



Upravlajte pristupom aplikacijama koristeći **Azure Active Directory**



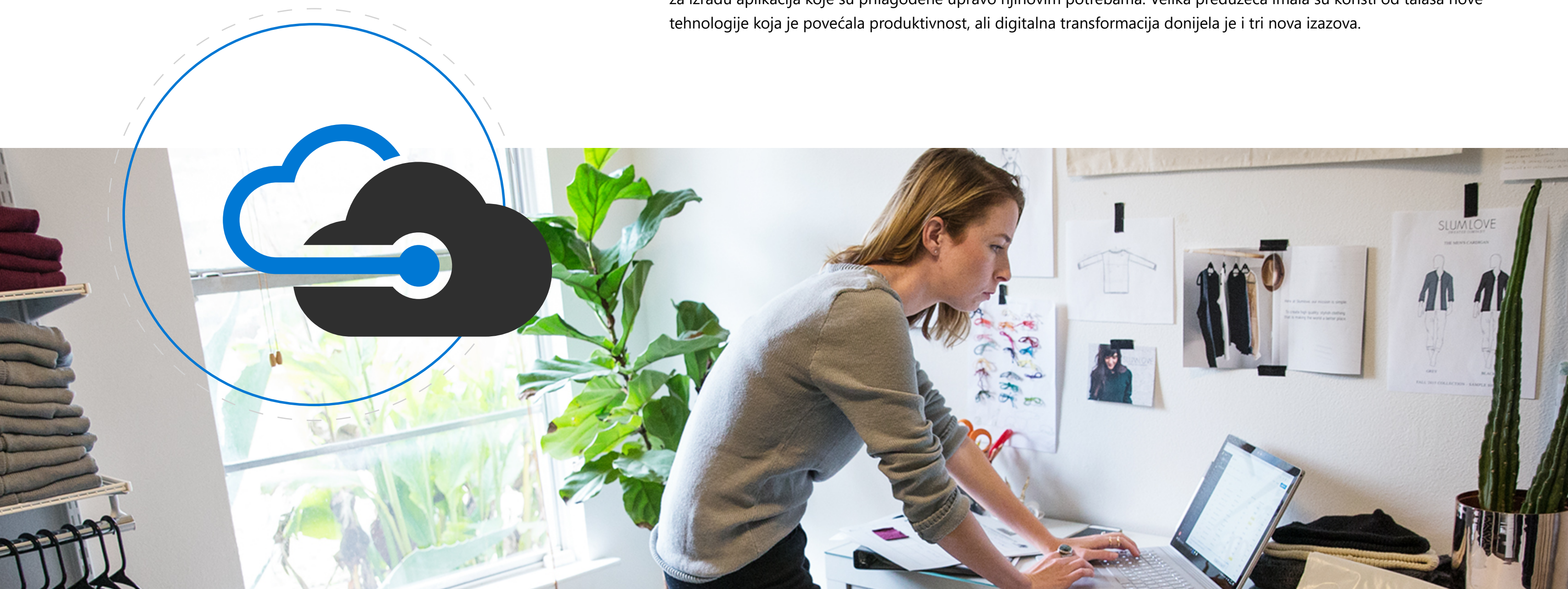
Odeljak 1

Šta je to upravljanje
identitetom i pristupom?

Šta je to upravljanje identitetom i pristupom?

