Microsoft 365

Od dohledu k přehledu: Řízení rizik stínové AI

Obsah

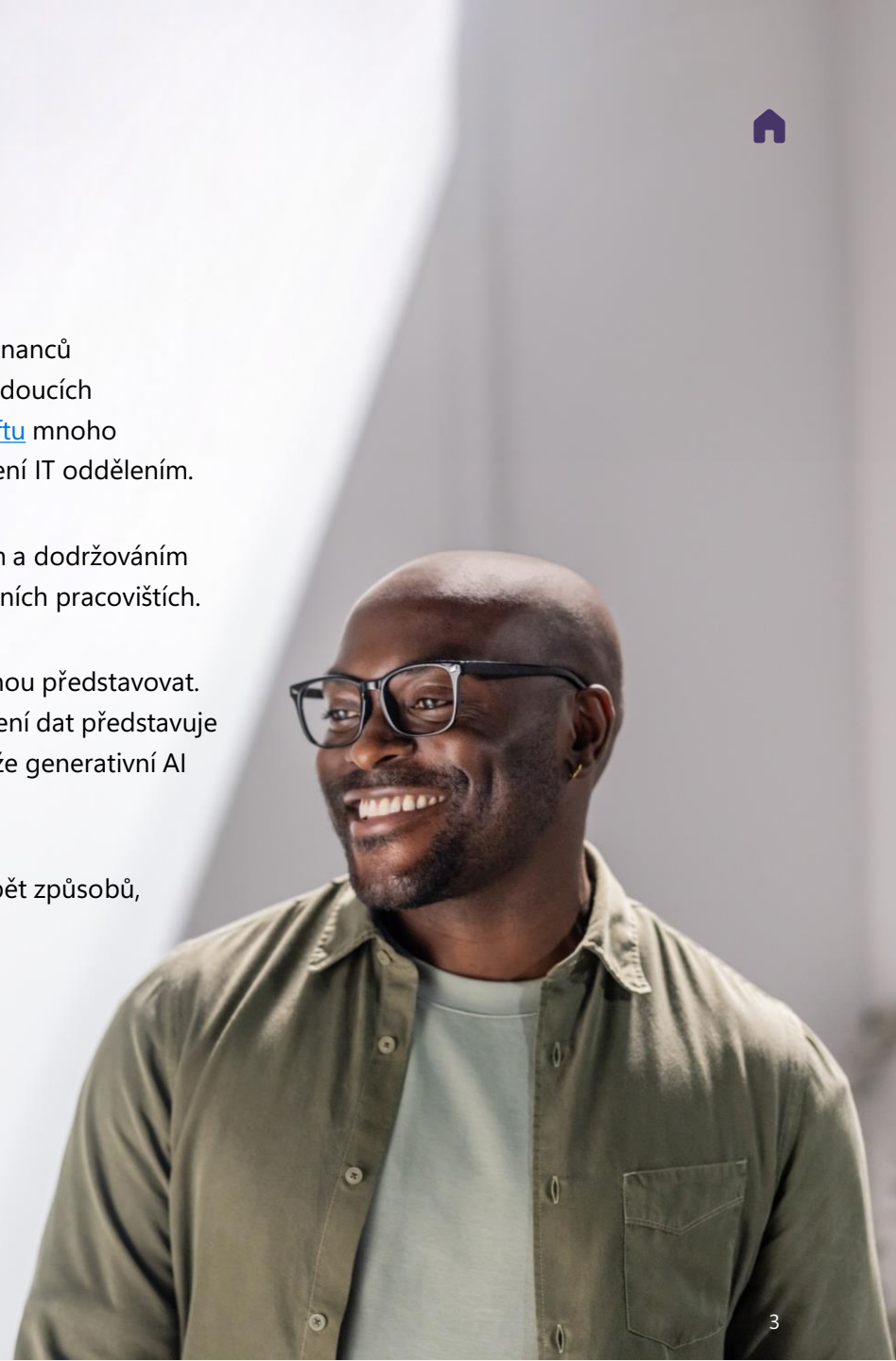
Úvod

V nedávné zprávě Index pracovních trendů více než 80 % dotazovaných znalostních pracovníků z 31 zemí – včetně zaměstnanců a vedoucích pracovníků – uvedlo, že mají pocit, že jim chybí čas nebo energie na práci. Navíc více než 50 % oslovených vedoucích pracovníků uvedlo, že ke splnění cílů je třeba zvýšit produktivitu.[1] Podle Zprávy Index pracovních trendů 2024 od Microsoftu mnoho zaměstnanců hledá nástroje generativní AI, aby tuto mezeru zaplnili, aniž by před jejich použitím čekali na oficiální schválení IT oddělením.

