

From Zero to Hero: How Artificial Intelligence can Supercharge Your Growth



Moderated by James Spignardo,
Strategic Solutions Consultant

MEET OUR PRESENTERS



Ben Wilcox

Chief Technology Officer



Andrew Rochfort-Hyde

Head of Delivery:
App Dev, Data & AI



Michael Montagliano

Chief Information
Security Officer

Agenda

- Quick AI Intro
- 5 Questions
- Live Q&A



Poll!

Where are you in your AI journey?

What is AI and how is the
situation today different?

Foundation Models

Large amount
of unlabeled
data

Transfer
Algorithm



Large Language Models (LLMs)

Large amount of
unlabeled **text-
based** data

Transfer
Algorithm



Generative AI - Generative AI refers to AI techniques that learn a representation of artifacts from data and models, and use it to generate brand-new, completely original artifacts that preserve a likeness to original data or models.

Foundation model - A foundation model is a large machine learning model trained on a very large amount of unlabeled data using a transformer algorithm; this training, augmented by a range of fine-tuning (adapter) mechanisms, results in a model that can be adapted to a wide range of applications.

Large Language Model (LLM) – an LLM is a type of foundation model specifically focused on natural language.

ChatGPT is a conversational **application** built on top of an LLM (in this case OpenAI's GPT model).

Foundation Models

Benefits

Versatility

Accessibility

Ecosystem

Potential for Lower Cost of Entry

Domain Adaptation

Risks

Domain Adaptation

Copyright Issues

Concentration of Power

Hallucination

Potential for Misuse

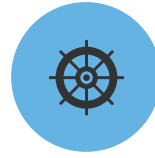
Opaque

Fundamentals of Generative AI



Data Driven

Output based on
what it has learned



Prompts

Prompts are the driving
force behind the output.



Creative Potential

Novel and "Original"
Content

What are some commonly used
AI tools and misconceptions
surrounding them?