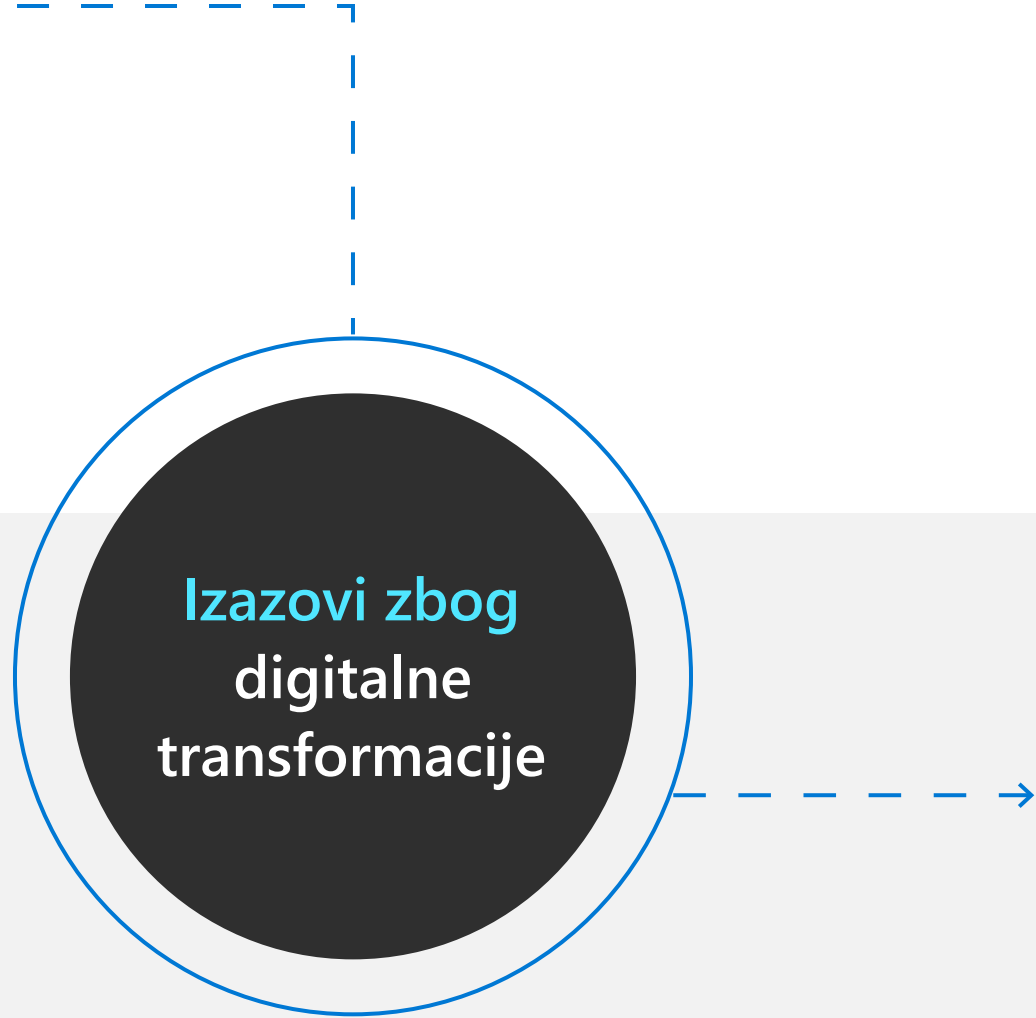
Digitalna transformacija

Računarstvo u oblaku i mobilni uređaji su transformisali moderno radno mesto. Svet rada sve više se globalizuje i dovoljno je fleksibilan da se raditi može s bilo kojeg mesta, pri čemu se izazovi na području produktivnosti i saradnje uspešno rešavaju besplatnim i povoljnim aplikacijama softvera kao usluge (SaaS). Velika preduzeća migriraju aplikacije i računarstvo u oblak da bi osavremenile svoju arhitekturu, a njihovi odseci koriste nove usluge u oblaku za izradu aplikacija koje su prilagođene upravo njihovim potrebama. Velika preduzeća imala su koristi od talasa nove tehnologije koja je povećala produktivnost, ali digitalna transformacija donijela je i tri nova izazova.



Šta je to upravljanje identitetom i pristupom?

Novi izazovi



Izazovi zbog
digitalne
transformacije

Bezbednosni rizik: pre revolucije u oblaku, IT je služio kao čuvar pristupa tehnologiji. Aplikacije i platforme koje ste štitili i kojima ste upravljali bile su zatvorene unutar granica mreže, a sve koji su se prijavili u resurse preduzeća morao je propustiti zaštitni zid. To je sada prošlost. Vaši zaposleni imaju veću kontrolu nad tehnologijom koju koriste, a velikom delu te tehnologije pristupa se putem interneta. Napadači na internetu naučili su kako da iskoriste te slabosti. Čak i kad korisnik zna pravu lozinku za pristup nalogu, ne možete uvek biti potpuno sigurni da se zaista radi o osobi koja se kao takva predstavlja.

