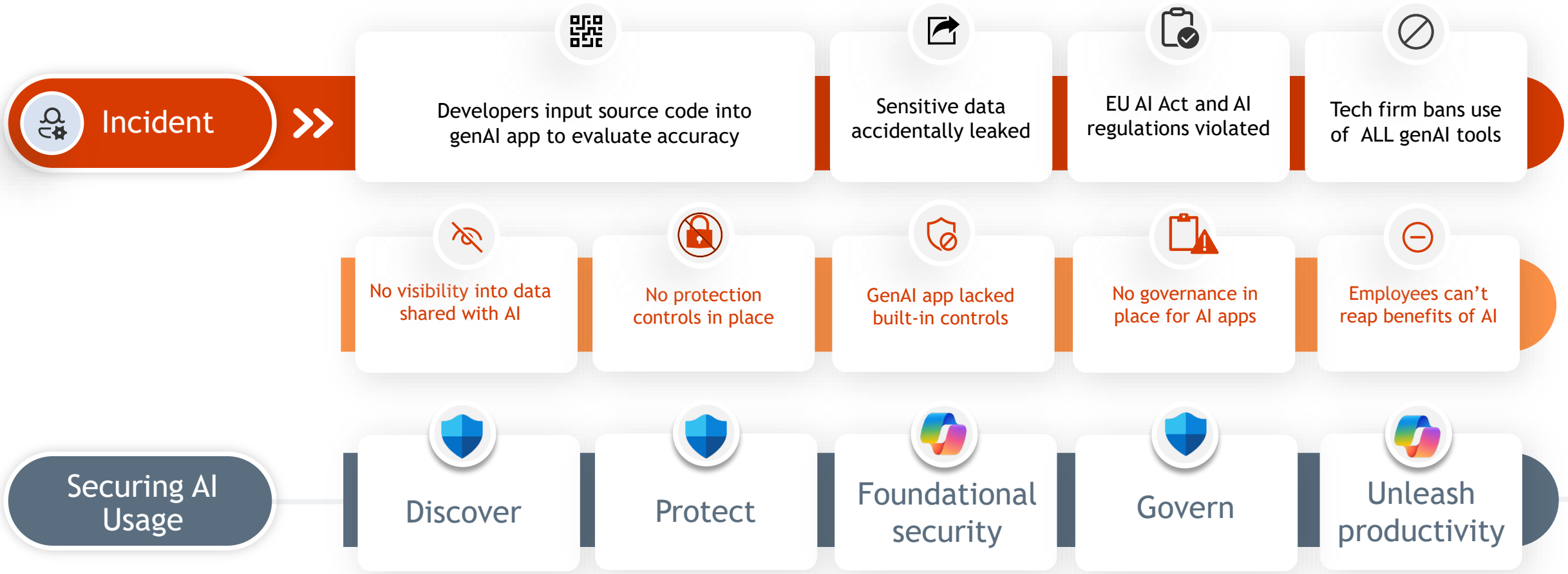
Challenge	❑ **Data Privacy and Exposure** – Significant risk of sensitive data being exposed by AI models and/or user prompts.	❑ **Unauthorized Access** – Risk of users gaining more system access than they should have, leading to insiders releasing sensitive data to AI applications potentially leading to data breaches/reputational damage.	❑ **Data Exfiltration** – AI applications may access and expose sensitive data to third parties due to improper data security policies, leading to potential data compromises.	❑ **Evolution Outpacing Regulations** – AI technology is advancing faster than regulatory framework can adapt, making it difficult to implement appropriate data retention and secure data disposal solutions while maintaining performance.
Solution	+ **Data Discovery** – Assess data quality, facilitate data clean-up, enforce least privilege access controls, and provide training.	+ **Data Access Control** – Review access controls, manage identities, and identify high-risk users and systems.	+ **Data Security** – Classify and protect data, implement data loss prevention measures.	+ **Risk and Compliance** – Manage the data lifecycle (discovery, retention and disposal) to meet regulatory requirements.