Generative AI App Landscape

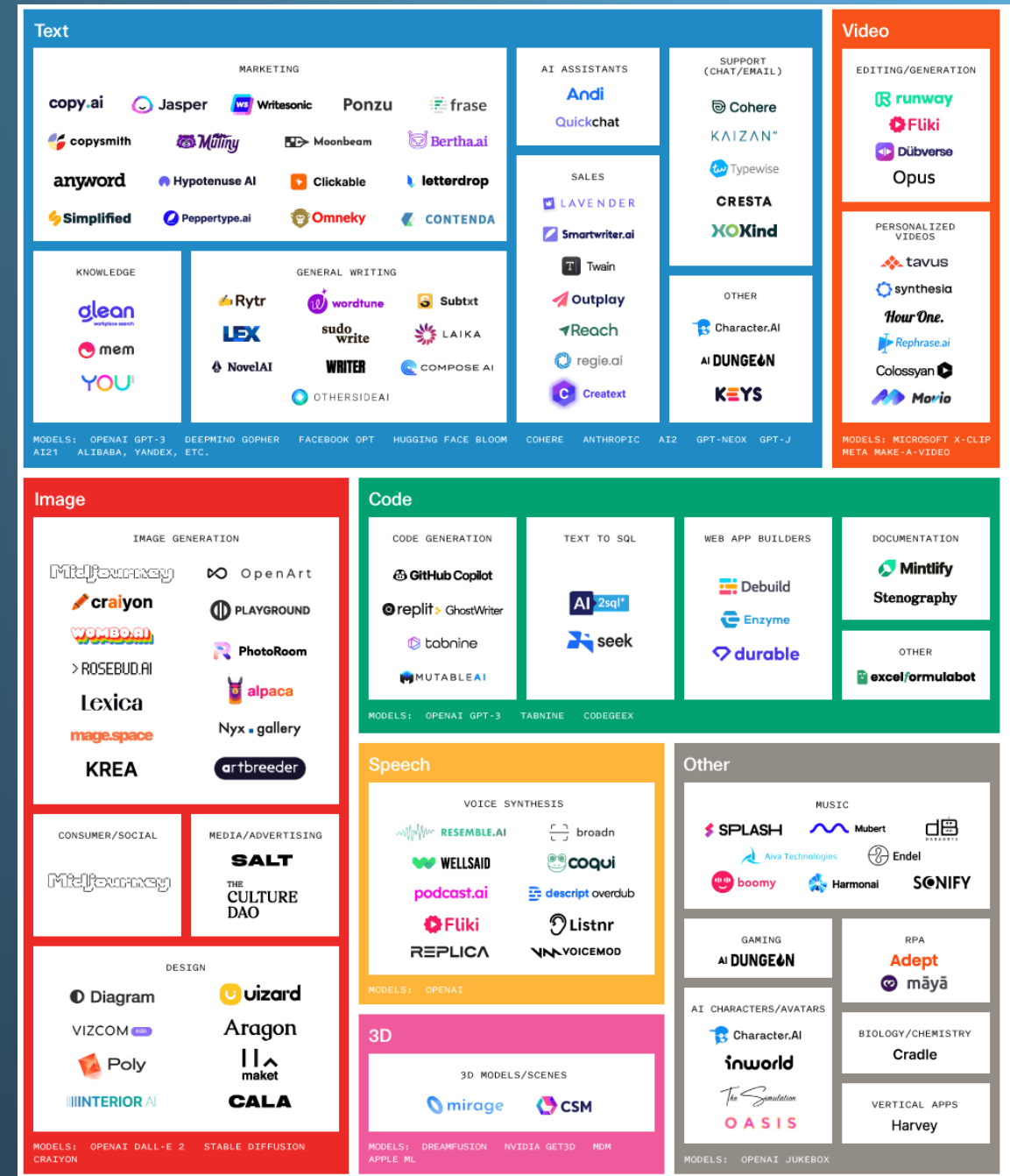
Areas for Application

- Information Technology
- Marketing and Sales
- Customer Service
- Product Development

2026

By 2026, over 100 million humans will engage robocolleagues (synthetic virtual colleagues) to contribute to enterprise work.

Gartner: Frances Karamouzis



Common Misconceptions

AI can replace all human tasks

AI is infallible

AI understands context like humans do

AI is completely objective and safe

AI is more creative

AI is only for large enterprises



How can *AI be* leveraged?

