Microsoft 365 Copilot

Adatbiztonság az AI korszakában

Útmutató IT-vezetőknek

E-könyv

Ez az útmutató olyan IT-vezetőknek készült, akiknek a feladatai közé tartozik az AI vállalati bevezetésének a lebonyolítása és az adatok védelme. E-könyvünk segít megérteni, hogy milyen kockázatokkal jár az AI az adatbiztonság és az adatvédelem terén, és hasznos betekintést nyújt, hogy Ön magabiztosan irányíthassa az AI-transzformációt.

Tartalom

1

Az AI-alapú munkavégzés új szabályai

A generatív AI új kapukat nyit meg az innováció előtt, és segíti a csapatokat, hogy minden eddiginél gyorsabban és intelligensebben dolgozzanak. Az előrelátó vállalatok számára az AI már nem csupán a legújabb trend a technológia terén, hanem elengedhetetlen üzleti eszköz, amely támogatja a működésüket, értéket teremt és segít a versenyelőny megőrzésében.

Az AI gyors terjedése azonban új kihívásokkal is járt, és néhány meglévő problémát is felerősített, amelyekre az IT-vezetőknek proaktív módon kell reagálniuk. Az AI-rendszerek a teljes adat-ökoszisztémából aktívan lehívhatnak információkat, majd ezeket kombinálhatják, ez pedig nagyobb biztonsági kockázatot jelent a hagyományos eszközökhöz képest. Az AI gyors terjedése ellenére a vállalatok mindössze **1%-a** számolt be arról, hogy a megfelelő biztonsági protokollok kialakítása mellett, teljes mértékben integrálta az AI-t a munkafolyamataiba.[1] Ha azonban már az AI-bevezetés első pillanatától kezdve szigorú biztonsági és irányítási intézkedéseket vezet be, a csapata nemcsak az innováció előnyeit élvezheti, hanem hatékonyan megvédheti a bizalmas és vállalati adatokat, valamint betarthatja a megfelelőségi előírásokat.

Az AI-bevezetés már nem a jövő

2

Az AI adatbiztonságra gyakorolt hatásának megértése

Mielőtt megismerkednénk a konkrét kihívásokkal, fontos, hogy megértsük, hogy milyen alapvető változásokat hoz az AI az adatbiztonsági környezetbe. A hagyományos szoftvere kifejezett csak erre vonatkozó utasítás esetén férnek hozzá az adatokhoz, a generatív AI azonban a kapott információkat alapján képes aktívan tartalmakat feldolgozni, elemezni és létrehozni.

Ez a különbség több okból is jelentős:

- Az AI-eszközök képesek olyan összefüggéseket feltárni az adatok között, amelyeket az emberek esetleg nem vesznek észre
- Képesek automatikusan szintetizálni a különböző forrásokból származó információkat
- Képesek új tartalmakat létrehozni, amelyek esetleg bizalmas bemenetekből származó elemeket tartalmazhatnak

A hagyományos biztonsági eszközök tervezése során általában nem vették figyelembe ezeket az új képességeket. A régebbi szoftverek kiszámítható útvonalat követnek az adatok elérésekor, az AI azonban váratlan módokon is áthaladhat az információs ökoszisztémán, és ennek során bizalmas adatokat tárhat fel.

Ez alapvető változást jelent, ami új megközelítést tesz szükségesség a biztonság és az adatgazdálkodás terén, olyat, amelyet kifejezetten az AI és a vállalati adatvagyon közötti interakciókra terveztek.

