

Případ pro konsolidaci IT



Obsah

01

Rozrůstání IT se vymklo kontrole



02

Zbavte svůj tým IT
oddělených řešení



03

Síla jednoty



04

Ochrana využití AI



05

Jednotná platforma



06

Vedení s pomocí
konsolidace IT



Příležitost ke konsolidaci IT

Tato e-kniha je určena vedoucím pracovníkům v IT, kteří chtějí přestat vládnout chaosu a nastolit harmonii v oblasti IT infrastruktury, managementu a zaměstnanců. Zjistěte, jak zvýšit výkon, snížit složitost a náklady, zvýšit efektivitu, posílit zabezpečení a připravit vaši organizaci na AI prostřednictvím konsolidace na sjednocenou platformu.

01

Rozrůstání IT se vymklo kontrole

Pokud jde o správu digitálního ekosystému, může se zdát, že jednotná kontrola je nedosažitelná. **Splnění vyvíjejících se požadavků organizace týkajících se produktivity, zabezpečení a připravenosti na AI často znamená dávat dohromady řešení po jednotlivých nástrojích.** Tento přístup sice umožňuje udržet věci v pohybu, ale zároveň vytváří složitý IT systém, který je často nepropojený, časově náročný a jeho údržba je nákladná.

Týmy IT mohou být rychle zahlceny tímto komplexním a často nákladným souborem nástrojů pro správu koncových bodů, správu identit a přístupu, zasílání zpráv, e-mailů, produktivity – seznam je dlouhý. Různé nástroje často znamenají různé dodavatele s jedinečnými požadavky a izolovanými prostředími. Není divu, že máme pocit, že rozpočty a zdroje jsou napjaté.

Složitost představuje výzvu pro celou organizaci. Produktivita klesá, když zaměstnanci tráví den používáním několika přihlašovacích údajů a snaží se sdílet informace v oddělených nástrojích. Vzhledem k tomu, že se snaží přistupovat ke zdrojům z různých zařízení a míst, ztěžuje roztržštěná správa koncových bodů týmům IT udržování zabezpečení. Je čas sjednotit IT nástroje a zjednodušit správu.

Ekosystém specializovaných IT nástrojů a dodavatelů se neustále rozrůstá, a to velmi rychle.



Přestaňte platit daň za složitost

Každá nová softwarová licence se řídí podobným vzorem: další řešení, další nákladové středisko, další vrstva složitosti. Vedoucí pracovníci IT musí s omezeným rozpočtem zvládnout mnoho úkolů a nějakým způsobem najít zdroje na podporu nových iniciativ v oblasti AI. Aby udrželi rozpočet pod kontrolou, musí mnozí vedoucí pracovníci v oblasti IT neustále vyhodnocovat svou infrastrukturu z hlediska duplicitních a nepoužívaných licencí. V roce 2024 vedoucí pracovníci v oblasti IT usilovali o úspory následujícími způsoby:

83 % snížilo náklady na nepoužívaný software²

82 % zlepšilo vyjednávání smlouvy s **dodavatelem**²

79 % zakoupilo levnější možnosti licencí²

Tyto strategie mohou přinést mírné úspory, ale má to háček. Správa této rostoucí mozaiky aplikací vytváří „daň za složitost“. Audit nástrojů a odstraňování nefunkčních funkcí při správě zabezpečení a nastavení přístupu k nesouvisejícím řešením vyžaduje drahocenný čas a personál. Místo toho, aby se IT týmy soustředily na práci s velkým dopadem, tráví drahocenný čas auditem licencí, vyjednáváním s dodavateli a hledáním přírůstkových úspor při individuální údržbě každého existujícího řešení. Tyto časově náročné úkoly odvádějí pozornost od smysluplnější práce.

Navzdory těmto opatřením na snížení nákladů se náklady na složitost postupně zvyšují. Jedinou udržitelnou cestou je přehodnotit přístup k technologiím. Konsolidace na komplexní platformu sníží složitost a umožní týmům soustředit se na transformaci podniku.