Approach

Outcomes

- **Balance Innovation and Security**
- **Strengthened Cybersecurity Posture**
- **Improved AI System Reliability**

Use Case - Engineers accidently leak data in AI app



Need a solution that inherits your security, compliance and privacy controls

How to secure and govern AI – Levels of Maturity

Maturity-1 (Basic)

Multi-factor Authentication

Basic Access Control / Role Based Access Management (RBAC)

Logging and Monitoring

Maturity-2 (Core)

Including maturity-1 controls

IAM foundation

Manual sensitivity labels

Data loss prevention controls

Advanced SharePoint sitewide access controls and reporting

Unified endpoint management

Maturity-3 (Advanced)

Including maturity-1 and 2 controls

IAM enhanced

Automatically apply sensitivity labels

Automatically remove inactive and stale content

Prevent data leak on endpoint devices

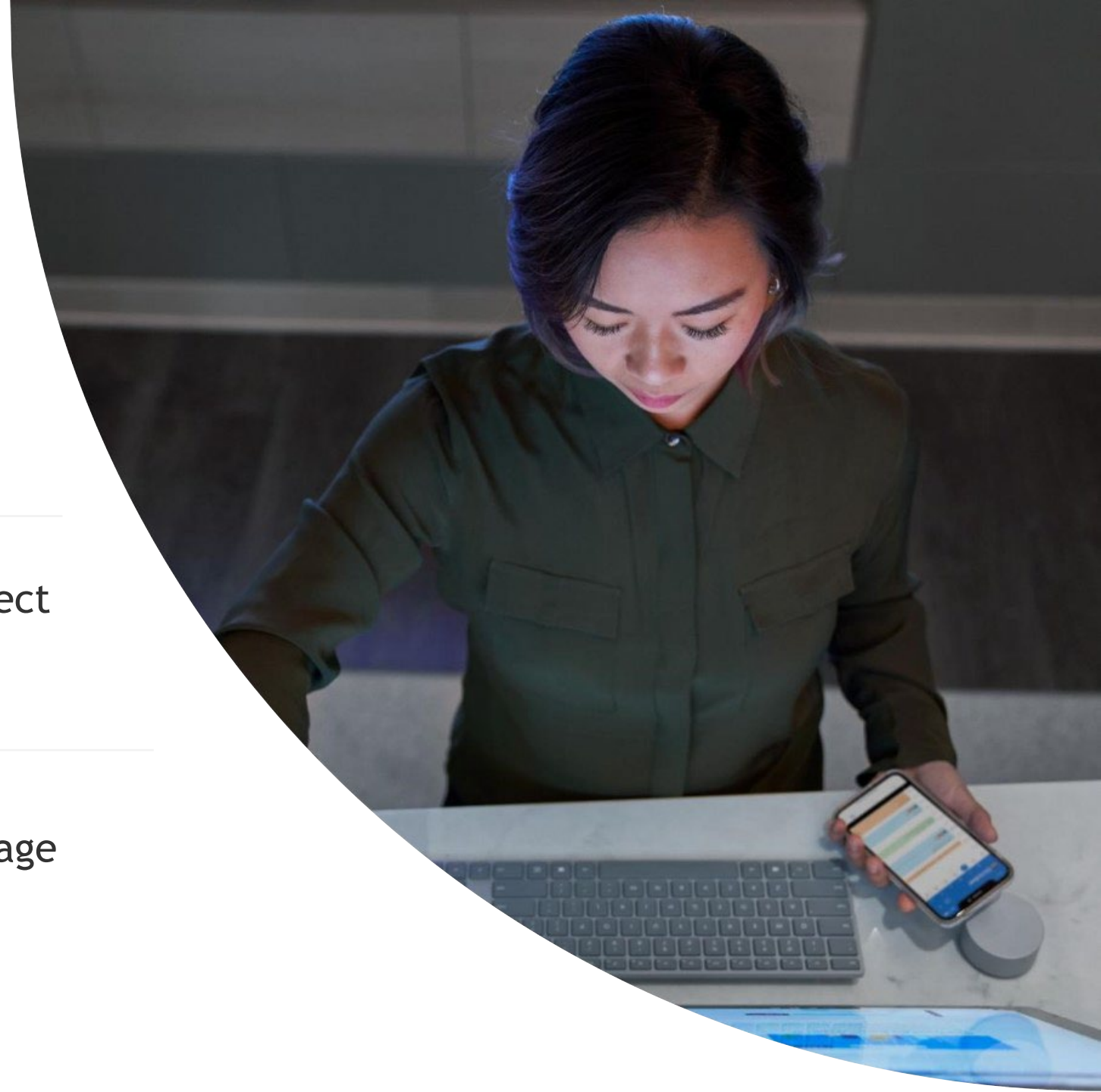
Detect non-compliant usage

Let’s hear from you

Does your organization know the types of sensitive information it has and where it lives?

How does your organization protect sensitive data across your environments?

How does your organization manage insider risks today?



DISCUSSION