Administrativno opterećenje: neverovatan rast broja krajnjih tačaka korisnicima omogućava mnogo više načina povezivanja, ali to je istovremeno i administrativna noćna mora. Mnoga preduzeća nisu svesna koje sve alate zaposleni koriste, a čak i kada imaju dobar pregled situacije, sama količina aplikacija u oblaku znači da morate upravljati većim brojem sistema identiteta, što povećava troškove i postojećim bezbednosnim rizicima dodaje nove.

Loše korisničko iskustvo: ni korisnicima nije lako. Iako vole fleksibilnost, frustrirani su brojem akreditiva koje moraju zapamtiti.



Bezbednosni rizik



Administrativno
opterećenje



Loše korisničko
iskustvo

Šta je to upravljanje identitetom i pristupom?

Upravljanje identitetima i pristupom kao središnja upravljačka osnova

Uobičajeni imenilac ovih problema jesu neefikasni sistemi za verifikaciju identiteta. Nekada je kao upravljačka osnova služila granica mreže, a sada tu ulogu preuzima identitet. Potrebna su vam rešenja kojima se povezuju različite alatke, arhitektura, uređaji i usluge na nivou preduzeća da bi organizacija bila zaštićenija i da bi se moglo upravljati pristupom zaposlenih i vanjskih saradnika. Sistemi za upravljanje identitetima i pristupom (IAM) objedinjuju pristupe, što omogućava bolju kontrolu. Oni vam omogućavaju neometanu saradnju izvan granica organizacije uz unapređenje zaštite poslovnih resursa. Dobro IAM rešenje vam omogućava da povežete korisnike sa svim njihovim aplikacijama za rad – bilo da su u oblaku ili lokalno – kroz jedan skup akreditiva. Rešenja za IAM osmišljena su tako da korisnicima omogućavaju pristup samo resursima koji su im potrebni i onemogućavaju korisnicima pristup podacima za koje nemaju ovlašćenje. Pravima pristupa i dozvolama za pristup upravlja se sa središnjeg portala, čime se smanjuje broj postupaka omogućavanja i onemogućavanja korišćenja korisničkih naloga koji se moraju obaviti ručno. Rešenja za IAM sadrže i alatke za upravljanje sigurnosnim pravilima primenjive za sve identitete i aplikacije. Najbolja rešenja za IAM bolje štite identitete, unapređuju korisnički doživljaj i povećavaju administrativnu efikasnost.

Rešenjima za IAM
odgovorite na ove
izazove



**Bolje zaštitite
identitete**



**Unapredite
korisnički doživljaj**



**Povećajte
administrativnu
efikasnost**

Odeljak 2

Pregled usluge Azure AD

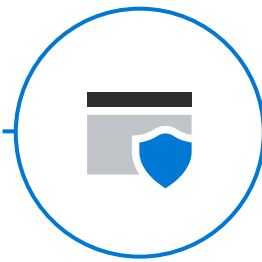
Sveobuhvatno rešenje

Microsoft Azure Active Directory (Azure AD) sveobuhvatno je rešenje u oblaku, vodeće na tržištu upravljanja direktorijima, pristupa aplikacijama i napredne zaštite identiteta. Azure AD omogućava organizacijama upravljanje identitetima i njihovu zaštitu kako bi zaposleni, partneri i klijenti mogli pristupiti aplikacijama i uslugama koji su im potrebni. Azure AD pomaže milionima organizacija da upravljaju i obezbede preko milion identiteta.



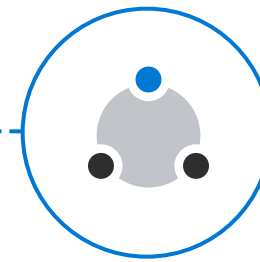
Modernizujte pristup

Zaštitite pristup podacima i resursima organizacije lokalno i u oblaku i upravljajte njime. Povežite sve korisnike, aplikacije i uređaje u oblaku za nesmetano i bezbedno pristupanje i veću vidljivost i kontrolu. Automatizujte tokove posla i omogućite samousluživanje da biste smanjili troškove i poboljšali produktivnost svojih korisnika.