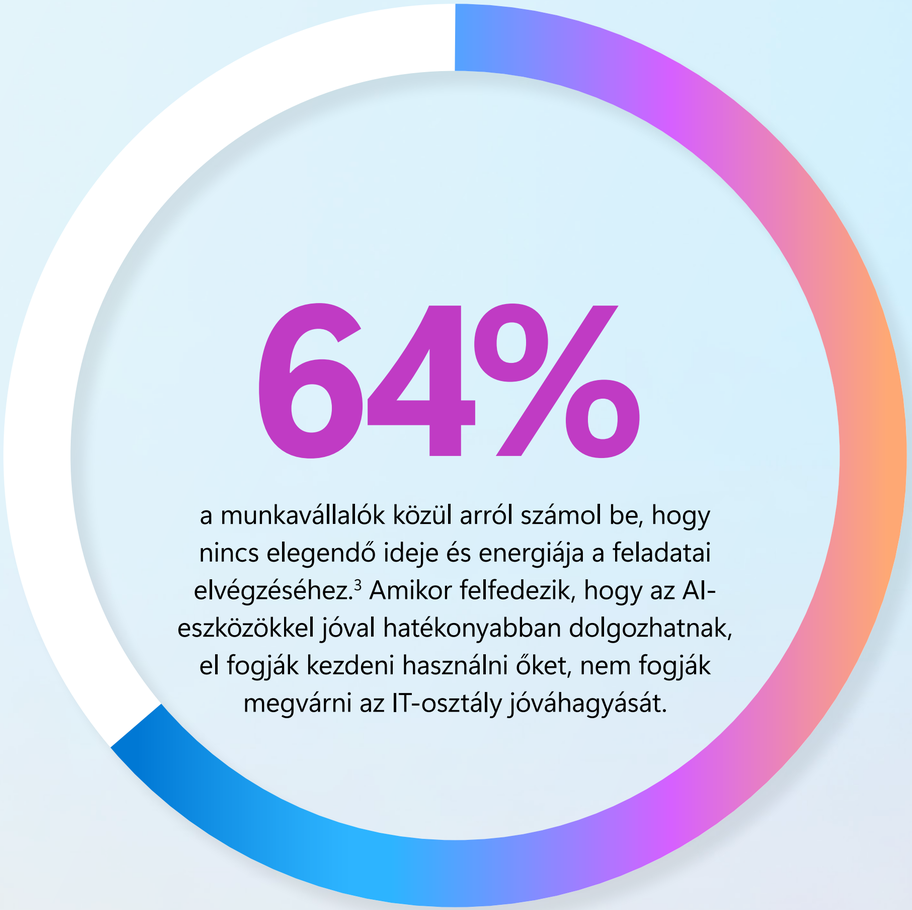
3

A rejtett AI kihívása

Bárhol is tart az Ön vállalata az AI bevezetéséhez vezető úton, a dolgozók már bizonyára megtalálták a saját megoldásaikat. Így jön létre az úgynevezett rejtett AI.

Ez az engedély nélküli használat jelentős vakfoltokat hoz létre a cég biztonsági helyzetében. Amikor a munkavállalók külső AI-rendszerekkel osztják meg a céges adatokat, megkerülik a meglévő biztonsági kontrollokat, és olyan biztonsági réseket hoznak létre, amelyeket a legtöbb vállalat ma nem képes felügyelni.

A rejtett AI nemcsak biztonsági probléma, hanem arra is utalhat, hogy a vállalat nem elégíti ki a munkatársai hatékonysági igényeit. Ha a dolgozók nem engedélyezett eszközöket kezdenek használni, azzal azt jelzik, hogy a hivatalos rendszerek nem felelnek meg a számukra. A rejtett AI kihívásának a leküzdéséhez erősebb irányításra és fejlettebb hatékonyságnövelő megoldásokra van szükség.



A rejtett AI megjelenésének okai:

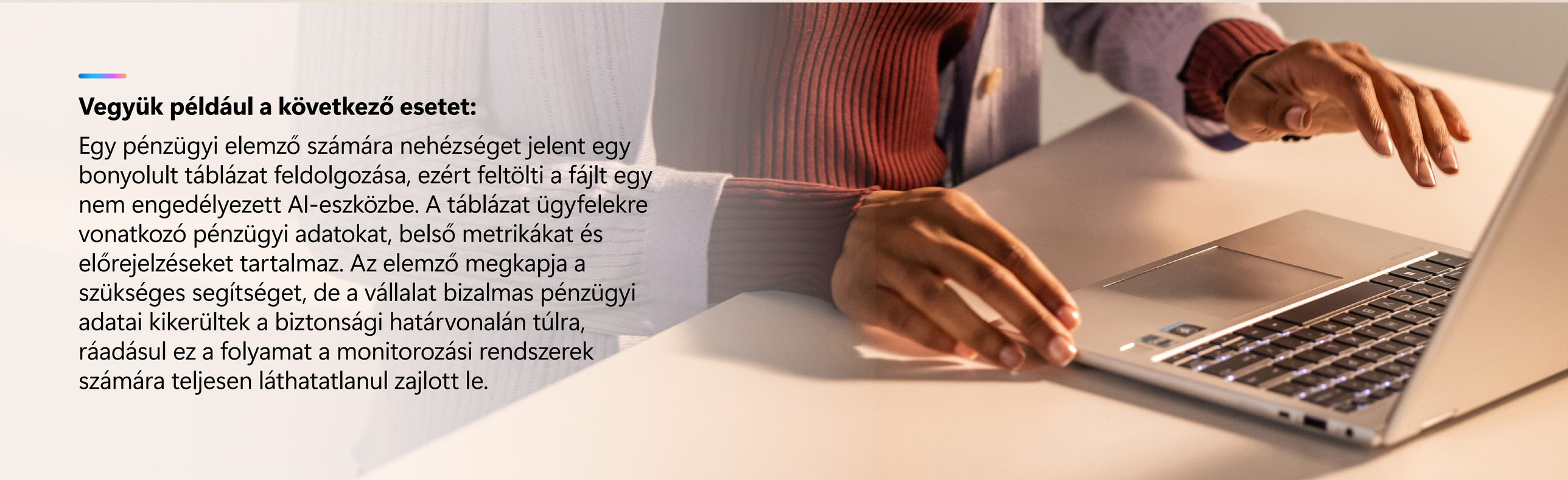
- A dolgozók alig várják, hogy az AI lenyűgöző képességeivel növeljék a hatékonyságukat
- A napi munkaterhelés egyre inkább meghaladja a rendelkezésre álló időt és energiát
- A csapatokra egyre nagyobb nyomás nehezedik, hogy ugyanannyi erőforrással többet érjenek el
- A fogyasztói AI-eszközök azonnali megoldást kínálnak, használatukat nem akadályozzák jóváhagyási előírások
- A hivatalos IT-beszerzési folyamatok nem tudnak lépést tartani az innováció ütemével

A rejtett AI kockázatai:

- A vállalatnak nincs rálátása arra, hogy milyen céges adatok kerülnek ki a külső AI-rendszerekbe
- Nincs garancia arra, hogy a külső rendszer nem őrzi meg a bizalmas információkat
- A különböző AI-platformok nem alkalmaznak egységes biztonsági szabványokat
- A külső rendszerek nem auditálhatók megfelelőségi célokból
- A külső rendszerek nem integrálhatók a meglévő biztonsági infrastruktúrával

Vegyük például a következő esetet:

Egy pénzügyi elemző számára nehézséget jelent egy bonyolult táblázat feldolgozása, ezért feltölti a fájlt egy nem engedélyezett AI-eszközbe. A táblázat ügyfelekre vonatkozó pénzügyi adatokat, belső metrikákat és előrejelzéseket tartalmaz. Az elemző megkapja a szükséges segítséget, de a vállalat bizalmas pénzügyi adatai kikerültek a biztonsági határvonalán túlra, ráadásul ez a folyamat a monitorozási rendszerek számára teljesen láthatatlanul zajlott le.