AI Uses Today & Near Future

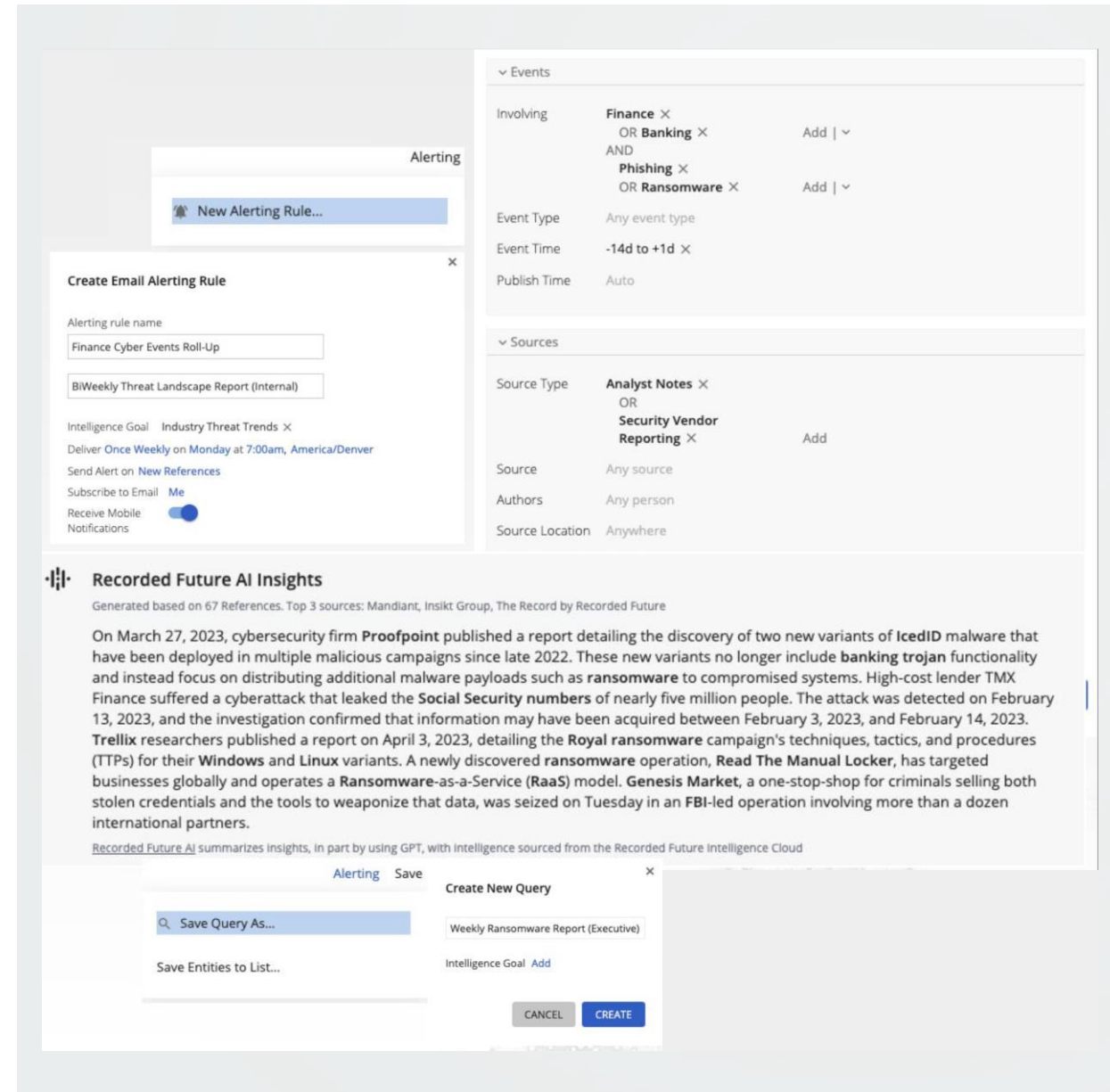
- Unstructured Data Analysis
- Engagement in Communications
- Ideation
- Personalized Explanations

Threat Intelligence AI Insights

Recorded Future uses AI Insights to quickly summarize their massive raw intelligence.

AI insights enable their clients to:

- Process and take action on alerts faster
- Reduce risk



The screenshot displays the Recorded Future interface, featuring a sidebar with 'Alerting' and 'New Alerting Rule...' options. The main content area is divided into two panels. The left panel, titled 'Create Email Alerting Rule', includes fields for 'Alerting rule name' (Finance Cyber Events Roll-Up), 'Intelligence Goal' (Industry Threat Trends), and 'Send Alert on' (New References). It also has a 'Subscribe to Email' toggle set to 'Me' and a 'Receive Mobile Notifications' toggle set to 'On'. The right panel, titled 'Events', shows filters for 'Involving' (Finance, Banking, Phishing, Ransomware) and 'Event Type' (Any event type). Below this, the 'Sources' panel shows filters for 'Source Type' (Analyst Notes, Security Vendor Reporting) and 'Source' (Any source). The bottom section, titled 'Recorded Future AI Insights', provides a summary of intelligence based on 67 references, highlighting recent reports on IcedID malware variants and the Royal ransomware campaign. A 'Create New Query' dialog box is open at the bottom, showing a search for 'Weekly Ransomware Report (Executive)' and a 'Save Query As...' button.

Recorded Future AI Insights

Generated based on 67 References. Top 3 sources: Mandiant, Insikt Group, The Record by Recorded Future

On March 27, 2023, cybersecurity firm **Proofpoint** published a report detailing the discovery of two new variants of **IcedID** malware that have been deployed in multiple malicious campaigns since late 2022. These new variants no longer include **banking trojan** functionality and instead focus on distributing additional malware payloads such as **ransomware** to compromised systems. High-cost lender **TMX Finance** suffered a cyberattack that leaked the **Social Security numbers** of nearly five million people. The attack was detected on February 13, 2023, and the investigation confirmed that information may have been acquired between February 3, 2023, and February 14, 2023. **Trellix** researchers published a report on April 3, 2023, detailing the **Royal ransomware** campaign's techniques, tactics, and procedures (TTPs) for their **Windows** and **Linux** variants. A newly discovered ransomware operation, **Read The Manual Locker**, has targeted businesses globally and operates a **Ransomware-as-a-Service (RaaS)** model. **Genesis Market**, a one-stop-shop for criminals selling both stolen credentials and the tools to weaponize that data, was seized on Tuesday in an FBI-led operation involving more than a dozen international partners.