15 %

organizací zaplatilo více než 5 milionů USD za **audity dodavatelů softwaru** za poslední 3 roky²

61 %

odborníků na správu IT majetku uvádí, že **stále nemá úplný přehled** o IT majetku, který má dopad na obchodní výsledky²

02

Zbavte svůj tým IT oddělených řešení

Pro organizace s rozsáhlou sadou technologických nabídek je každodenní realita práce s IT vyčerpávající. Každé specializované řešení vyžaduje vlastní odborné znalosti. Technologický ekosystém se stává bludištěm neintegrovaných nástrojů.

IT týmy jsou přetíženy všemi úkoly správy, údržby, integrace a podpory. Každý specializovaný nástroj vyžaduje praktickou správu, takže budete potřebovat více specialistů s úzkou kvalifikací, abyste mohli udržovat systémy v provozu. Již nyní **64 %** vedoucích pracovníků IT hlásí problémy při náboru kandidátů kvůli nedostatku potřebných dovedností nebo zkušeností.³ To vám ztěžuje přijetí, zaškolování a udržování odborných znalostí v týmu.



03

Síla jednoty

Existuje lepší přístup ke správě IT. Konsolidací na jednotné řešení můžete snížit přetížení IT a udržet silný, flexibilní a soustředěný tým. To vám umožní:

Zefektivnění správy uzavírání smluv s dodavateli, údržby a provozu.

Zvýšení produktivity zrychlením podpory a správy požadavků.

Proaktivní zabezpečení IT prostředí pomocí jednotné viditelnosti a správy.

Nejde jen o zefektivnění systémů. Jde o uvolnění cesty pro to nejdůležitější: umožnit vašemu týmu utvářet budoucnost fungování vaší organizace.

Minimalizace digitálních problémů

Technologie by měly pomáhat uvolnit cestu vpřed, nikoli vytvářet překážky. Jako vedoucí pracovník IT víte, že **nesoulad mezi nástroji pro produktivitu ovlivňuje celou organizaci**.

Šedesát dva procent lidí říká, že se během pracovního dne potýkají s příliš velkým množstvím času stráveného hledáním informací.⁵ Průměrný zaměstnanec dnes tráví **57 %** svého pracovního dne schůzkami, e-maily a chaty. Není divu, že **68 %** lidí říká, že nemají dostatek času bez vyrušování na intenzivní práci.⁵

Nesouvisející bodová řešení vytvářejí v každodenních pracovních postupech nenápadné překážky, ale frustrace přichází rychle. Vícenásobné přihlašování, oddělená práce, rozptýlené informace, systémy, které nefungují společně – každý třetí bod je malou daní za kreativitu a inovace.

Konsolidací na jedné platformě můžete tyto překážky snížit a vytvořit prostor pro vznik hodnotné kreativity. Představte si, jak se vaše organizace proměnila díky konsolidaci. Pracovníci využívají centrální zabezpečenou bránu pro přístup ke všem nástrojům a zdrojům, které potřebují. Informace volně proudí a spolupráce probíhá přirozeně.

Když třenice zmizí, lidé znovu objeví schopnost smysluplnější práce. Nejde jen o odstraňování překážek – jde o vytvoření prostředí, kde technologie umocňují to, co lidé mohou dělat.



Centralizace zabezpečení

Prostředí kybernetických hrozeb je složitější než kdykoli předtím. Špatní aktéři mají lepší zdroje, jsou sofistikovanější a vyzbrojeni taktikami, které jsou výzvou i pro nejlépe připravené bezpečnostní týmy. Vzhledem k tomu, že bezpečnostní hrozby se stávají stále sofistikovanějšími, je stále těžší s nimi držet krok. **Osmdesát procent** organizací má vektory útoku, které odhalují kritické majetky.⁶ **Osmdesát dva procent** vedoucích pracovníků v oblasti zabezpečení bylo překvapeno selháním zabezpečení, které uniklo kontrole, o níž si mysleli, že je zavedena.⁷

Organizace nyní vynakládají **65 %** svých rozpočtů na zabezpečení na produkty třetích stran, zatímco pouze **35 %** jde na interní pracovníky.⁸

Co je hnacím motorem těchto nerovnoměrných výdajů? Velké podniky často spravují širokou škálu nástrojů, aby si zajistily nejlepší řešení pro každý konkrétní úkol, i když to znamená žonglování s větší sadou nástrojů. Tento přístup může vést ke zvýšeným výdajům a složitosti.

