Microsoft 365 Copilot

Zabezpečení dat v éře AI

Průvodce pro vedoucí pracovníky IT

E-kniha

Tato příručka je určena pro vedoucí pracovníky IT, kteří potřebují podpořit zavádění AI a zároveň zabezpečit data svých organizací. Pomůže vám pochopit rizika, která AI představuje pro zabezpečení dat a soukromí, a zároveň vám poskytne informace potřebné k tomu, abyste mohli s jistotou vést transformaci vaší společnosti v oblasti AI.

Obsah

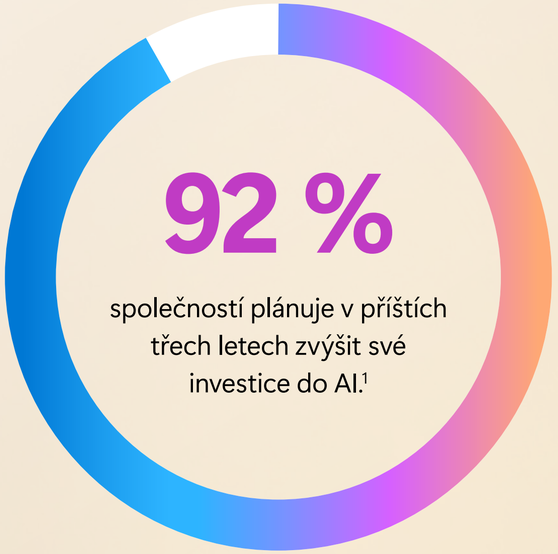
01

Nová pravidla práce využívající AI

Generativní AI otevírá nové dveře pro inovace a pomáhá týmům pracovat rychleji a chytřeji než kdykoli předtím. Pro organizace, které myslí na budoucnost, není AI jen dalším technologickým trendem – je to obchodní imperativ, který je nezbytný pro jejich fungování, poskytování hodnoty a udržení konkurenční výhody.

Toto rychlé zavádění však přináší nové a intenzivnější výzvy, které musí vedoucí pracovníci IT aktivně řešit a kontrolovat. Systémy AI mohou aktivně vyhledávat a kombinovat informace v celém datovém ekosystému, což zvyšuje bezpečnostní rizika nad rámec tradičních nástrojů. Navzdory rychlému rozšíření AI pouze **1 %** organizací uvádí, že plně integrovalo AI do svých pracovních postupů s řádnými protokoly zabezpečení.[1] Zavedením důkladných bezpečnostních a řídicích opatření od začátku cesty k AI může váš tým účinně chránit citlivá data, dodržovat požadavky na dodržování předpisů a chránit informace vaší organizace – to vše při současném umožnění rozvoje inovací.

Vlna zavádění AI je již tady



02

Pochopení dopadu AI na zabezpečení dat

Než se pustíme do konkrétních výzev, je důležité pochopit, jak AI zásadně mění prostředí zabezpečení dat. Na rozdíl od tradičního softwaru, který přistupuje k datům pouze na základě konkrétních pokynů, generativní AI aktivně zpracovává, analyzuje a vytváří obsah na základě všech získaných informací.

Tento rozdíl je významný z několika důvodů:

- Nástroje AI dokážou odhalit souvislosti mezi daty, které by lidem mohly uniknout.
- Mohou automaticky syntetizovat informace napříč více zdroji.
- Mohou generovat nový obsah, který obsahuje prvky z citlivých vstupů.

Vaše tradiční nástroje zabezpečení pravděpodobně nebyly navrženy s ohledem na tyto možnosti. Zatímco běžný software se při přístupu k datům řídí předvídatelnými cestami, AI se může vydat neočekávanými cestami skrze váš informační ekosystém a potenciálně odhalit citlivá data způsobem, který jste nepředpokládali.

Tento zásadní posun vyžaduje nové přístupy k zabezpečení a řízení dat, které se konkrétně zabývají tím, jak AI interaguje s informačními zdroji vaší organizace.