[Recorded Future AI](#) summarizes insights, in part by using GPT, with intelligence sourced from the Recorded Future Intelligence Cloud

Alerting Save

Save Query As...

Save Entities to List...

Create New Query

Weekly Ransomware Report (Executive)

Intelligence Goal Add

CANCEL CREATE

What are the regulatory
implications and cyber risks?

Identify and Assess the Risks Associated With the Technology

LLMs are open-access platforms

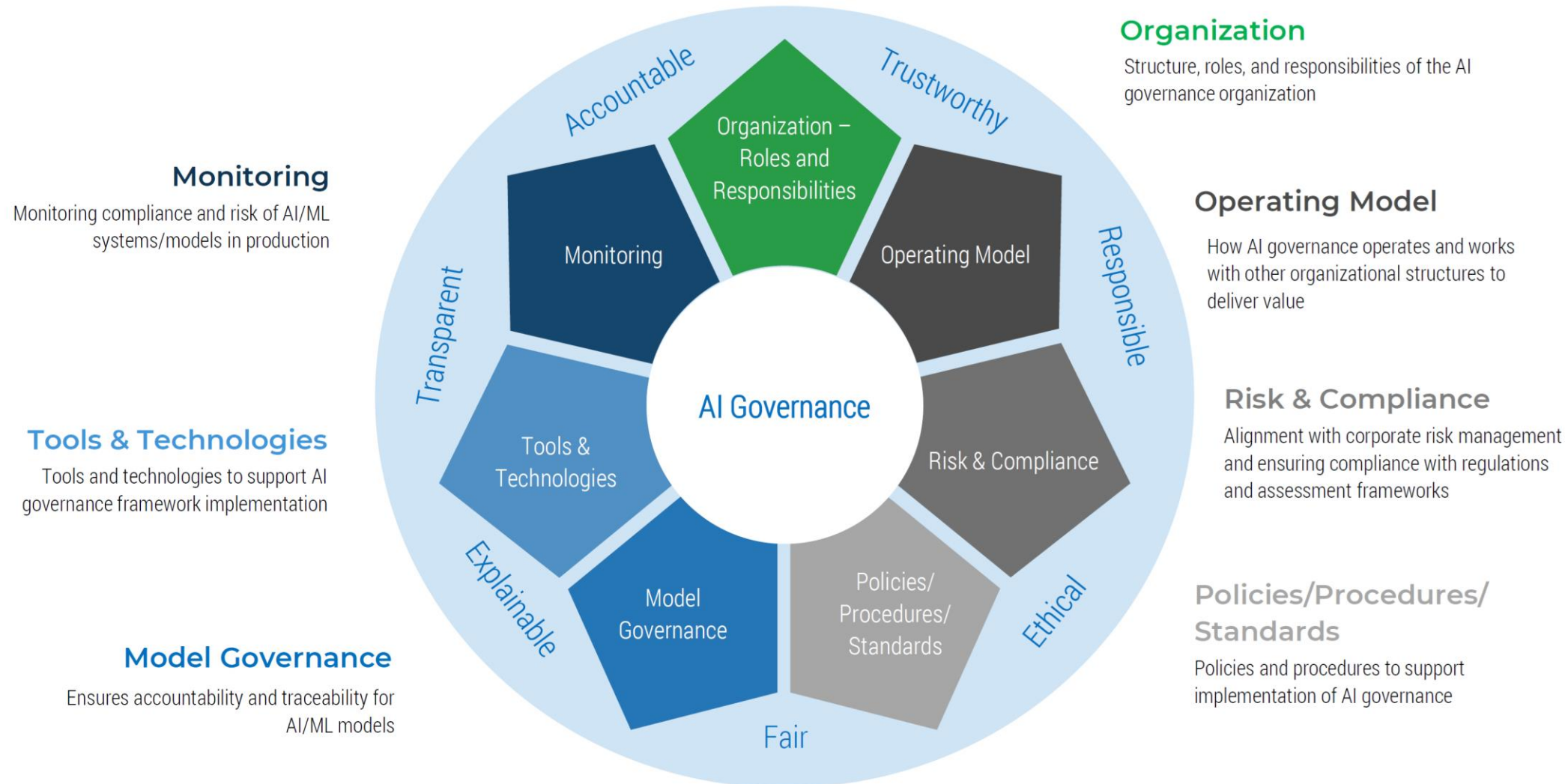
Risks come from:

- bad actors outside of the organization
- inside the organization in both governed and ungoverned ways.

Risks Associated with Generative AI (Chat GPT)

Vector	Risk Type
Use by actors outside the organization	<ul style="list-style-type: none">• Cybersecurity Risk• Reputational Risk
Ungoverned use by employees (AlaaS)	<ul style="list-style-type: none">• Information Security Risk• Privacy Risk
Unintended consequences of enterprise use	<ul style="list-style-type: none">• Reputational Risk• Legal and Regulatory Risk

AI Governance Framework



Poll!

Are you familiar with Microsoft
Copilot?

What are the first steps
for an organization to
embark on their AI journey?

Start with Assessing

- **Define Objectives:** Understand what problems you aim to solve with AI. Experiment in uses
- **Assess AI Readiness:** Evaluate technical infrastructure, data availability, and necessary skill sets.
- **Educate and Train Your Team:** Ensure your team understands AI and its implications.
- **Choose the Right Problems to Solve:** Identify problems that are well-suited to AI solutions.

How should organizations prepare for the addition of generative AI?

Knowledge Management

Current use of knowledge assets is inefficient

Workers struggle to find data, leading to faulty business decisions

Generative AI can help optimize the use of content and data to add value

Requires a reassessment of knowledge management strategies

Skills and Adoption

Non-IT employees need to understand and acquire skills in generative AI

Rapid changes expected in content-related job responsibilities due to AI

Employee attitudes toward AI vary

Resistance poses a challenge to the widespread adoption

Work Routines

Significant impact of work routine anticipated

Many simple processes are expected to use AI within 3 years

Successful integration of AI requires giving employees the right context for its use

Now, less than 40% of employees feel informed about how their roles and skills will change due to AI

