



Spravovanie a zabezpečenie prístupu k aplikáciám so službou **Azure Active Directory**



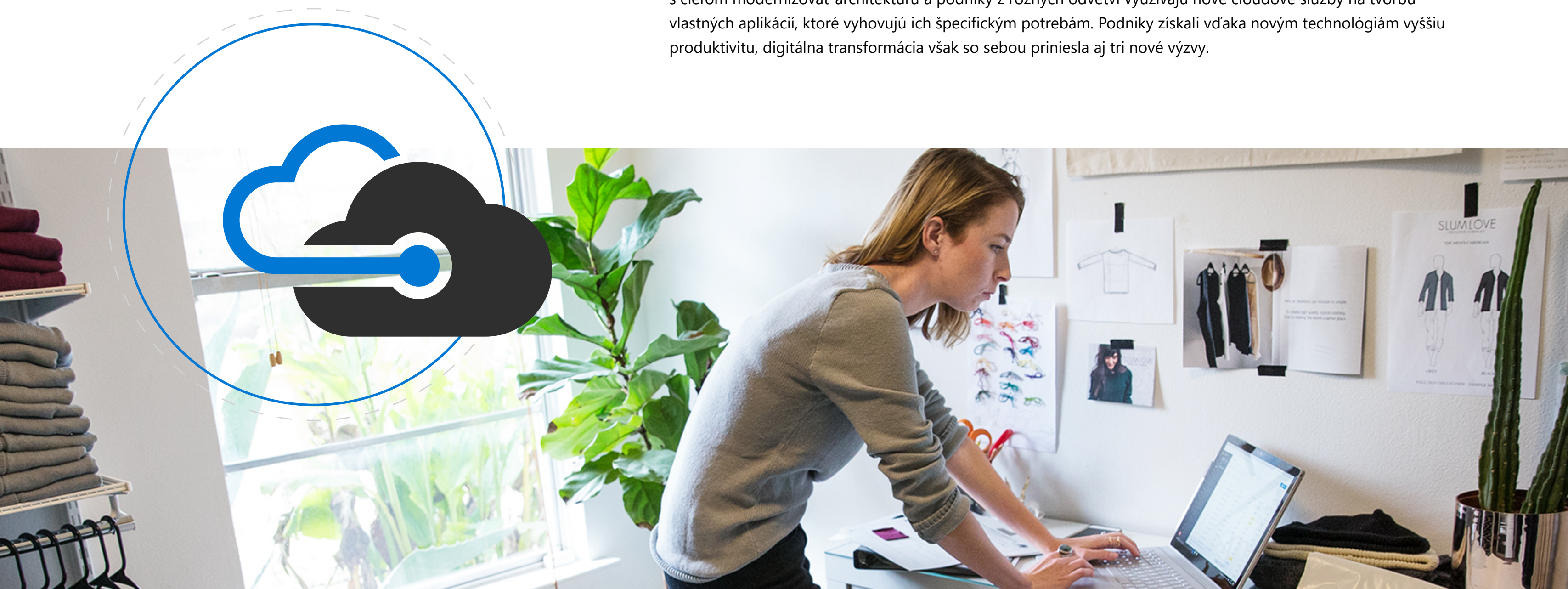
Sekcia 1

Čo je správa
identít a prístupu?

Čo je správa identít a prístupu?

Digitálna transformácia

Cloud computing a mobilné zariadenia transformovali moderné pracovisko. Čoraz vyšší počet pracovníkov po celom svete má možnosť flexibilne pracovať z ľubovoľného miesta pomocou aplikácií poskytovaných vo forme služby (Software as a service, SaaS), ktoré sú bezplatné alebo len s nízkymi nákladmi. Pomáhajú tak riešiť výzvy súvisiace s produktivitou a spoluprácou. Veľké podniky migrujú aplikácie a výpočty do cloudu s cieľom modernizovať architektúru a podniky z rôznych odvetví využívajú nové cloudové služby na tvorbu vlastných aplikácií, ktoré vyhovujú ich špecifickým potrebám. Podniky získali vďaka novým technológiám vyššiu produktivitu, digitálna transformácia však so sebou priniesla aj tri nové výzvy.



Čo je správa identít a prístupu?