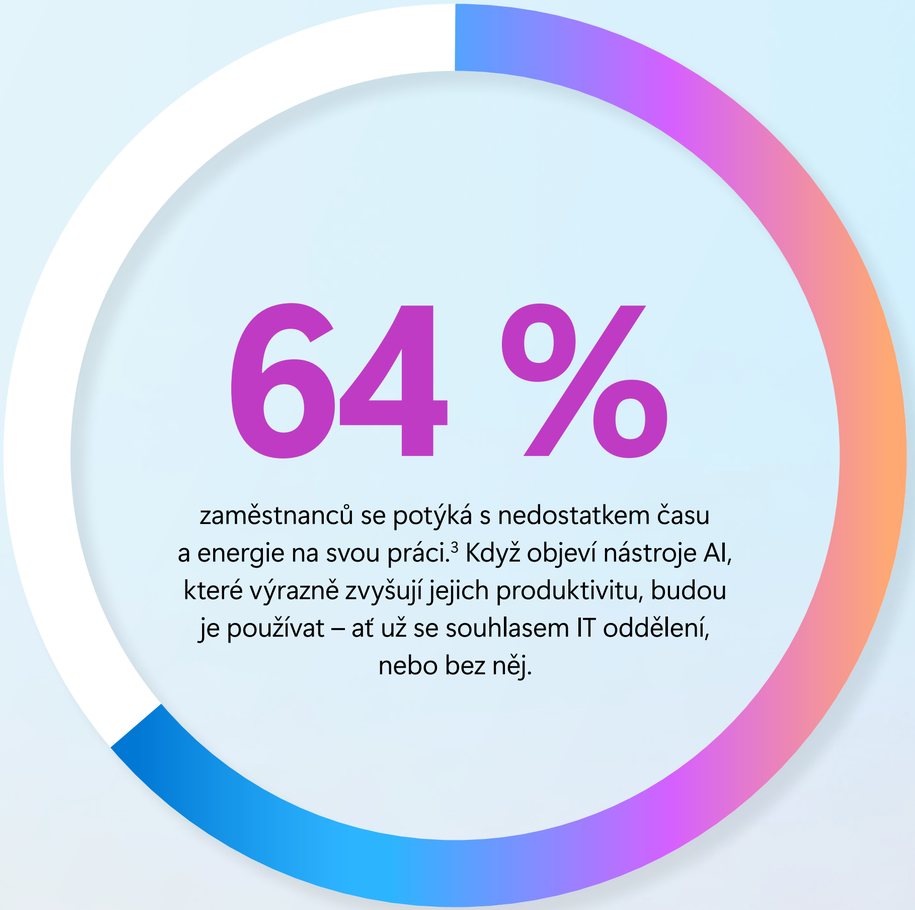
03

Výzva stínové AI

Ať už jste na cestě k přijetí AI kdekoli, vaši zaměstnanci již nacházejí vlastní řešení a vytvářejí takzvanou „stínovou AI“.

Toto neoprávněné použití vytváří významná slepá místa v zabezpečení. Když zaměstnanci sdílejí firemní data s externími systémy AI, obcházejí stávající bezpečnostní kontrolní mechanismy a vytvářejí zranitelná místa, na která většina organizací není připravena.

Stínová AI není jen bezpečnostní problém, ale může být také příznakem neuspokojených požadavků na produktivitu ve vaší organizaci. Když se zaměstnanci obrátí na neschválené nástroje, signalizují, kde vaše oficiální systémy nesplňují jejich požadavky. Řešení problematiky stínové AI vyžaduje jak silnější řízení, tak vylepšená řešení pro produktivitu.



Proč vzniká stínová AI:

- Zaměstnanci chtějí zvýšit produktivitu pomocí působivých schopností AI.
- Každodenní pracovní zátěž stále více přesahuje čas a energii, které mají k dispozici.
- Týmy čelí rostoucímu tlaku, aby se stejnými zdroji dodávaly více.
- Nástroje AI pro spotřebitele nabízejí okamžitá řešení bez překážek při schvalování.
- Oficiální procesy zadávání zakázek v oblasti IT nemohou odpovídat tempu inovací.