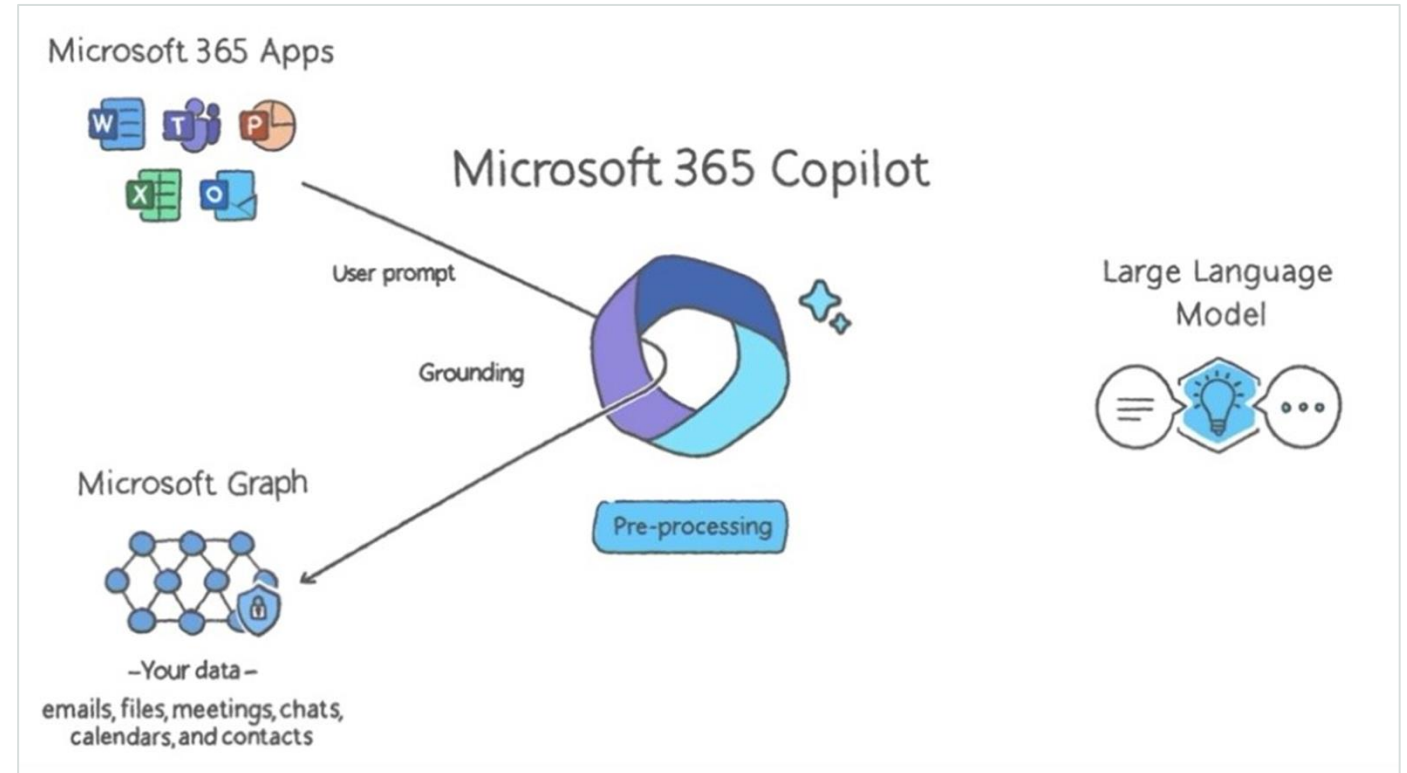
Copilot System Explained

The user's prompt is first preprocessed by Copilot, then grounded via Microsoft Knowledge graph to get more context.

This context is then included in the original prompt, which is now the "Modified Prompt".

The output produced by the LLM is sent back through Copilot, resulting in further grounding via the knowledge graph.

Then security checks, content checks, "responsible AI checks", and compliance/privacy checks occur, and then finally, command generation.