Nové výzvy

Výzvy v súvislosti
s digitálnou
transformáciou

Bezpečnostné riziko: Pred nástupom cloudovej revolúcie bolo úlohou IT oddelenia „strážit“ technológie. Aplikácie a platformy, ktoré ste spravovali a mali zabezpečené, sa nachádzali v rámci siete a každý, kto sa prihlasoval k podnikovým zdrojom, najprv prešiel overením prostredníctvom brány firewall. Tieto časy sú však preč. Pracovníci majú vyššiu mieru kontroly nad technológiami, ktoré používajú, pričom väčšina z nich je prístupná cez internet. Kybernetickí útočníci sa naučili využiť tieto zraniteľné miesta. Dokonca ani vtedy, keď používateľ pozná správne heslo ku kontu, nemôžete mať istotu, že je skutočne tým, za koho sa vydáva.

Administratívne zaťaženie: Výrazný nárast počtu koncových bodov poskytuje používateľom viac možností pripojenia, správcom však spôsobuje vrásky na čele. Mnohé podniky nedokážu evidovať všetky nástroje, ktoré zamestnanci používajú, dokonca aj keď majú dobrú evidenciu inventára. Už len samotné množstvo cloudových aplikácií znamená, že musíte spravovať niekoľko systémov identít, čo zvyšuje náklady a znásobuje existujúce bezpečnostné riziká.

Horšie možnosti pre používateľov: Používatelia sú zasiahnutí tiež. Majú radi flexibilitu, ale sú znechutení množstvom prihlasovacích údajov, ktoré si musia pamätať.



Bezpečnostné riziko



Administratívne
zaťaženie



Horšie možnosti
pre používateľov

Čo je správa identít a prístupu?

Správa identít a prístupu ako centrálna riadiaca časť

Riešenia správy
identít a prístupu
riešia tieto výzvy

Spoločným menovateľom všetkých uvedených kritických problémov sú neefektívne systémy na overovanie identity. Identita nahradila nárazníkovú sieť a prevzala na seba úlohu novej riadiacej časti. Potrebujete riešenia, ktoré spájajú rôznorodé nástroje, architektúru, zariadenia a služby v rámci podniku, aby lepšie chránili organizáciu a spravovali jednotný prístup do systémov správy identít a prístupu (identity and access management, IAM) pre zamestnancov aj externých partnerov v rámci jedného systému, čím získate lepšiu kontrolu. Poskytujú bezproblémovú spoluprácu aj mimo hraníc vašej organizácie a zároveň zvyšujú zabezpečenie firemných zdrojov. Vhodné riešenie správy identít a prístupu umožňuje pripojiť všetkých používateľov k pracovným aplikáciám prostredníctvom jednej množiny prihlasovacích údajov bez ohľadu na to, či sú umiestnené v cloude alebo lokálne. Riešenia správy identít a prístupu sú navrhnuté tak, aby používateľom poskytli prístup len k zdrojom, ktoré potrebujú, a zablokovali neoprávneným používateľom prístup k údajom, ku ktorým prístup mať nemajú. Prístupové práva a povolenia používateľov sa spravujú z centralizovaného portálu, čím sa do veľkej miery znižuje množstvo manuálnych procesov potrebných na zriaďovanie a rušenie zriaďovania používateľských kont. Riešenia správy identít a prístupu ponúkajú nástroje na spravovanie politik zabezpečenia v rámci identít a aplikácií. Tie najlepšie riešenia správy identít a prístupu dokážu lepšie chrániť identity, zlepšiť možnosti pre používateľov a zefektívniť spravovanie.



Lepšie zabezpečenie
identít



Lepšie možnosti
pre používateľov



Efektívnejšie
spravovanie

Sekcia 2

Prehľad služby Azure AD

Prehľad služby Azure AD

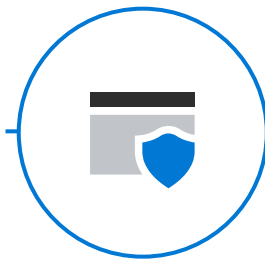
Komplexné riešenie

Microsoft Azure Active Directory (Azure AD) je komplexné riešenie správy identít a prístupu v cloude. Je lídrom na trhu v oblasti spravovania adresárov, prístupu k aplikáciám a rozšírenej ochrany identít. Azure AD umožňuje organizáciám spravovať a zabezpečiť identity zamestnancov, partnerov aj zákazníkov, aby mohli získať prístup k aplikáciám a službám, ktoré potrebujú. Azure AD pomáha miliónom organizácií spravovať a zabezpečiť viac ako jednu miliardu identít.