Rizika stínové AI:

- Chybí přehled o tom, jaká firemní data zpracovávají externí systémy AI.
- Chybí záruka, že nebudou uchovávány důvěrné informace.
- Chybí jednotné bezpečnostní standardy pro různé platformy AI.
- Chybí auditovatelnost pro účely dodržování předpisů.
- Chybí integrace se stávající infrastrukturou zabezpečení.

Zvažte tento scénář:

Finanční analytik, který si neví rady se složitou tabulkou, ji nahraje do neautorizovaného nástroje AI, aby získal pomoc. Tato tabulka obsahuje finanční údaje zákazníků, interní metriky a projekce. Přestože analytik získá potřebnou pomoc, citlivá finanční data vaší organizace se nyní nacházejí mimo bezpečnostní perimetr, zcela neviditelná pro vaše monitorovací systémy.

04

Realita BYOAI

Bez jasného vedení ze strany vedení přebírají zaměstnanci stále častěji zavádění AI do vlastních rukou – **78 %** uživatelů AI uplatňuje v práci přístup „přines si vlastní AI“ (BYOAI).[2] Tento trend je ještě výraznější v malých a středních firmách, kde postupy BYOAI využívá **80 %** zaměstnanců.[2]

Tento neschválený přístup má značné nevýhody. Zaměstnanci často tají, že používají AI – **52 %** se zdráhá přiznat, že používá AI pro důležité úkoly a **53 %** se obává, že kvůli používání AI budou vypadat jako nahraditelní.[2] Toto utajování nejenže brání organizacím plně využít výhod strategické implementace AI, ale také vytváří vážné bezpečnostní slabiny v prostředí, kde vedoucí pracovníci uvádějí kybernetické zabezpečení a ochranu osobních údajů jako své **největší** obavy.[2]

Vzhledem k rozšířenému používání a nevyhnutelnému růstu AI není otázkou, zda povolit AI ve vaší organizaci. Jde o to, jak poskytnout bezpečné řešení, které splní potřeby vašich zaměstnanců a zároveň ochrání data vaší organizace.

05

Bludiště regulací

Rámce a zákony týkající se ochrany osobních údajů a zabezpečení dat vytvářejí při zavádění AI další vrstvu složitosti. Zatímco některé rámce jsou speciálně navrženy pro řízení AI, jiné mají širší aplikace, které stále ovlivňují způsob, jakým nakládáte s informacemi. Sankce za porušení zůstávají přísné.

Pokud vaši zaměstnanci používají nástroje AI bez řádného dohledu, mohou neúmyslně způsobit porušení předpisů. AI toto riziko zvyšuje, protože může přistupovat k regulovaným informacím, kombinovat je a zveřejňovat způsobem, jakým to tradiční technologie nedokáží.

Klíčové předpisy ovlivňující vaše používání AI:

GDPR

Obecné nařízení Evropské unie o ochraně osobních údajů dává lidem kontrolu nad jejich osobními údaji a vyžaduje jasný souhlas s jejich zpracováním.

Akt EU o umělé inteligenci

Komplexní rámec Evropské unie, který je speciálně navržen tak, aby reguloval systémy AI na základě jejich úrovně rizika.

HIPAA

Tento americký federální zákon o zdravotní péči stanoví přísné standardy pro nakládání s chráněnými zdravotními údaji.

NIST AI Risk Management Framework

Tento dobrovolný americký metodický pokyn pomáhá organizacím řešit rizika při návrhu, vývoji a zavádění systémů AI.

Rizika spojená s dodržováním předpisů u AI:

- Zpracování zákaznických dat na serverech mimo schválené oblasti.
- Používání osobních údajů bez řádného souhlasu.
- Citlivá data zůstávající v systémech bez náležitých kontrolních mechanismů uchovávání.
- Chybějící auditní stopa o tom, jak se přistupuje k chráněným informacím a jak jsou používány.
- Obsah generovaný AI, který porušuje požadavky na dodržování předpisů specifické pro dané odvětví.