Když nástroje fungují mimo viditelnost IT oddělení, mohou představovat rizika pro organizace související se zabezpečením a dodržováním předpisů. Stínová AI – používání nástrojů AI bez schválení IT oddělením – se stává nejnovější formou stínového IT na dnešních pracovištích.

S rostoucím zaváděním AI se vedoucí pracovníci snaží udržet si náskok a zmírnit potenciální rizika, která tyto nástroje mohou představovat. V nedávné studii iSMG více než 70 % oslovených vedoucích pracovníků uvedlo, že zajištění ochrany soukromí a zabezpečení dat představuje hlavní výzvu při integraci generativní AI do stávající IT infrastruktury.[2] Navíc více než 90 % dotázaných CIO a CTO uvedlo, že generativní AI již podnítila nebo podnítí zvýšené investice do kybernetického zabezpečení v jejich organizaci.[3]

V této e-knize se seznámíte s běžnými scénáři využití stínové AI, porozumíte možným rizikům pro organizace, dozvíte se pět způsobů, jak tato rizika řídit, a zjistíte, jak vám může pomoci řešení Microsoft 365 E3.



[1] **Výroční zpráva Index pracovních trendů 2025,** Microsoft, Inc., duben 2025. Společnost Microsoft analyzovala data z průzkumu, do kterého se mezi 6. únorem 2025 a 24. březnem 2025 zapojilo 31 000 zaměstnanců na plný úvazek nebo samostatně výdělečně činných znalostních pracovníků z 31 zemí, trendy na trhu práce podle LinkedIn a biliony signálů produktivity z Microsoft 365.

[2] **iSMG Second Annual Generative AI Study: Business Rewards vs. Security Risks,** na základě odpovědí z průzkumu od více než 360 odborníků v oblasti obchodu a kybernetického zabezpečení ve třetím čtvrtletí v 6 regionech (Severní Amerika, Evropa, Asie, Jižní Amerika, Austrálie a Afrika).

[3] **The AI Security Balancing Act: From Risk to Innovation, NTT DATA, červen 2025,** na základě dat z průzkumu společnosti NTT DATA, do kterého se zapojilo více než 2 300 vedoucích pracovníků s rozhodovací pravomocí v oblasti GenAI, včetně 1 500 vedoucích pracovníků z 34 zemí.

Co je stínová AI? A proč je důležitá viditelnost?

Stínová AI odkazuje na používání nástrojů a aplikací s AI zaměstnanci bez výslovného souhlasu nebo dohledu ze strany IT oddělení, často mimo dohled oficiálních rámců zabezpečení a dodržování předpisů. Protože se zaměstnanci snaží zvýšit produktivitu a zvládnout rostoucí pracovní zátěž, mohou sáhnout po těchto neschválených řešeních ke zjednodušení práce, spolupráci nebo vytváření nového obsahu – často bez povědomí o možných rizicích. Stínová AI není pro IT oddělení viditelná, což organizacím komplikuje zjištění, které aplikace se používají a které z nich představují největší riziko.

Proč je viditelnost stínové AI důležitá?

Pokud IT oddělení o aplikaci nebo službě neví, nemůže ji zabezpečit ani podporovat. Tento *nedostatek viditelnosti* ztěžuje přesnou identifikaci, správu nebo zmírnění potenciálních hrozeb souvisejících s únikem citlivých dat, nedodržením předpisů a ztrátou kontroly nad proprietárními informacemi. IT a vedoucí pracovníci musí získat přehled o stínové AI používané v organizaci, řešit nově vznikající rizika spojená s využíváním AI a rozhodnout, které nástroje budou povoleny s odpovídajícími kontrolními mechanismy. Organizace mají příležitost proměnit stínovou AI z rizika na šanci pro bezpečnou inovaci pracovních procesů. K tomu je zapotřebí lepší rovnováha – umožnit zaměstnancům využívat užitečné nástroje AI v řízeném a bezpečném rámci ke zmírnění potenciálních rizik.

