

AGENTIC AI A PILOTON TÚL

Hogyan kerüljük el a korai
bevezetés hibáit?

Readiness

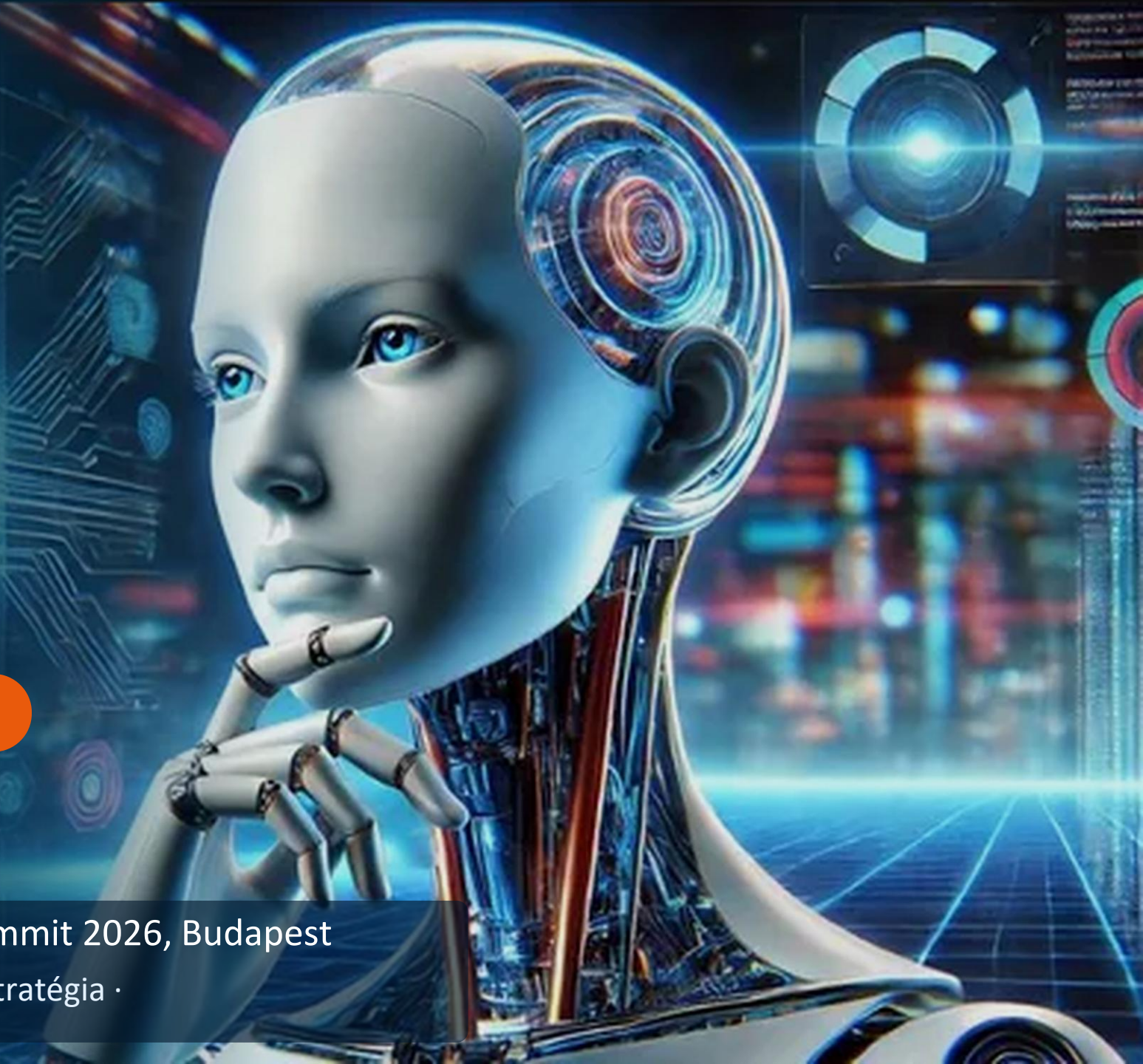
AI governance

Human-in-the-loop

ROI

Dalos-Kovács Gabriella, MBA · AI Summit 2026, Budapest

AI Officer as a Service · AI governance · AI stratégia ·

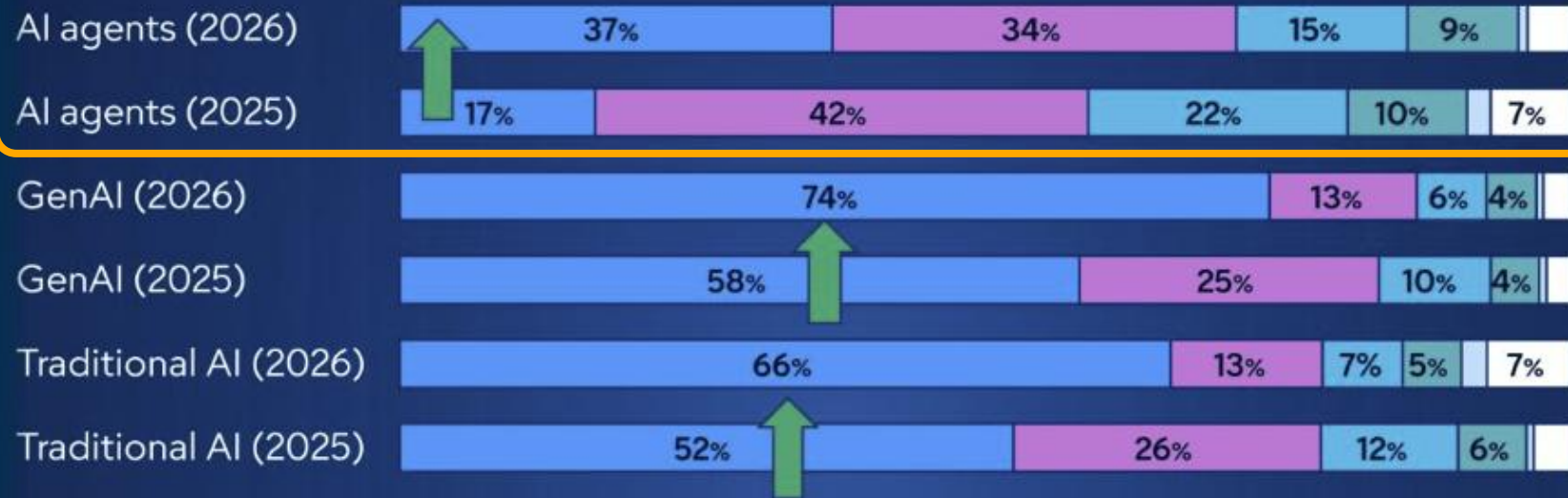


MIÉRT RELEVÁNSAK AZ AI AGENTEK 2026-BAN?

State of deployment for AI, GenAI and agentic AI

Percentage of respondents

■ Have already deployed ■ Will deploy within next 12 months ■ Will deploy in 12-24 months ■ Will deploy in 2-3 years ■ No interest ■ Not sure



Source: Gartner
© Gartner, Inc. and/or its affiliates. All rights reserved. 5254950

Gartner

Éles agent-bevezetés egy év alatt: 17% → 37% - és további 34% érkezik egy éven belül.

PARADIGMAVÁLTÁS: A HAGYOMÁNYOS MI-TŐL AZ AGENTIC AI FELÉ

Mi az agent - és mi nem?