Tato porušení mohou mít vážné důsledky:

- Vysoké finanční sankce (pokuty podle nařízení GDPR mohou dosáhnout **až 4 %** vašich celosvětových výnosů).[4]
- Požadavky na oznamování úniků dat dotčeným stranám.
- Právní kroky dotčených subjektů.
- Poškození pověsti vaší společnosti a důvěry zákazníků.

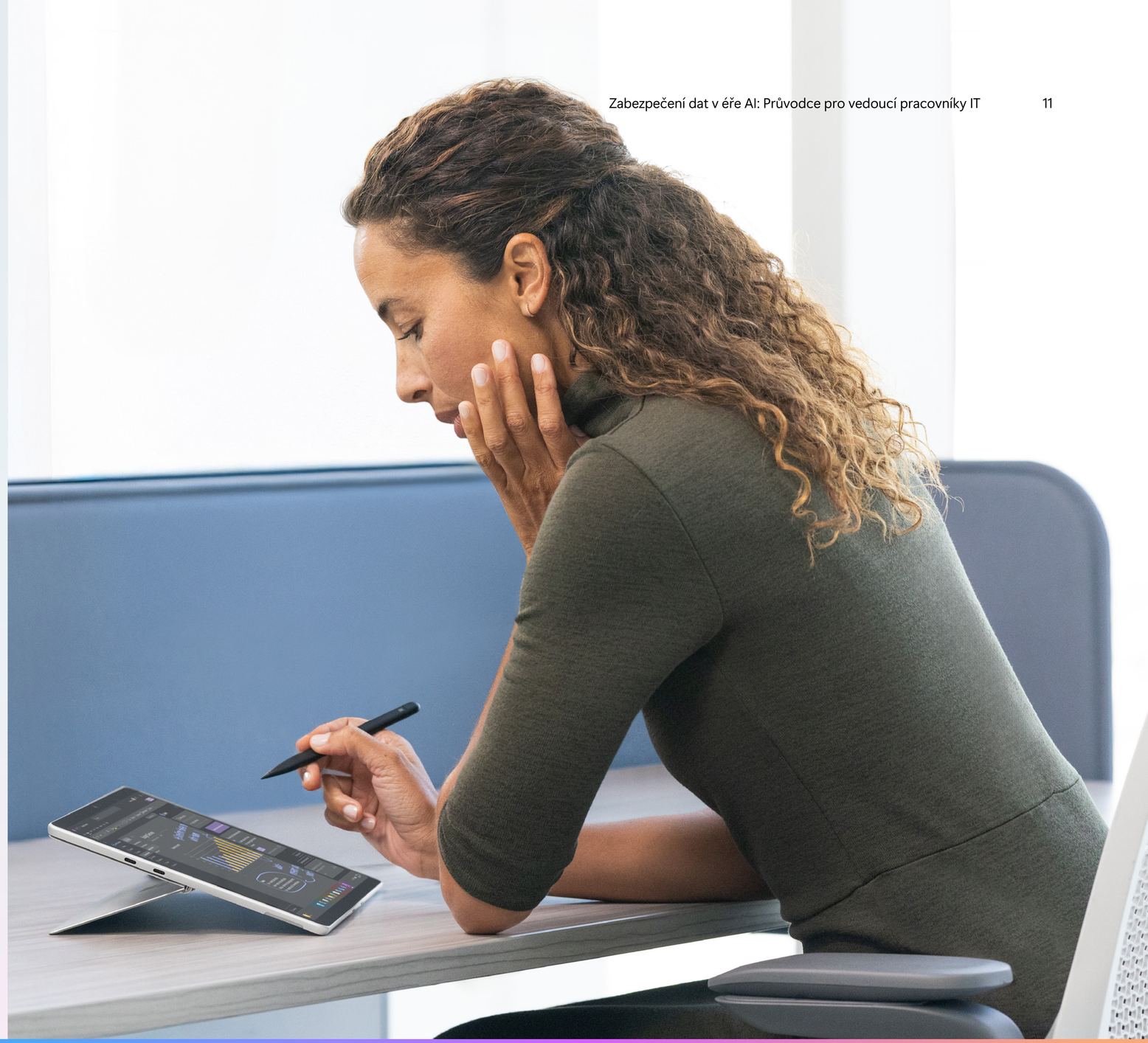
S rostoucím využíváním AI ve vaší organizaci potřebujete zásady správného řízení, které lidem pomůžou pracovat efektivně a zároveň zajistí soulad vaší organizace s předpisy, které se týkají vaší firmy a vašich zákazníků.