PŘEHLED

Nemůžete zabezpečit to, co nevidíte. Pokud IT oddělení nemá přehled o používaných aplikacích nebo službách, nemůže je zabezpečit. To je jádro problému stínové AI – a zdůrazňuje to, proč je zapotřebí nový přístup. Pouhý zákaz všech externích nástrojů není praktický, pokud zaměstnanci považují tyto nástroje AI za nezbytné pro dosažení svých cílů. Organizace musí naopak stínovou AI vynést na světlo – získat přehled o tom, co zaměstnanci používají, zavést vhodné kontrolní mechanismy a nabídnout bezpečné, schválené alternativy, které splňují potřeby organizace. Stručně řečeno, výzvou je vybavit týmy AI *bez* ohrožení zabezpečení.

Stínová AI na pracovišti: Příkladové scénáře a potenciální rizika

Stínová AI vychází od zaměstnanců, kteří chtějí zvýšit svou produktivitu a efektivitu nebo vyzkoušet novou technologii. Níže uvádíme několik fiktivních příkladů, které ilustrují, jak mohou být neschválené nástroje AI používány a jaká potenciální rizika mohou přinášet:

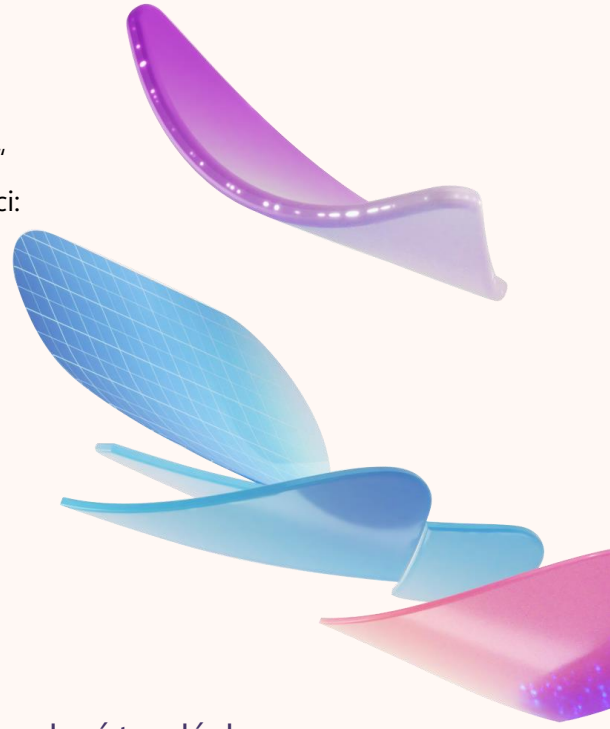
Role	Příkladový scénář	Potenciální rizika neschválených nástrojů
Marketingové oddělení	Použití nástroje generativní AI pro tvorbu marketingových textů nebo návrhů s využitím dat značky společnosti.	Únik citlivých informací o značce nebo produktu; ztráta kontroly nad tím, jak může externí služba AI ukládat nebo používat kreativní aktiva společnosti.
Finanční oddělení	Nahrávání firemních finančních údajů do analytické nebo vizualizační služby založené na AI pro získání rychlého přehledu.	Vystavení důvěrných finančních údajů (rozpočtů, prognóz) třetí straně; možné porušení předpisů o ochraně osobních údajů (např. GDPR), pokud jsou zahrnuta data zákazníků nebo zaměstnanců bez dostatečných ochranných opatření.
Zákaznická podpora	Sdílení dat klientů nebo přepisů chatů podpory v nástroji AI za účelem přípravy odpovědí nebo shrnutí případů.	Porušení pravidel ochrany osobních údajů a správy dat – citlivé informace o zákaznících mohou být uloženy mimo firemní systémy; není zaručeno uchovávání dat ani jejich řádné odstranění poskytovatelem AI.
První kontakt – maloobchod	Manažeři prodejen používají na svých telefonech aplikace s AI pro optimalizaci rozpisu směn zaměstnanců.	Data o zaměstnancích společnosti (jména zaměstnanců, rozvrhy) byla nahrána do neschválené aplikace, což znamená riziko porušení ochrany osobních údajů. Pokud návrhy AI nejsou v souladu s pracovními předpisy, může dojít ke konfliktům v rozvrhu nebo k porušení zásad.
První kontakt – zdravotní péče	Zdravotní sestry nebo lékaři používají AI chatbota, který jim pomáhá sepsat zdravotní záznamy pacientů nebo odpovídat na lékařské otázky.	Informace o zdravotním stavu pacientů (PHI) mohou být zpřístupněny externí službě bez jakýchkoli záruk, což porušuje požadavky na dodržování předpisů a důvěrnost. Lékařské rady AI mohou být také neověřené, což představuje bezpečnostní riziko.