600 mil. útoků kyberzločinců se odehrálo denně v roce 2024⁶

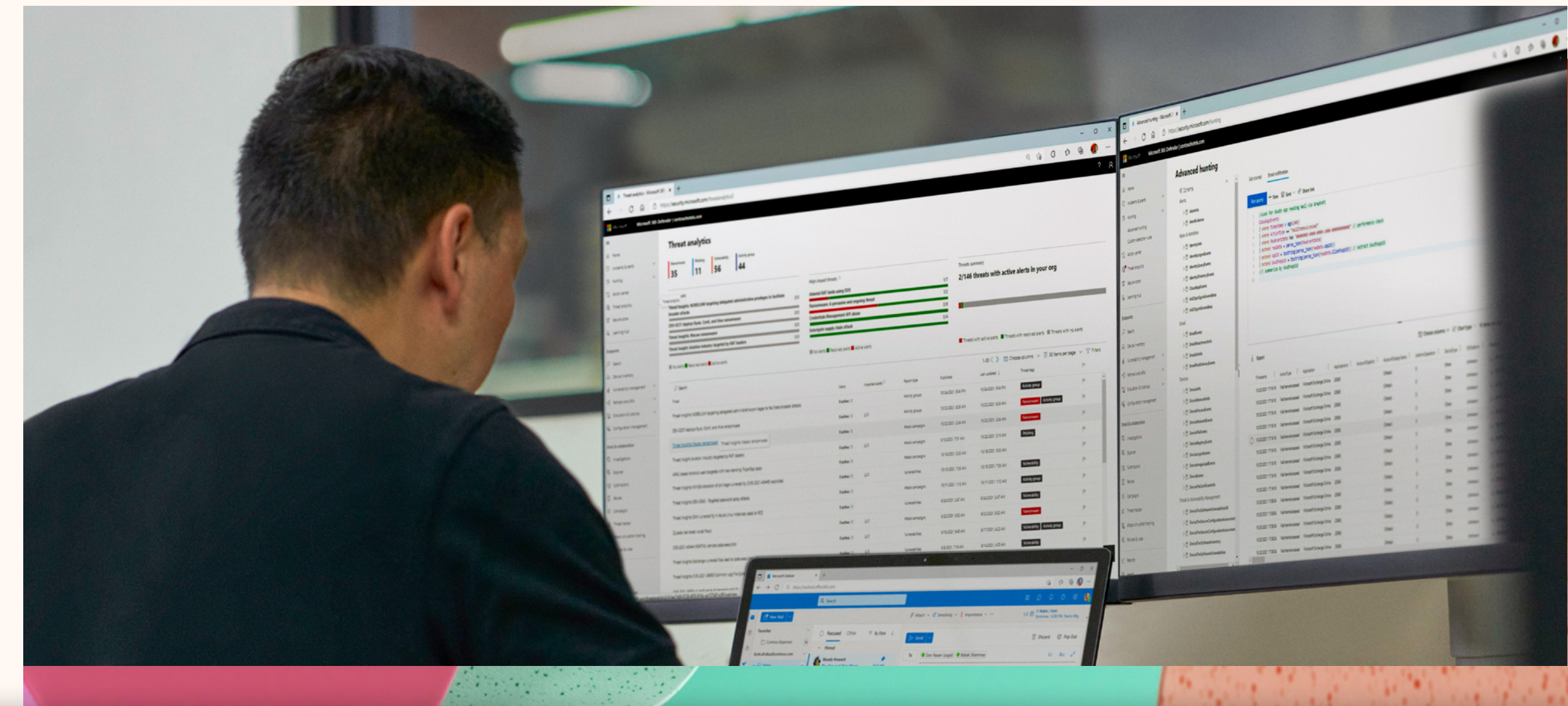
2,75x meziroční nárůst počtu případů ransomwaru řízeného člověkem⁶

V reakci na rostoucí hrozby přidávají týmy zabezpečení další řešení.