06

Rámec pro hodnocení řešení AI zaměřený na zabezpečení

Vzhledem k tomu, že stínová AI, BYOAI a předpisy vytvářejí významná rizika, potřebujete strukturovaný přístup k hodnocení řešení AI, který zajistí, že mohou vaší organizaci pomoci podporovat inovace a zároveň chránit citlivá data a zajistit soulad s vyvíjejícími se regulačními požadavky.

Následující rámec obsahuje šest jednoduchých otázek, které umožňují posoudit, zda platforma AI splňuje obě tyto podmínky.



1. otázka

Nabízí zabezpečení na podnikové úrovni od základů?

Se správným řešením se vaše zabezpečení přesune od pouhého reagování na problémy poté, co nastanou, k proaktivnímu vyhledávání zranitelných míst v datech vaší organizace – dříve, než se z nich stanou větší problémy.

Hledejte řešení, která:

- Poskytují přehled v reálném čase o celém datovém ekosystému.
- Automaticky identifikují potenciální rizika pro data dříve, než se z nich stanou incidenty.
- Chrání citlivé informace na všech úrovních.

2. otázka

Může snadno přijmout a rozšířit stávající kontrolní mechanismy zabezpečení?

Zásady zabezpečení vaší organizace by měly bezproblémově spolupracovat s AI. Poskytovatel řešení AI by měl respektovat vaše stávající bezpečnostní rámce a integrovat se do nich – nikoli vyžadovat vytvoření zcela nových.

Hledejte řešení, která:

- Bez problémů převezmou vaše stávající zásady zabezpečení, popisky citlivosti a nastavení ochrany informací.
- Uplatňují granulární řízení přístupu na individuální úrovni, takže žádný uživatel nemá přístup k datům, ke kterým by neměl.
- Aktivně označují pokusy o narušení kontroly přístupu.

3. otázka

Obsahuje integrované kontrolní mechanismy pro zásady správného řízení a ochranu osobních údajů?

Protože nástroje AI fungují proaktivněji, musí být proaktivní i vaše bezpečnostní opatření. Zavedení důsledného řízení dat vytváří jasné hranice, kde mohou vaši zaměstnanci bezpečně inovovat, aniž by ohrozili citlivé informace.

Hledejte řešení, která:

- Centralizují řízení AI pomocí automatizovaného prosazování zásad v rámci všech aktivit.
- Nabízí včasné odhalení potenciálního sdílení dat.
- Sladí se s regulačními rámci a zajistí používání AI v souladu s předpisy.

4. otázka

Může být nasazena konzistentně v celé organizaci?

Vaši zaměstnanci mají svůj vlastní styl práce, své vlastní rozvrhy a mohou se nacházet po celém světě. AI by měla být přínosem pro všechny.

Hledejte řešení, která:

- Nabízí bezproblémové nastavení a snadné přijetí AI v každodenních pracovních postupech.
- Poskytují flexibilní přístup, od bezplatného chatu s AI až po škálovatelná řešení agentů.
- Pomáhají zaměstnancům budovat znalost AI a integrovat ji do jejich práce.