V každém z výše uvedených případů měl konkrétní zaměstnanec dobré úmysly a snažil se zvýšit produktivitu, ale organizace tím může nést určitá rizika.

Informace společnosti mohou být roztříštěny na neschválených platformách, což způsobuje *problémy s řízením dat*. Neprověřené aplikace mohou obsahovat malware nebo bezpečnostní chyby, čímž rozšiřují potenciální oblast útoku mimo působnost IT oddělení. Může to mít také důsledky pro dodržování předpisů. Z pohledu IT podpory: pokud dojde k problému s nástrojem stínové AI, helpdesk nemusí být schopen pomoci koncovým uživatelům, protože nemá nad tímto nástrojem žádný přehled ani kontrolu.

Pět způsobů, jak řídit rizika stínové AI

Díky správné strategii a nástrojům můžete proměnit stínovou AI z potenciální hrozby na příležitost k posílení kultury bezpečných inovací. Poskytněte svým týmům nástroje AI pro zvýšení produktivity a *zároveň* zachovejte dohled potřebný k ochraně vaší firmy. Jedná se o posun od postoje „ne, nikdy“ k postoji „ano, ale s patřičnými bezpečnostními opatřeními“. Následujících pět tipů vám pomůže spravovat a kontrolovat stínovou AI ve vaší organizaci:



01 Zjištění stopy stínové AI pro vyhodnocení a stanovení priorit rizik

Nemůžete chránit to, co nevidíte. Získejte přehled o aplikacích používaných ve vaší organizaci prostřednictvím protokolů aktivit. Jakmile budete znát používané aplikace, můžete identifikovat správné nástroje pro zpracování citlivých dat a zároveň upozornit na ty, které nejsou v souladu s vašimi zásadami zabezpečení a dodržování předpisů. Díky těmto přehledům můžete učinit informovanější rozhodnutí o tom, které aplikace chcete povolit, sledovat nebo omezit, abyste zmírnili potenciální rizika.

02 Implementace rychlých řešení pomocí zásad zabezpečení a dodržování předpisů

Povolte nebo použijte opravy zásad, abyste lépe zmírnili potenciální rizika vyplývající z používání stínové AI. Pomocí zásad podmíněného přístupu můžete omezit používání rizikových aplikací, pomocí zásad prevence ztráty dat pro citlivé informace můžete omezit nadměrné sdílení a únik dat a pro všechny uživatele můžete vynutit základní vícefaktorové ověřování a dodržování předpisů zařízení. Tyto kroky rychle snižují nejzávažnější rizika, i když ještě nemáte úplný přehled o používaných aplikacích s AI.

03 Poučení zaměstnanců o potenciálních rizicích stínové AI

Zaměstnanci si často nejsou vědomi rizik, která může používání neschválených nástrojů AI představovat pro organizaci. Informujte uživatele o rizicích stínové AI pomocí vhodně umístěných varování ochrany před únikem informací, připomínek firemních zásad a krátkých školení, která jim pomohou přejít na bezpečnější postupy bez nutnosti přísného vynucování.

04 Poskytnutí schválených nástrojů AI pro další snižování rizik

Pokud je to možné, nabídněte zaměstnancům schválené nástroje AI jako alternativu k neschváleným nástrojům. Skvělým způsobem, jak omezit stínovou AI, je pokrýt nejběžnější případy použití ve vaší organizaci pomocí schváleného řešení. To umožňuje IT oddělení udržovat si přehled a kontrolu a zároveň poskytovat uživatelům podporu při řešení vzniklých problémů.

05 Zavedení trvalých zásad správného řízení

Integrujte kontroly do rutiny správy IT – pravidelně kontrolujte protokoly aktivit a hlášení, aktualizujte zásady podle nových služeb AI a informujte vedení o pokroku (například o snížení neoprávněného používání aplikací nebo zabránění incidentům). To vám pomůže zmírnit potenciální rizika nyní i v budoucnu, protože situace se neustále vyvíjí.