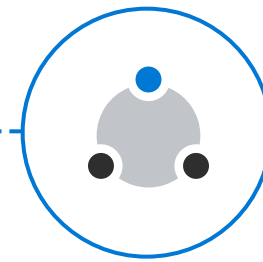
Modernizácia prístupu

Spravujte a zabezpečte prístup k údajom a zdrojom svojej organizácie lokálne aj v cloude. Pripojte všetkých používateľov, aplikácie a zariadenia do cloudu a získajte bezproblémový zabezpečený prístup a lepší prehľad aj kontrolu. Automatizujte pracovné postupy a povoľte samoobslužné možnosti, ktoré vám pomôžu udržať nízke náklady a zefektívniť prácu používateľov.



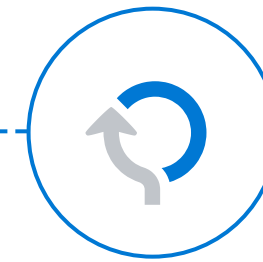
Zabezpečenie a riadenie

Každý deň dochádza k množstvu útokov na prihlasovacie údaje používateľov. Riešenie, ako predchádzať zneužitiu, spočíva v nepretržitom sledovaní normálneho a abnormálneho správania v rámci čo najširšej množiny signálov, použití umelej inteligencie a automatizácii odpovedí. Nájdite rovnováhu medzi produktivitou a zabezpečením so včasným prístupom k správnym zdrojom a s pravidelnými kontrolami prístupu a vynucovaním politiky.



Pripojenie a spolupráca

Rozšírte svoje podnikanie prostredníctvom spoľahlivej cloudovej služby, ktorá ponúka špičkové zabezpečenie a flexibilitu umožňujúcu škálovanie až na milióny používateľov. Spojte sa s externými používateľmi a podporte ich produktivitu pomocou jednoducho použiteľného samoobslužného prostredia a vstavaných kontrolných mechanizmov zabezpečenia.



Vývoj a integrácia

Vytvárajte aplikácie, ktoré používateľom umožnia jednoduché prihlásenie prostredníctvom ich osobného konta Microsoft, pracovného alebo školského konta či konta zo sociálnych médií. Začnite s pripojením k Microsoft Graphu, ktorý je bránou k údajom a funkciám inteligencie v službe Microsoft 365, a vytvárajte aplikácie so širokou ponukou možností. Povoľte jediné prihlásenie, automatizujte zriaďovanie používateľov a oslovte najväčšie svetové organizácie.

Sekcia 3

Azure AD pre
vaše aplikácie

Azure AD pre vaše aplikácie

Univerzálna platforma

Azure AD umožňuje spravovať spoločnú identitu jednotlivých používateľov v hybridnej infraštruktúre na prístup ku všetkým potrebným aplikáciám vrátane cloudových a lokálnych podnikových (LOB) aplikácií. Spravujte všetky identity prostredníctvom univerzálnej platformy, zvýšte efektivitu spravovania a získajte vyššiu mieru kontroly. Použite podrobné politiky zabezpečenia v rámci jednotlivých aplikácií používaných v organizácii.



Úspora času a peňazí

Služba Azure AD je vopred integrovaná v tisíckach aplikácií vrátane populárnych možností ako Workday, ServiceNow, SuccessFactors, Adobe a Concur. Vďaka tomu môžete tieto aplikácie jednoduchšie sprístupniť používateľom. Pomocou jednej konzoly nasadíte jednotné politiky a monitorujete prístupové práva. Môžete automatizovať pracovné postupy na zriaďovanie používateľov a spravovanie životného cyklu a ušetriť čas aj zdroje pomocou samoobslužného spravovania konta. Môžete tiež zahrnúť informácie o používateľoch z personálnych nástrojov ako jediného správneho zdroja, čím eliminujete potrebu tvorby vlastných skriptov alebo manuálnych procesov na spravovanie atribútov používateľov.

Aplikácie nakonfigurované prostredníctvom Azure AD povoľujú jediné prihlásenie (SSO) na bezproblémový prístup, čo znamená, že používatelia si nemusia pamätať samostatné prihlasovacie údaje pre každú aplikáciu ani opakovane používať slabé heslá a riskovať tým únik údajov. Kontá, ktoré boli nakonfigurované na automatické zriaďovanie, poskytujú používateľom včasný prístup k novým zdrojom. V prípade zriaďovania Azure AD zabezpečuje, aby mali noví zamestnanci hneď od prvého dňa prístup ku všetkým relevantným zdrojom.