4

A realitás: BYOAI

Ha a vezetőség nem ad egyértelmű útmutatást, a munkavállalók a saját kezükbe fogják venni az AI-bevezetést: az AI-felhasználók **78%-a** már jelenleg is saját AI-t használ a munkahelyén (ezt nevezzük BYOAI megközelítésnek).[2] Ez a trend még erősebb a kis- és középvállalatoknál, ahol a dolgozók **80%-a** alkalmaz BYOAI-megoldásokat.[2]

Ez a nem jóváhagyott megközelítés jelentős hátrányokkal jár. A dolgozók gyakran titokban tartják, hogy AI-t használnak: **52%** nem szívesen vallja be, hogy AI-t használt valamilyen fontos feladathoz, **53%** pedig aggódik, hogy ha AI-t használ, lecserélhetőnek fog tűnni.[2] Ez a titkolózás megakadályozza, hogy a vállalatok teljes mértékben kihasználhassák a stratégiai célú AI-bevezetés előnyeit, emellett súlyos sebezhetőséget jelent, különösen ma, amikor a vezetők **első számú** aggálynak tartják a kiberbiztonságot és az adatvédelmet.[2]

Tekintettel az AI széles körű és elkerülhetetlen terjedésére, a kérdés nem az, hogy érdemes-e engedélyezni az AI-t a vállalatnál, hanem hogy hogyan lehet olyan biztonságos megoldást kínálni, amely megfelel a dolgozók igényeinek, miközben hatékony védelmet nyújt a vállalat adatainak.

5

A szabályozások labirintusa

Az adatvédelemmel és -biztonsággal kapcsolatos keretrendszerek és jogszabályok az összetettség újabb rétegével nehezítik az AI bevezetését. Egyes keretrendszereket kifejezetten az AI-irányításhoz terveztek, mások azonban szélesebb körű használatra készültek, és ez meghatározza, hogy az Ön vállalata hogyan kezeli az információkat. A szabályok megszegése szigorú büntetést von maga után.

Ha a dolgozók megfelelő felügyelet nélküli AI-eszközöket használnak, akaratlanul is megsérthetik az előírásokat. Az AI növeli ezt a kockázatot, mivel a hagyományos technológiák számára nem elérhető módokon tud hozzáférni az adatokhoz, amelyeket kombinálhat, valamint megjeleníthet.

Az AI használatára vonatkozó legfontosabb szabályozások:

Általános adatvédelmi rendelet (GDPR)

Az Európai Unió általános adatvédelmi rendelete ellenőrzést biztosít az emberek számára személyes adataik felett, és egyértelmű hozzájárulást igényel az adatkezeléshez

Az EU AI-törvénye

Az Európai Unió átfogó keretrendszere, amelyet kifejezetten az AI-rendszerek kockázati szintek szerinti szabályozására terveztek

HIPAA

Az Egyesült Államok egészségügyi törvénye, amely szigorú szabályokat állít fel a védett egészségügyi információk kezelésére vonatkozóan

NIST AI-kockázatkezelési keretrendszer

Ez az önkéntes egyesült államokbeli útmutatás segít a vállalatoknak mérsékelni az AI-rendszerek tervezésével, fejlesztésével és üzembe helyezésével kapcsolatos kockázatokat

Az AI-val kapcsolatos megfelelőségi kockázatok:

- Az ügyféladatok jóváhagyott régiókon kívüli szervereken való feldolgozása
- A személyes adatok megfelelő hozzájárulás nélküli felhasználása
- Bizalmas adatok tárolása olyan rendszerekben, amelyek nem alkalmaznak megfelelő megőrzési kontrollokat
- A védett információk elérését és felhasználását tartalmazó auditnaplók hiánya
- AI által generált tartalmak, amelyek megszegik az ágazatspecifikus megfelelőségi követelményeket

Ezek a szabálysértések súlyos következményekkel járhatnak:

- Nagy összegű bírságok (a GDPR alapján kirótt bírságok akár a vállalat globális bevételének **4%-át** is elérhetik)[4]
- Az érintett feleket kötelező tájékoztatni az adatbiztonsági incidensekről
- Az érintett felek jogi lépéseket tehetnek
- Csorbulhat a vállalat megítélése és az ügyfelek bizalma