EZ NEM AGENT



Chatbot, copilot - válaszol, nem cselekszik



Excel-makró, automata folyamat - rögzített lépések, nincs tervezés



Machine learning modell - előrejelzést ad, nem hajt végre



Generatív AI önmagában - tartalmat készít kérésre

EZ AGENT



Célt kap, nem utasítás sort - maga bontja lépésekre



Eszközöket hív: API-k, rendszerek, adatbázisok



Önállóan végrehajt - több lépésben, jóváhagyás nélkül is

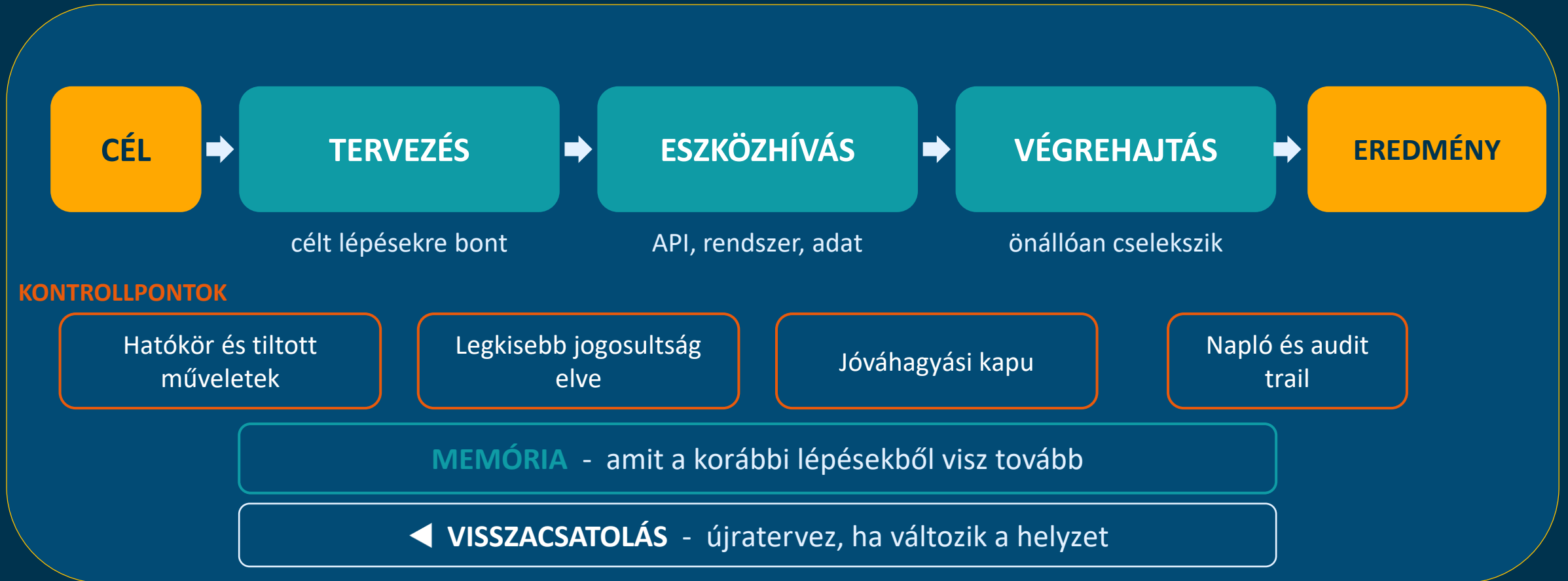


Alkalmazkodik - újratervez, ha változik a helyzet

Gyorsteszt: célt kap, maga tervez, eszközzel végre is hajt? Agent.
Csak válaszol vagy előre írt lépést követ? Nem az.

AZ AGENT ANATÓMIÁJA – NÉGY KONTROLLPONT

Miből áll egy agent - és hol tud a governance beavatkozni?



Az agent nem doboz, hanem hurok - és minden pontján más kontroll kapcsolódik.

MIT BÍZHATUNK AGENTRE – ÉS MIT NEM?

AGENTRE BÍZHATÓ

emberi beavatkozás nem kell

-  Adatok másolása rendszerek között
-  Standard válaszok kiküldése
-  Kalkuláció és riport készítése
-  Fordítás és továbbküldés
-  Összefoglaló készítése, kiküldése
-  Formázás és rendszerezés
-  Keresés, gyűjtés több forrásból

EMBERI BEAVATKOZÁS KELL

-  Egészségügyi döntések
-  Biztonsági protokollok
-  Pénzügyi tranzakciók jóváhagyása
-  Jogi dokumentumok véglegesítése
-  Adóbevallás benyújtása

Az elv: nem az számít, mit tud az agent - hanem mi a hiba ára.