**Šetrenie času
a peňazí**



**Vstavané
integrácie SaaS**



Jediné prihlásenie



**Prístup používateľov
od prvého dňa**

Azure AD pre vaše aplikácie

Lepšie zabezpečený prístup ku všetkým aplikáciám

Azure AD poskytuje komplexnú ochranu identít vo všetkých aplikáciách, SaaS aj lokálnych podnikových (LOB) aplikáciách. Nezáleží na tom, či používateľ žiada o prístup do Microsoft Wordu alebo Boxu, Azure AD zabezpečí, že pred udelením prístupu sa overí jeho identita. Môžete tiež zaviesť politiky riadenia prístupu, aby mali používatelia prístup len k aplikáciám, ktoré potrebujú, a vtedy, keď ich potrebujú. Môžete používateľom nastaviť, aby museli žiadať o povolenia na prístup, rovnako tiež môžete nastaviť časový limit, na ako dlho budú mať k aplikácii prístup. Pravidelne môžete kontrolovať dodržiavanie súladu pri prístupe.

Služba Azure AD tiež využíva výhody softvéru Microsoft Intelligent Security Graph a strojového učenia, čo umožňuje analyzovať miliardy signálov zo všetkých našich produktov a služieb, identifikovať atypické správanie a priradiť jednotlivým reláciám relatívnu mieru rizika. Azure AD berie pri vyhodnocovaní rizika prihlásenia do úvahy zariadenie, polohu a ďalšie kontextové informácie. Môžete zaviesť politiku podmieneného prístupu Azure AD, ktorá automaticky použije bezpečnostné opatrenia, ako napríklad blokovanie žiadosti o prístup alebo vyžadovanie resetovania hesla v prípade, že prihlásenie bude považované za riskantné alebo budú splnené konkrétne podmienky politiky.



Opatrenia na
zabezpečenie aplikácií



Ochrana
identity



Riadenie
prístupu



Politiky podmieneného
prístupu

Sekcia 4

Spravovanie a zabezpečenie aplikácií so službou Azure AD

Azure AD zjednodušuje udržiavanie kontroly a znižovanie nákladov pomocou automatizácie, samoobslužných možností a vynucovania politík.

Spravovanie a zabezpečenie aplikácií so službou Azure AD



Integrácia aplikácií Azure AD

Galéria aplikácií Azure AD umožňuje jednoducho nakonfigurovať a pripojiť ktorúkoľvek z tisícok vopred integrovaných aplikácií do nájomníka. Všetky tieto aplikácie podporujú používanie jediného prihlásenia a možno v nich jednoducho nakonfigurovať podmienený prístup Azure AD pre každú aplikáciu samostatne alebo ako súčasť politik v rámci celej organizácie. Keď aplikáciu pridáte a nakonfigurujete podľa potreby, používatelia s overeným prístupom ju môžu jednoducho nájsť na portáli Azure AD Moje aplikácie, centralizovanom portáli pre koncových používateľov na vyhľadávanie a spúšťanie aplikácií.

Ak ste vytvorili aplikáciu alebo potrebujete integrovanú aplikáciu pre svoju organizáciu, môžete tiež požiadať, aby bola uvedená v galérii aplikácií služby Azure AD.

[Preskúmať tisícky vopred integrovaných aplikácií >](#)



Zabezpečený prístup do hybridného prostredia

Azure AD Application Proxy umožňuje poskytovanie zabezpečeného vzdialeného prístupu k lokálnej webovej aplikácii založeného na deklarácii identity bez potreby použitia siete VPN. App Proxy vyžaduje inštaláciu zjednodušenej verzie konektora a IT oddeleniu aj koncovým používateľom poskytuje rovnaké prostredie ako SaaS aplikácie prepojené prostredníctvom galérie aplikácií služby Azure AD.

Ak chcete využiť investície do existujúcej infraštruktúry, napríklad s partnermi ako F5 ZScaler, SAP, Oracle alebo Ping Identity, a spojiť sa s ostatnými typmi aplikácií, napríklad tými, ktoré používajú overovací protokol založený na hlavičkách alebo overovací protokol Kerberos, máte aj túto možnosť. Naďalej pritom platí, že získate výhody centralizácie a zabezpečenia, ktoré Azure AD ponúka.