What to do about Microsoft Copilot for Microsoft 365

First Steps

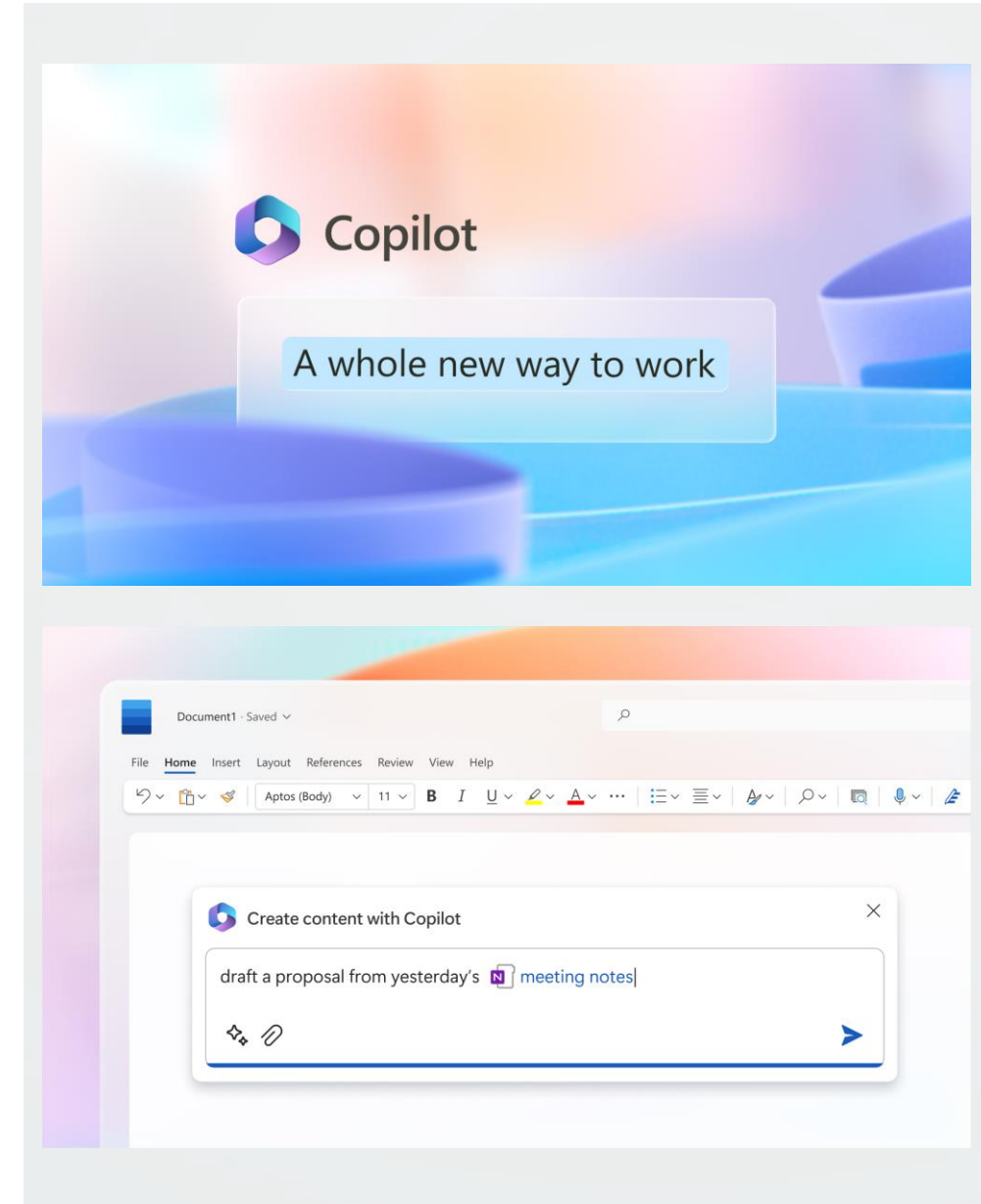
- Assign a resource to lead the organization's response to Copilot.
- Prepare talking points for key figures in the organization about Copilot issues.
- Form a governance committee of key figures for more education, decision-making, and policy setting.

Interim Steps

- Use governance committee decisions to establish technical controls and initial guidelines for employees, outlining expectations, opportunities, challenges, and rules of engagement.
- Form a community of interest for employees and talking points for network influencers.
- Identify a range of use cases, from low-risk/high-reward scenarios to "no-fly zones."

Steps Before Deployment

- Implement an acceptable use policy across all generative AI.
- Determine criteria that all generative AI instances must meet before deployment.
- Assign operational ownership of Copilot and specific tasks to team members.
- Ensure M365 tenant controls align with acceptable use, data privacy, and security policies.
- Develop knowledgebase articles for IT Service Desk use.
- Finalize initial communication and guidance for early stages of deployment.



Cont...

Steps Before Deployment Cont.