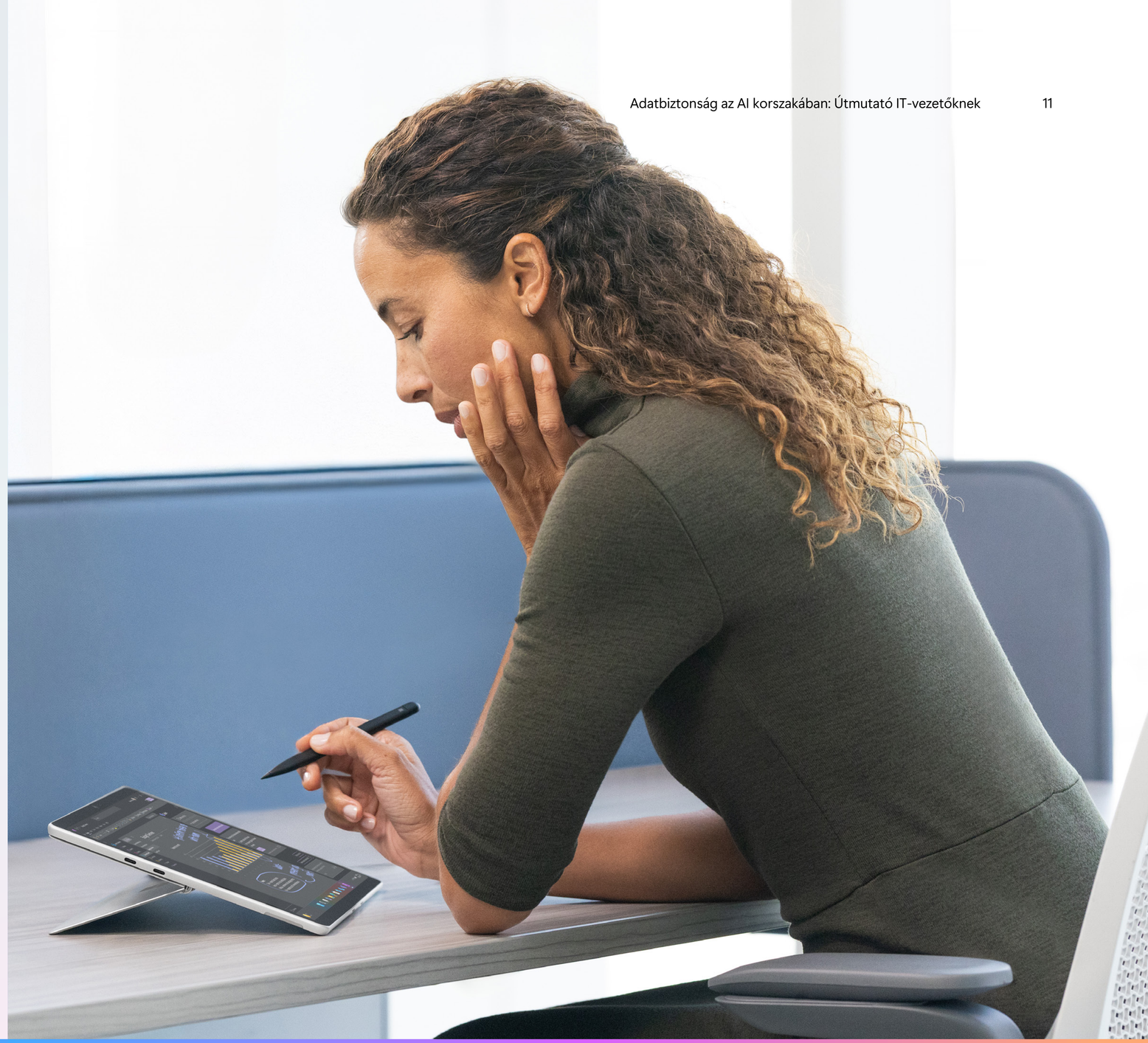
Ahogy a vállalatnál egyre jobban elterjed az AI használata, annál inkább szükség lesz olyan irányítási megoldásokra, amelyek elősegítik a hatékony munkát, de közben gondoskodnak róla, hogy a cég megfeleljen az üzleti tevékenységére és az ügyfeleire vonatkozó előírásoknak.