AZ AGENT MÁR OTT VAN **A RENDSZEREKBEN**



Agent platformok



Itt épül a saját agent.

Microsoft Copilot Studio · Google Vertex AI Agent Builder · AWS Bedrock AgentCore · OpenAI AgentKit · Anthropic Claude Agent SDK · IBM watsonx Orchestrate



Folyamat integráció

Ugyanaz a licenc, más képesség.

UiPath · Zapier · Automation Anywhere · Workato · Make · Microsoft Power Automate



Funkcionális agentek

A szakrendszerbe gyárilag beépítve.

Salesforce Agentforce · SAP Joule · ServiceNow AI Agents · Workday Illuminate · HubSpot Breeze · Atlassian Rovo · QuickBooks AI Agents



Fejlesztői agentek

Kódot ír, futtat, éles rendszerhez fér.

GitHub Copilot coding agent · Claude Code · Cursor · Replit Agent 3 · OpenAI Codex · Devin · Google Jules

Egyik sem az AI-projekt része - mégis mind agent, és mind hozzáfér a vállalati adatokhoz.

READINESS: A PILOT ELŐTT DŐL EL

1 INFRASTRUKTÚRA

Az agent nem éri el az adatot és a rendszereket - vagy a rendszer nem bírja a terhelést.

2 GOVERNANCE

Nincs eldöntve, mihez nyúlhat az agent, ki hagyja jóvá a lépéseit, és kié a felelősség.

3 MÉRHETŐSÉG

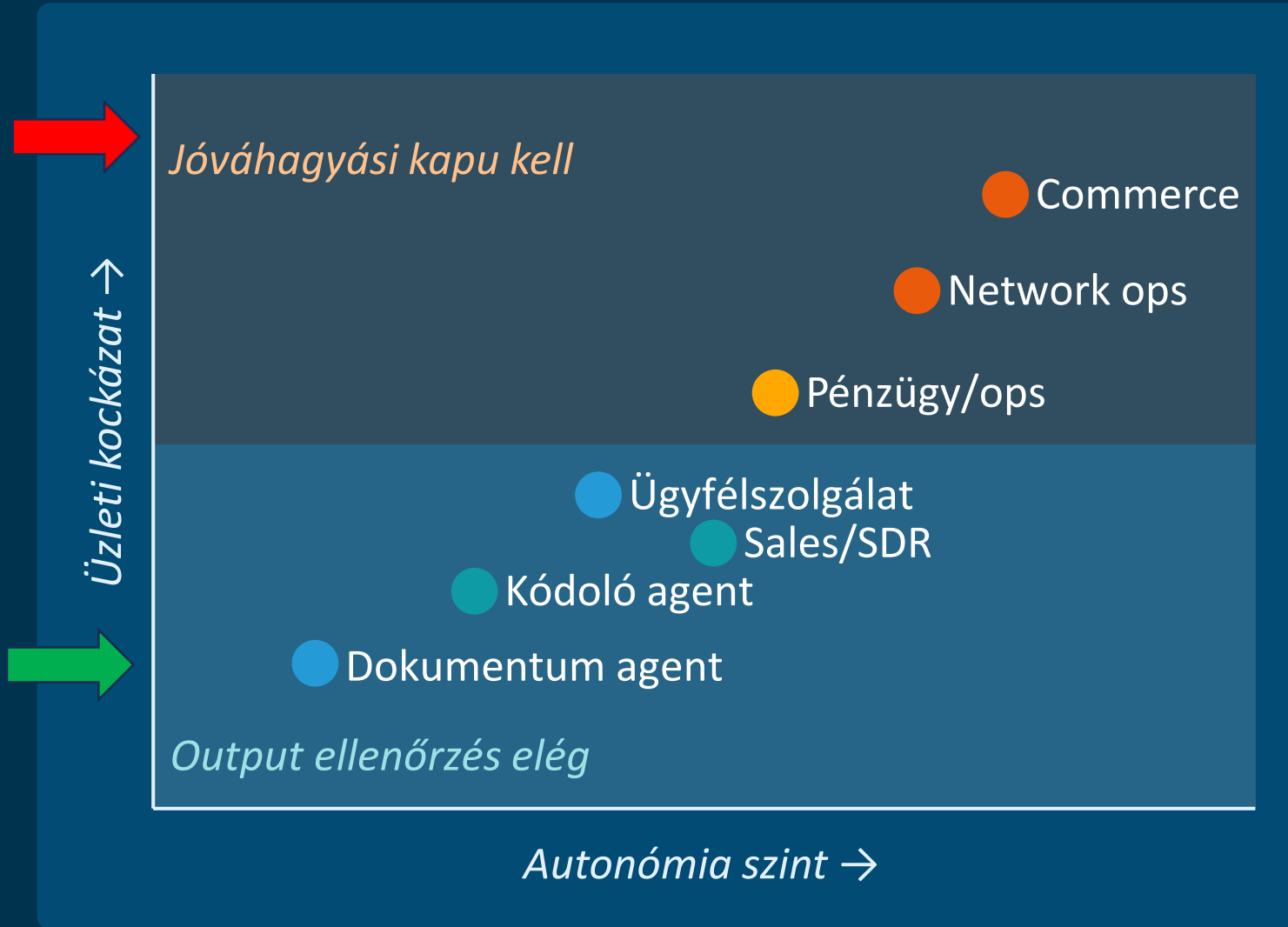
Nincs sikerkritérium és nincs nyomon követés - nem dönthető el, működött-e.