[Prečítať si, ako pridať lokálnu aplikáciu prostredníctvom protokolu App Proxy >](#)

[Pripojiť ďalšie siete a cloudy aplikácií od partnerov >](#)

Spravovanie a zabezpečenie aplikácií so službou Azure AD



Automatické zriaďovanie

Azure AD umožňuje automatizovať vytváranie, údržbu a odstraňovanie identít používateľov v obľúbených SaaS aplikáciách. Keď sa do vášho tímu alebo vašej organizácie zapoja noví ľudia, môžete im automaticky vytvoriť nové kontá v správnych systémoch. Pri odchode ľudí z tímu alebo organizácie môžete nastaviť politiky, ktoré automaticky deaktivujú ich kontá v príslušných systémoch. Automatizáciou týchto úloh môžete zabezpečiť, aby boli identity vo vašich aplikáciách a systémoch aktuálne a zodpovedali zmenám v adresári či systéme ľudských zdrojov. Znižuje sa tým riziko chýb a šetrí čas.

[Ďalšie informácie o nastavení automatizovaného poskytovania a rušenia poskytovania SaaS aplikácií >](#)



Správa skupín

Azure AD vám pomôže poskytovať prístup k zdrojom vašej organizácie tým, že udelíte prístupové práva buď jednému používateľovi, alebo celej skupine v službe Azure AD. Keď vlastník zdroja použije skupiny, môže nastaviť povolenia na prístup pre všetkých členov v danej skupine a nemusí práva udeľovať každému používateľovi samostatne. Tento spôsob je bezpečnejší, keďže je menej pravdepodobné, že niekomu omylom udelíte nevhodný prístup. Navyše sa týmto spôsobom šetrí čas. Správu skupín tiež môžete dynamicky škálovať automatizovanou registráciou prostredníctvom politik založených na atribútoch identity.

[Ako vytvoriť skupinu na portáli Azure >](#)

Spravovanie a zabezpečenie aplikácií so službou Azure AD



Použitie samoobslužných funkcií

Na dokončenie niektorých úloh sa nevyžadujú IT profesionáli – Azure AD vám umožňuje delegovať tieto úlohy na ostatných používateľov v organizácii. Používateľom môžete umožniť, aby v Azure AD vytvárali a spravovali vlastné skupiny zabezpečenia. Vlastníci skupín môžu schváliť alebo zamietnuť žiadosti o členstvo alebo môžu delegovať kontrolu nad členstvom v skupine.

[Nastaviť skupiny s vlastným spravovaním >](#)

Možnosti samoobslužných funkcií sa vzťahujú aj na používateľov. Používatelia si môžu zaregistrovať konto prostredníctvom samoobslužného portálu, stačí im na to overený e-mail. Pomocou portálu si tiež môžu resetovať heslo. Vďaka tomu môže vaše pracovisko technickej podpory ušetriť množstvo času a peňazí.

[Konfigurovať samoobslužné resetovanie hesla >](#)



Modernizácia overovania

Ak aktuálne používate lokálne overovanie, napríklad službu Active Directory Federation Services (AD FS), zvážte migráciu aplikácií do Azure AD. Používatelia budú môcť využívať rovnaké výhody, napríklad jediné prihlásenie, ale získajú aj výhody škálovania a zabezpečenia dostupné v cloude, ako napríklad použitie podrobných kontrolných mechanizmov prístupu pre jednotlivé aplikácie prostredníctvom podmieneného prístupu Azure AD alebo možnosť udeliť partnerom prístup k zdrojom v rámci spolupráce Azure AD B2B. Aplikácie, ktoré používajú štandardy SAML 2.0, WS-Federation, OAuth alebo OpenID Connect na federované prihlásenie, možno všetky migrovať.

[Vytvoriť politiky podmieneného prístupu Azure AD na zabezpečenie prístupu k aplikáciám >](#)

[Použiť Azure AD B2B na bezproblémovú spoluprácu s externými partnermi >](#)

Bezpečné pripojenie ľubovoľnej aplikácie v akomkoľvek cloude alebo na akomkoľvek serveri do Azure AD.

1 milión pripojených aktívnych jedinečných aplikácií.

Začnite už dnes.

[Začnite používať bezplatnú mesačnú skúšobnú verziu služby Azure AD](#) a zistite, aké jednoduché je zabezpečiť organizáciu a spravovať prístup používateľov ku všetkým aplikáciám.