Provedením výše uvedených kroků můžete podpořit inovace i zabezpečení.

Zaměstnanci mohou využívat schválená řešení AI v práci, zatímco IT oddělení nad těmito nástroji udržuje kontrolu a zajišťuje dodržování předpisů.

Zjištění a správa rizik stínové AI pomocí služby Microsoft 365 E3

Microsoft 365 E3 poskytuje organizacím možnosti odhalit stínové IT, posoudit potenciální rizika a implementovat zásady zabezpečení a dodržování předpisů *bez* omezení inovací. Tato sada integrovaných funkcí pro produktivitu, zabezpečení a správu vám umožní přímo řešit výzvy spojené se stínovou AI.

Řešení Microsoft 365 E3	Jak pomáhá zvládat potenciální rizika stínové AI
Cloud App Discovery	**Zjistěte a přijměte opatření proti neschváleným aplikacím.** Cloud App Discovery vám umožňuje nahrávat protokoly aktivit a vytvářet přehledové zprávy, čímž získáte přehled o více než 31 000 cloudových aplikacích – včetně více než 400 aplikací generativní AI. Umožní vám zjistit, které aplikace se ve vaší organizaci používají, kdo je používá a jak často. Tyto informace vám umožňují činit informovaná rozhodnutí o tom, které aplikace povolit nebo omezit.
Ochrana před únikem informací Microsoft Purview (DLP)	**Minimalizujte úniky citlivých dat.** Ochrana před únikem informací Microsoft Purview DLP vám umožňuje definovat a používat zásady, které detekují citlivé informace a blokují nebo omezují sdílení e-mailů a souborů mezi službami Microsoft 365. Můžete například nastavit pravidlo, které bude monitorovat, auditovat nebo zastavovat sdílení citlivých informací uživateli prostřednictvím e-mailu či sdílení souborů a upozorňovat uživatele.
Microsoft Entra ID P1	**Spravujte přístup ke cloudovým aplikacím.** Microsoft Entra ID P1 umožňuje zásadám podmíněného přístupu řídit, kdo má za jakých podmínek přístup ke kterým aplikacím. Například můžete zvolit požadavek na vícefaktorové ověřování nebo dokonce omezit přihlašování pomocí firemních přihlašovacích údajů do aplikací, u kterých jste určili vyšší riziko. Microsoft Entra ID P1 poskytuje přístup ke cloudovým zdrojům správným osobám, na vyhovujících zařízeních, za schválených podmínek – a zároveň omezuje přístup k neschváleným aplikacím.
Microsoft Intune P1	**Vynucujte zásady používání zařízení a aplikací.** Microsoft Intune P1 vám umožňuje povolit používání spravovaných zařízení, která splňují požadavky pro práci, a poskytuje vám nástroje pro správu těchto zařízení. Může například zakázat instalaci neschváleného softwaru do firemních počítačů nebo nastavit konfigurace, které omezují přístup k určitým webům či službám.
Microsoft Defender for Endpoint P1	**Omezte provoz na neschválené adresy URL.** Microsoft Defender for Endpoint P1 pomáhá snižovat rizika spojená s weby, které považujete za rizikové, tím, že blokuje přenos dat na neschválené adresy URL ze spravovaných zařízení. Například zaměstnancům, kteří se pokoušejí navštívit známou rizikovou stránku AI na firemním notebooku, bude přístup na tuto stránku zablokován.

Další krok na cestě k přijetí AI →

Vše začíná povědomím, správnými nástroji a proaktivním plánem. Microsoft 365 E3 poskytuje nástroje, které vaší organizaci umožní vytvořit robustní základ zabezpečení a rámec zásad správného řízení pro řešení AI. Získáte přehled o neschválených nástrojích, budete moci zavést zásady na ochranu citlivých dat a udržet si kontrolu nad přístupem uživatelů i zabezpečením zařízení. Připravte se na přechod od reaktivního přístupu (vyhledávání a blokování stínové AI po jejím vzniku) k proaktivnějšímu přístupu, který povede k bezpečnému a řízenému využívání AI. Absolvujte posouzení zabezpečení pro AI a zjistěte, jak můžete zlepšit stav zabezpečení AI. Zjistěte více o funkcích zahrnutých v řešení Microsoft 365 pro firmy.