5. otázka

Integruje se bez problémů do stávajících rámců?

Vaše firma v současné době provozuje vlastní digitální infrastrukturu softwarových programů, aplikací a dalších prvků.

Hledejte řešení, která:

- Se bez problémů propojí s vašimi nástroji a programy, aby se minimalizovalo narušení.
- Zajistí nepřetržitý provoz AI ve všech aplikacích, aby práce mohla plynule probíhat mezi jednotlivými nástroji.
- Automatizují a optimalizují úlohy v rámci stávajících pracovních postupů.

6. dotaz

Mají uživatelé možnost inovovat?

Ve své podstatě by AI měla změnit způsob práce. Nejde jen o automatizaci – jde o zvýšení produktivity a podporu inovací.

Hledejte řešení, která:

- Mění časové ztráty na zefektivnění procesů.
- Automatizují opakující se úlohy.
- Umožní pracovníkům, aby ušetřili čas a soustředili se na priority.

07

Microsoft 365 Copilot: AI, které můžete důvěřovat

Microsoft 365 Copilot je řešení generativní AI vytvořené pro robustní zabezpečení, řízení a kontrolu přístupu, které zajišťuje bezpečné nasazení a dlouhodobé inovace. Zvyšuje produktivitu pomocí intuitivních nástrojů, jako je Copilot Chat, který funguje tam, kde pracujete, a Copilot Studio, kde váš tým může vytvářet vlastní agenty AI bez znalostí kódování.

Copilot se bez problémů integruje do prostředí Microsoft 365 a přebírá uživatelská oprávnění, popisky citlivosti, zásady prevence ztráty dat a požadavky na geografickou rezidenci dat – bez další konfigurace. Začleněním AI do nástrojů, které vaši zaměstnanci již používají, Copilot snižuje bezpečnostní rizika a zároveň uchovává data v důvěryhodném prostředí Microsoft 365.

Závazky Microsoftu zajišťují, že si vaše organizace udrží kontrolu:

- Vaše data jsou zabezpečená v klidovém stavu i při přenosu.
- Vaše data se nepoužívají k trénování modelů AI.
- Sami rozhodujete, které informace se dostanou do cloudu.
- Jste chráněni před riziky spojenými se zabezpečením AI a autorskými právy.

Cíleně vytvořené nástroje pro zásady správného řízení, jako je Copilot Control System a SharePoint Advanced Management, poskytují týmům IT přehled, kontroly a auditní protokoly potřebné k zachování dodržování předpisů.

S řešením Microsoft 365 Copilot nemusíte volit mezi inovací a zabezpečením – můžete mít obojí.

08

Bezpečná cesta k transformaci AI

Revoluce v oblasti AI představuje pro vedoucí pracovníky IT jedinečnou příležitost poskytovat strategickou hodnotu vyvážením inovací a zabezpečení.

Implementací bezpečných nástrojů AI, jako je Microsoft 365 Copilot, poskytnete zaměstnancům nástroje pro vyšší produktivitu a zároveň eliminujete rizika stínové AI. Cesta vpřed spočívá v bezpečném umožnění inovací. Vaše vedoucí postavení v zavádění zabezpečené AI postaví IT do pozice hybatele transformace, který pomůže vaší organizaci prosperovat v této nové éře a zároveň zajistí zabezpečení dat a dodržování předpisů.

Začínáme s řešením Microsoft 365 Copilot

Zdroje:

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

[2] „AI dorazila do pracovního prostředí. Teď přichází ta těžká část.“ Index pracovních trendů od Microsoftu, 8. května 2024. https://www.microsoft.com/en-us/worklab/work-trend-index/ai-at-work-is-here-now-comes-the-hard-part.

[3] „Napraví AI práci?“ Index pracovních trendů od Microsoftu, 9. května 2023. https://www.microsoft.com/en-us/worklab/work-trend-index/will-ai-fix-work.

[4] „Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů),“ Evropský parlament a Rada Evropské unie, 27. dubna 2016. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.