19 % Dvouletý průměrný nárůst počtu bezpečnostních nástrojů, které velké podniky používají.⁷

Přidání dalších bezpečnostních nástrojů se může jevit jako vytvoření silnější obrany organizace. Honba za větším počtem řešení však může ve skutečnosti způsobit, že vaše organizace bude zranitelnější. Složitité IT prostředí s mnoha vzájemnými závislostmi je těžší pochopit, spravovat a zabezpečit. Přetížení nástroji vám brání v získání jasného pohledu na sadu technologií v celém podniku. Vytváří také větší potenciální plochu pro útoky s větším počtem „postranních vrátek“ do podnikových systémů.

Konsolidací zabezpečení na komplexní platformě změníte složitost v přehlednost. To znamená jasný pohled na celé vaše digitální prostředí. Nejsilnější zabezpečení nespočívá v rostoucí kolekci různých nástrojů. Vznikne, když vytvoříte správný základ s centrální platformou.



04

Ochrana využití AI

Zaměstnanci chtějí, aby jim AI ulehčila práci.

75 % zaměstnanců **používá AI** při práci.⁹

78 % pracovníků využívajících AI **přináší do práce své vlastní nástroje s AI**.⁹

Zaměstnanci nečekají, až protokoly zabezpečení doženu vývoj. S rostoucí oblibou nástrojů typu BYOAI (Bring your own AI) mohou organizace zaostávat. Pouze **24 %** iniciativ v oblasti generativní AI zahrnuje robustní bezpečnostní opatření.¹⁰

Pokud organizace nevytvoří správný základ pro bezpečné používání AI, mohou zaměstnanci zaplnit mezeru v produktivitě pomocí stínové AI: neschválené nástroje, které existují mimo vaše systémy a mimo vaši kontrolu.

Stínová AI vytváří dvě klíčové výzvy:

Bez dohledu

Stínová AI otevírá dveře vážným rizikům; co brání zaměstnancům v tom, aby kopírovali citlivé informace do svého osobního nástroje AI? Každá interakce s nekontrolovanou BYOAI se stává dalším bezpečnostním rizikem. Vaše data mohou uniknout nebo mohou být použita k trénování externího modelu.

Omezená užitečnost

Sedmdesát devět procent zaměstnanců by se cítilo pohodlně při používání AI pro analytické úkoly,⁵ ale nástroj AI je jen tak dobrý, jak dobré jsou informace, které má k dispozici. Segmentované, izolované nástroje AI často poskytují neúplné odpovědi. Proto mají nástroje BYOAI pro pracovníky jen omezený přínos.





Organizace se nyní nachází na křižovatce: nechat roztržštěné používání AI roztočit spirálu, která může vést k potenciálním bezpečnostním selháním, nebo převzít kontrolu a přijmout jednotnou platformu připravenou na AI. Jako vedoucí pracovníci v oblasti IT máte klíčovou strategickou příležitost provést svou organizaci tímto kritickým okamžikem. Využijte plný potenciál AI v celé organizaci díky podnikové sadě, která spojuje aplikace pro zvýšení produktivity, zabezpečení a zajištění dodržování předpisů – vše navrženo pro bezproblémovou integraci AI.

Konsolidovaná platforma umožňuje efektivně nasazovat správné nástroje pro snížení rizik spojených s používáním AI a ochranu vašich dat. Konsolidace také pomáhá lépe nasazovat a spravovat bezproblémové a zabezpečené propojení mezi řešením AI vaší organizace a proprietárními daty, zdroji a pracovními postupy. Vaše řešení s AI tak může poskytovat přesné a prakticky použitelné poznatky, které zaměstnanci potřebují k tomu, aby mohli vykonávat práci s vysokým dopadem.

Jednotná platforma

Microsoft 365 E3 je jednotná platforma, která zjednodušuje správu IT, zvyšuje produktivitu vaší organizace prostřednictvím propojených prostředí, zabezpečuje nástroje a koncové body a umožňuje bezproblémovou integraci s AI.