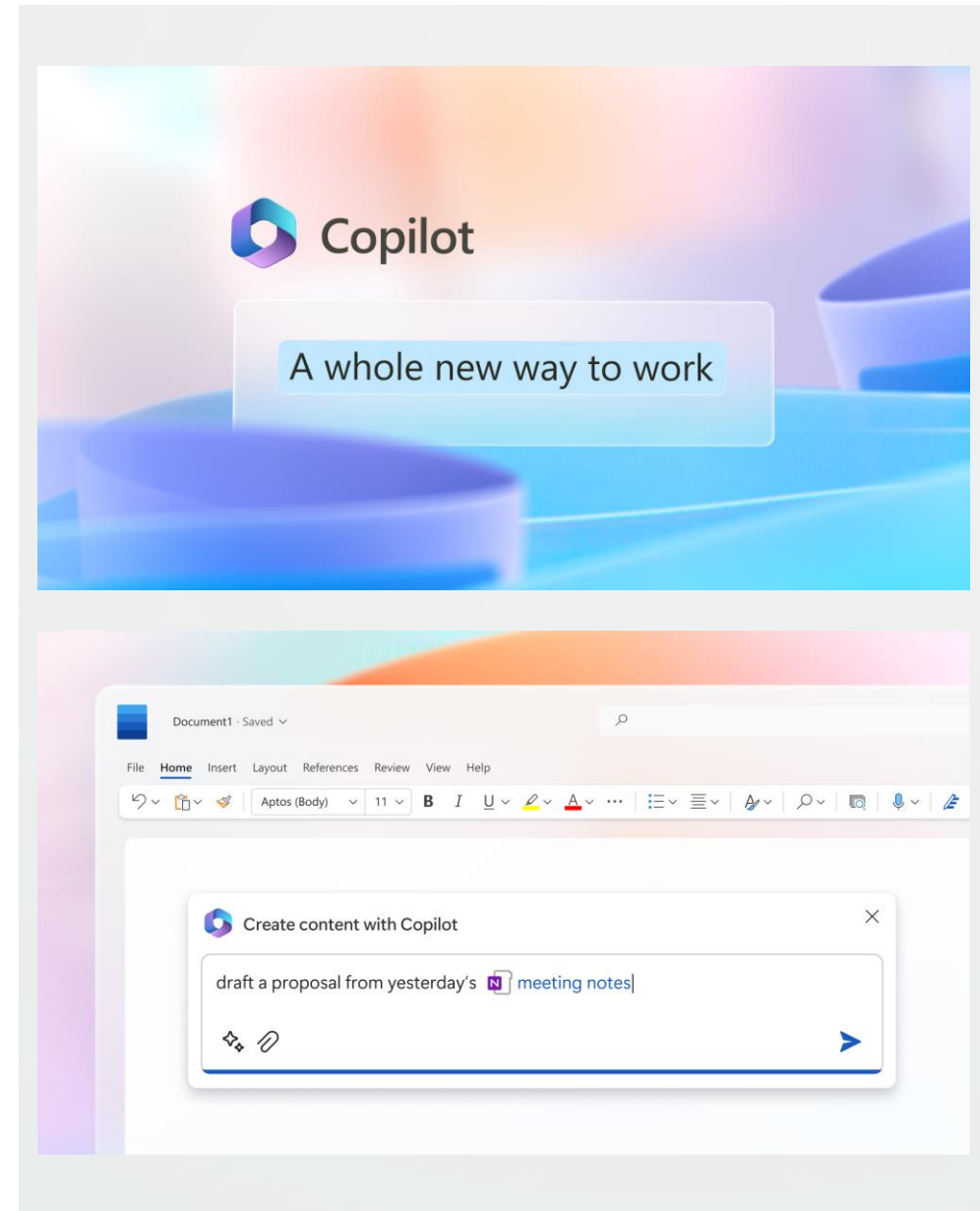
- Select where initial (beta/early adopter) deployment will occur.
- Prepare how to handle business units demanding early access.
- Develop success metrics and reporting and feedback mechanisms.
- Create 'use when' and 'don't use when' scenarios
- With HR, establish guidance for managers about the potential impact on team members
- Communicate to unit leaders the benefits and challenges
- Evaluate and select a Microsoft SKU and understand the full effort

Steps upon Deployment

- Track authorized use cases, collect wins and fails
- Use the feedback to broaden the deployment
- Convert the Copilot community of interest to a community of practice
- Assist HR in carefully tracking how roles and responsibilities are changing
- With HR minimizes change fatigue and AI and job-related anxiety

Steps Post Deployment

- Establish a bi-annual report on Copilot with metrics, wins/failures to help track progress over time
- Extend the range of Copilot with connectors to third-party data repositories
- Prepare for the next wave of Everyday AI



Questions?



THANK YOU FOR JOINING US | [PROARCH.COM](https://proarch.com)