6

Biztonságot előtérbe helyező keretrendszer az AI-megoldások kiértékeléséhez

A rejtett AI, a BYOAI és a szabályozások jelentős kockázatokkal járnak, a vállalatnak strukturált megközelítést kell alkalmaznia az AI-megoldások kiértékelése során, hogy olyan eszközt válasszon, amely ösztönzi az innovációt, ugyanakkor megóvja a bizalmas adatokat és elősegíti a változó szabályozási követelmények betartását.

Az alábbi keretrendszer hat egyszerű kérdést tartalmaz, amelyek segítenek felmérni, hogy egy adott AI-platform mindkét területen jól teljesít-e.



1. kérdés

Kínál a rendszer az alapoktól kezdve nagyvállalati szintű biztonságot?

A megfelelő megoldás birtokában elérheti, hogy a vállalat ne csak reagáljon a már bekövetkezett problémákra, hanem proaktívan keresse a biztonsági réseket a céges adatokban, még nagyobb problémává válnának.

Keressen olyan megoldást, amely:

- Valós idejű átláthatóságot biztosít a teljes adat-ökoszisztéma fölött
- Automatikusan azonosítja a potenciális adatkockázatokat, mielőtt bekövetkezne az incidens
- Minden szinten védi a bizalmas információkat

2. kérdés

Képes a rendszer átvenni és továbbfejleszteni a meglévő biztonsági kontrollokat?

A vállalat biztonsági szabályzatainak zökkenőmentesen együtt kell működniük az AI-val. Az AI-megoldás szolgáltatójának figyelembe kell vennie és integrálnia kell a meglévő biztonsági keretrendszereket, nem követelheti meg teljesen újak létrehozását.

Keressen olyan megoldást, amely:

- Zökkenőmentesen átveszi a meglévő biztonsági szabályzatokat, bizalmassági címkéket és információvédelmi beállításokat
- Részletes hozzáférés-szabályozást alkalmaz az egyének szintjén, így egyetlen felhasználó sem férhet hozzá olyan adatokhoz, amelyekhez nem szabad
- Aktívan jelzi a hozzáférési szabályok megkerülésére irányuló kísérleteket

3. kérdés

Tartalmaz a rendszer beépített irányítási és adatvédelmi kontrollokat?

Az AI-eszközök proaktívabban működnek, ezért a biztonsági intézkedéseknek is proaktívnak kell lenniük. Erős adatgazdálkodás bevezetésével egyértelmű határokat húzhatunk, így biztonságos innovációt kínálhatunk a dolgozóknak, anélkül, hogy veszélybe sodornánk a bizalmas információkat.

Keressen olyan megoldást, amely:

- Minden tevékenységhez központi AI-irányítást és automatikus szabályzatbetartatást biztosít
- Képes korán észlelni az adatok túl széles körű megosztását
- Igazodik a szabályozási keretrendszerekhez a szabálykövető AI-használat érdekében

4. kérdés

Egységesen bevezethető a rendszer a vállalat minden részén?

A munkavállalók gyakran a világ különböző pontjairól dolgoznak, saját munkamódszerekkel és időbeosztással. Az AI-nak mindenki számára előnyösnek kell lennie.

Keressen olyan megoldást, amely:

- Zökkenőmentes telepítést és egyszerű AI-használatot kínál a mindennapos munkafolyamatokban
- Rugalmas hozzáférést biztosít az ingyenes AI-csevegéstől kezdve a skálázható ügynökmegoldásokig
- Segít a dolgozóknak az AI-használat elsajátításában és az eszköz munkájukba való beépítésében

5. kérdés

Zökkenőmentesen integrálódik a meglévő keretrendszerekbe?

Az Ön vállalata jelenleg szoftverekből, alkalmazásokból és más eszközökből álló saját digitális infrastruktúrát működtet.

Keressen olyan megoldást, amely:

- Zökkenőmentesen illeszkedik a vállalat meglévő eszközeihez és programjaihoz a fennakadások minimalizálása érdekében
- Folyamatos AI-képességeket biztosít az összes alkalmazásban, így minden eszközben egyformán megkönnyíti a munkát
- Automatizálja és optimalizálja a feladatokat a meglévő munkafolyamatokon belül

6. kérdés

Támogatja a rendszer a felhasználókat az innovációban?