Výhody konsolidace pomocí služby Microsoft 365 E3

Snížení nákladů na IT

Vyberte si komplexní řešení, které zjednodušuje správu z cloudu a konsoliduje dodavatele, aby se minimalizovaly celkové náklady a zlepšila návratnost investic.

Ochrana organizace

Zabezpečte přístup k datům, aplikacím a prostředkům pomocí centralizovaného řešení pro ochranu před hrozbami, silného vícefaktorového ověřování, zásad podmíněného přístupu a nepřetržitého vyhodnocování přístupu.

Bezpečné zavedení generativní AI

Vybudováním zabezpečeného základu s komplexní platformou, která udržuje soukromí a zabezpečení dat, bude vaše organizace připravena nasadit AI s nástrojem Microsoft 365 Copilot.

Překonání složitosti IT

Centralizujte správu aplikací, koncových bodů a identit a zároveň omezte bodová řešení pro produktivitu – kontrolujte přístup a používání bez přerušení toku práce v organizaci.

Konsolidací svého ekosystému IT pomocí Microsoft 365 E3 si zvolíte bezpečnější a produktivnější způsob práce. Tato komplexní platforma vybaví váš tým IT a celou vaši organizaci tak, aby dokázala čelit všem dalším výzvám.

Vedení s pomocí konsolidace IT

Dnešní tempo rozrůstání IT již není udržitelné. Konsolidace digitálního ekosystému není jen strategickým krokem, ale je zásadní pro snížení nákladů, zjednodušení správy, zvýšení produktivity a posílení zabezpečení. Sjednocením nástrojů a procesů umožníte své organizaci pracovat efektivněji, rychleji inovovat a s jistotou využívat AI.



Zdroje:

¹ „The state of observability in 2024“ Dynatrace, 2024.
<https://www.dynatrace.com/info/reports/state-of-observability-2024/>

² „2024 State of ITAM Report“ Flexera, 2024.
<https://info.flexera.com/ITAM-REPORT-State-of-IT-Asset-Management>

³ „Challenges in recruiting employees in the IT industry worldwide 2023“ Statista, 5. prosince, 2023.
<https://www.statista.com/statistics/1425097/recruitment-challenges-in-the-tech-industry-worldwide/>

⁴ „Is IT Complexity Standing in the Way of Your Organization’s Growth?“ Harvard Business Review, 9. prosince, 2022.
<https://hbr.org/sponsored/2022/12/is-it-complexity-standing-in-the-way-of-your-organizations-growth>

⁵ „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>

⁶ „Zpráva společnosti Microsoft o digitální obraně 2024“, Zabezpečení od Microsoftu, 2024.
<https://www.microsoft.com/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024>

⁷ „2022 Security Leaders Peer Report“ Panaseer, 2022.
<https://panaseer.com/resources/reports/2022-security-leaders-peer-report>

⁸ „The cybersecurity provider’s next opportunity: Making AI safer“ McKinsey & Company, 14. listopadu 2024.
<https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cybersecurity-providers-next-opportunity-making-ai-safer>

⁹ „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>

¹⁰ „Cost of a Data Breach Report 2024,“ IBM, 2024.
<https://www.ibm.com/reports/data-breach>

¹¹ „Zabezpečení dat jako základ pro bezpečné zavedení AI“, Zabezpečení od Microsoftu, 2024.
<https://clouddamcdnprodep.azureedge.net/gdc/gdckHueRY/original>

© 2025 Microsoft Corporation. Všechna práva vyhrazena. Tento dokument je poskytován „tak, jak je“. Informace a názory v něm vyjádřené včetně webových adres a dalších odkazů na webové stránky mohou být bez předchozího upozornění změněny. Nesete veškerá rizika vyplývající z jeho používání. Tento dokument vám neuděluje žádné právní nároky k duševnímu vlastnictví k žádným produktům společnosti Microsoft. Tento dokument smíte kopírovat a používat pro své interní referenční účely.