A három ok, amiért az agent megáll a pilotnál. Egyik sem modellprobléma.

A legnagyobb egyedi akadály a mérhetőség: ha nem látjuk, mit csinált az agent lépésről lépésre, nincs hibakeresés, nincs bizonyíték, és nincs jóváhagyás.

Tanulság a gyakorlatból: az agentek túlterhelhetik a back-end rendszereket - nem ilyen használatra tervezték őket.

AI AGENT GOVERNANCE: NEM BINÁRIS – AUTONÓMIASZINT-ALAPÚ



Gartner, 2026:

„Teljes zár vagy teljes bizalom” – a bináris governance a kudarc gyökere.

2027-re a vállalatok 40%-a fokoz le agenteket – éles incidens után felfedezett governance-rések miatt.

TECHNIKAI KONTROLLOK: KÉT SZINT

MINDEN AGENTNÉL

- Hozzáférés-naplózás
- Integrációs kontroll
- Output validáció
- Adat rezidencia

Kivétel nélkül, minden agentnél.

MAGAS KOCKÁZATNÁL, EZEKEN FELÜL

- Jóváhagyási kapu
- Visszaállítás (rollback)
- Vészleállító (kill switch)
- Teljes audit trail
- Terhelés korlátozás

Az előző dia felső sávjába eső agenteknél.

A szint nem az agent képességéből jön - hanem abból, hova esett az előző ábrán.

AI AGENT GOVERNANCE PROGRAM - NÉGY LÉPÉSBEN

1. LÉPÉS: FELMÉRÉS

KIMENET

Agent nyilvántartás

- Agent use case-ek és beágyazott vendor agentek felmérése
- Minden agent regisztrálva az AI nyilvántartásban
- Autonómia, eszköz-hozzáférés és hatókör dokumentálva

2. LÉPÉS: BESOROLÁS

KIMENET

Kockázati és felügyeleti besorolás

- Osztályozás autonómia, ágencia és üzleti hatás szerint
- EU AI Act szerinti kockázati kategória megadása
- Emberi felügyeleti szint hozzárendelése (HITL / HOTL / HIC)

3. LÉPÉS: KONTROLLOK

KIMENET

Kontroll terv, jóváhagyási rend

- Az előző dia két szintje beépítve, agentenként
- Eszkalációs útvonal és névre szóló felelős kijelölve
- Vendor agenteknél: átláthatóság és tesztelési jog a szerződésben

4. LÉPÉS: MŰKÖDTETÉS

KIMENET

Mért működés, bővítési döntések

- Fokozatos bevezetés: alacsony kockázatú use case-ekkel indulva
- Folyamatos monitoring, metrikák és incidens kezelés
- Autonómia bővítés csak mért bizonyíték alapján

MIT MÉRJÜNK EGY AGENTNÉL? HÉT KULCSMETRIKA



A mérés nem cél, hanem a bővítés feltétele - autonómiát csak mért működésre adunk.