Az AI-nak alapvetően át kell alakítania a munkavégzés módját. Ez nem csak az automatizálásról szól, hanem a hatékonyság növeléséről és az innováció ösztönzéséről is.

Keressen olyan megoldást, amely:

- Megszünteti és jelentősen egyszerűsíti az időigényes folyamatokat
- Automatizálja az ismétlődő feladatokat
- Támogatja a dolgozókat abban, hogy visszaszerezzék az idejüket és a fontos feladatokra összpontosítsanak

7

Microsoft 365 Copilot: AI, amelyben megbízhat

A Microsoft 365 Copilot egy generatív AI-megoldás, amely átfogó biztonsági, irányítási és hozzáférés-szabályozási funkciókat biztosít, és elősegíti a biztonságos üzembe helyezést és a folyamatos innovációt. Olyan intuitív eszközökkel fokozza a hatékonyságot, mint a Copilot Chat, amely közvetlenül a munkaeszközökben érhető el, vagy éppen a Copilot Studio, amelyben a csapata kódolás nélkül hozhat létre egyéni AI-ügynököket.

A Copilot zökkenőmentesen beépül a Microsoft 365-környezetbe, további konfigurálás nélkül örökli a felhasználói engedélyeket, a bizalmassági címkéket, az adatvesztés-megelőzési szabályzatokat és a földrajzi adatok tárolási helyére vonatkozó előírásokat. A Copilot AI-t ágyaz be a dolgozók által használt eszközökbe, így csökkenti a biztonsági kockázatokat, az adatokat pedig a megbízható Microsoft 365-környezetben tartja.

A Microsoft kötelezettségvállalásai gondoskodnak róla, hogy az irányítás a vállalat kezében maradjon:

- Az adatokat tárolás és továbbítás esetén egyaránt titkosítjuk
- Az adatokat nem használjuk fel az AI-modellek betanításához
- Ön dönti el, hogy mely információk kerüljenek fel a felhőbe
- Ön védelmet élvez az AI-val kapcsolatos biztonsági és szerzői jogi kockázatokkal szemben

A célirányosan kialakított irányítási eszközök, például a Copilot Control System és a SharePoint Advanced Management átláthatóságot, kontrollokat és auditnaplókat biztosítanak az IT-csapatoknak a megfelelőség megőrzéséhez.

A Microsoft 365 Copilottal nem kell választania az innováció és a biztonság között, mindkettő előnyeit élvezheti.

8

Biztonságos út a mesterséges intelligenciára való áttéréshez

Az AI-forradalom egyedülálló lehetőséget kínál az IT-vezetőknek, hogy megtalálják az egyensúlyt az innováció és a biztonság között, és így stratégiai értéket teremtsenek.

Biztonságos AI-eszközök, például a Microsoft 365 Copilot bevezetésével a dolgozók hatékonyabban végezhetik a munkájukat, a vállalat pedig a rejtett AI kockázataitól is megszabadul. A jövő a biztonságos innovációé. Ha az AI biztonságos bevezetésének az élére áll, azzal az átalakulás támogatójaként pozicionálhatja az IT-osztályt, és segítheti a vállalatot, hogy ebben az új korszakban is sikeresen működjön, valamint hatékony adatvédelmet és erős megfelelőséget érhet el.

Kezdjen el ismerkedni a Microsoft 365 Copilottal!

Források:

[1] „Superagency in the workplace: Empowering people to unlock AI's full potential", McKinsey & Company, 2025. január 28. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/superagency-in-the-workplace-empowering-people-to-unlock-ais-full-potential-at-work.

[2] „Az AI megérkezett a munkahelyre. Most jön a neheze", Microsoft Work Trend Index, 2024. május 8. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part.

[3] „Megoldja az AI a munkahelyi problémákat?", Microsoft Work Trend Index, 2023. május 9. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[4] „Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet)", Az Európai Parlament és az EU Tanácsa, 2016. április 27. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.