ROI: A KÉT OLDAL

MENNYIT HOZ

3,7x

ennyiszeresen térül meg a befektetett összeg

És gyorsan: a szervezetek fele 3-6 hónap alatt jut el ötlettől éles üzemig.

MILYEN GYAKRAN

25%

ennyi kezdeményezés hozta a várt megtérülést

Négyből egy. 2000 vezérigazgató válasza alapján.

Mérj: 1.ciklus időt. 2. hiba arányt, 3. NPS-t. Ne generikus produktivitást.

AGENT-TÍPUS KATALÓGUS – MIT HOZ ÉS MIKOR TÉRÜL?



Ügyfélszolgálat

Salesforce Agentforce: 100M USD éves support-megtakarítás · –8% ügyszám



Kódozó agent

GitHub–Accenture: +8,7% pull request/fejlesztő · +15% merge arány



Sales / SDR

JPMorgan: +20% bruttó értékesítés (vagyonkezelés, 2023→2024)



Ajánlat / RFP

Vodafone: RFP-válasz 10-30 munkanapról percekre



Jogi működés

Salesforce: 12 000 óra jogi munka szabadult fel évente



Network operations

NTT Docomo: 1M+ eszköz · >50% gyorsabb hibareakció



Agentic commerce

Alipay: 120M+ agent-indított tranzakció egy hét alatt

Típusonként más az autonómia, más a kockázat, más a felügyelet.

HOL ÉRDEMES KEZDENI? 3 ALACSONY KOCKÁZATÚ AGENT



Jogosultságkezelő agent

Belső IT-hozzáféréseket kezel: jogosultságot javasol, kioszt és visszavon.

Alacsony kockázat: legkisebb jogosultság, jóváhagyási kapu, teljes audit trail.

REFERENCIA: 6 hónapon belüli megtérülés



Jogszabály figyelő agent

Jogszabályváltozást figyel, és redline-javaslatot készít az érintett szerződésekhez.

Alacsony kockázat: csak javasol - minden módosítást jogász hagy jóvá.

REFERENCIA: ~240 óra / év / jogi szakember



Projektmenedzser agent

Státuszriport, roadmap-vázlat, RACI, emlékeztetők, meeting-ütemezés.

Alacsony kockázat: adminisztratív output - a PM ellenőrzi, mielőtt kimegy.

REFERENCIA: a munkahét 25%-a információkeresés

Közös bennük: visszafordítható, szűk hatókör, ember-ellenőrzött output - és 12 hónapon belül mérhető érték.



KÖSZÖNÖM A FIGYELMET!

Dalos-Kovács Gabriella, MBA

HOL TALÁLKOZHATUNK?



- AI governance képzés
- AI stratégia vállalati workshopok
- EU AI megfelelés a vállalati gyakorlatban képzés

10% kedvezmény - kuponkód: DALOS10

dalos.hu

linkedin.com/in/daloskovacsgabriella

Kérdése van az agentic governance-ről? Keressen bátran.

AGENTIC AI GOVERNANCE – 4 AJÁNLOTT KERETRENDSZER

Model AI Governance Framework for Agentic AI (2026)

IMDA, Szingapúr – az agentic governance vállalati alapjai

AI Agents in Action (2025)

World Economic Forum – agent-bevezetés arányos guardrailekkel

OWASP Top 10 for Agentic Applications (2025)

OWASP – tíz biztonsági kockázat és a kulcsmitigációk

Safeguards for Agentic Finance at Runtime (2026)

MAS, Szingapúr – futásidejű agent governance (SAFR)

Mind a négy anyag nyilvános és ingyenesen elérhető.