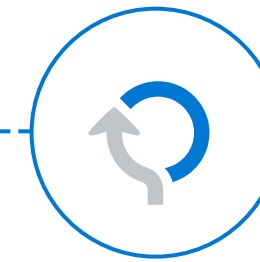
Bezbednost i upravljanje

Uz veliki broj svakodnevnih napada na akreditivne korisnika, da bi se sprečilo ugrožavanje sistema potrebno je kontinuirano praćenje normalnog i abnormalnog ponašanja uz najširi mogući raspon signala, primenu veštačke inteligencije i automatizovanje odgovora. Održite ravnotežu između produktivnosti i bezbednosti pravovremenim pristupom odgovarajućim resursima, kao i redovnim ocenjivanjem pristupa i nametanjem pravila.



Deljenje i saradnja

Proširite svoje poslovanje pouzdanom uslugom u oblaku koju mogu koristiti milioni korisnika i čije su bezbednost i fleksibilnost najbolje u branši. Povežite se s spoljnim korisnicima i omogućite im produktivnost pružanjem jednostavnog interfejsa kojim se mogu sami služiti i ugrađenim bezbednosnim kontrolama.



Razvoj i integracija

Izradite aplikacije koje korisnicima omogućavaju jednostavnu prijavu na Microsoft privatne naloge, naloge za posao ili obrazovanje ili naloge društvenih mreža. Počnite se povezivati sa interfejsom Microsoft Graph, mrežnim prolazom ka podacima i informacijama u okruženju Microsoft 365, i razvijte aplikacije bogate sadržajem. Omogućite jedinstveno prijavljivanje i automatsko obezbeđivanje korisnika da biste doprli do najvećih svetskih organizacija.

3. deo

Azure AD za aplikacije

Azure AD za aplikacije

Univerzalna platforma

Azure AD vam omogućava da upravljate zajedničkim identitetom za svakog korisnika u okviru hibridne infrastrukture da biste pristupili svim aplikacijama koje su im potrebne, što obuhvata i aplikacije karakteristične za njegovo područje rada, kako lokalne tako i u oblaku. Upravljajte svim identitetima s univerzalne platforme da biste povećali administrativnu efikasnost i imali bolju kontrolu. Primените granularna bezbednosna pravila na svaku aplikaciju koju koristite u svojoj organizaciji.



Uštedite vreme i novac

Azure AD unaprijed je integrisan s hiljadama aplikacija, uključujući one popularne, kao što su Workday, ServiceNow, SuccessFactors, Adobe i Concur, pa te aplikacije možete lako staviti na raspolaganje svojim korisnicima. Koristite jednu konzolu da biste dosledno sprovodili pravila i nadzirali pristupna prava. Tokove rada za dodelu korisničkih ovlašćenja i upravljanje životnim ciklusima možete automatizovati i tako uštedeti vreme i resurse pomoću samouslužnog upravljanja nalogom. Možete koristiti i dolazne informacije o korisnicima iz alatki za upravljanje ljudskim resursima kao izvor tačnih podataka, pa nema potrebe za prilagođenim skriptama ili ručnim postupcima za upravljanje korisničkim atributima.

Aplikacije konfigurisane pomoću usluge Azure AD omogućavaju jedinstvenu prijavu za neometan pristup, što znači da korisnici ne moraju da pamte akreditive za svaki nalog aplikacije ili višekratno da koriste slabe lozinke i rizikuju ugrožavanje bezbednosti podataka. Nalozi konfigurisani za automatsku dodelu ovlašćenja omogućavaju korisnicima pristup novim resursima što je pre moguće. Na području ulazne dodele ovlašćenja Azure AD omogućava novim zaposlenima pristup svim potrebnim resursima od prvog dana.



**Ušteda vremena
i novca**



**Ugrađene SaaS
integracije**



**Jedinstveno
prijavljivanje**



**Korisnički pristup
od prvoga dana**

Omogućite sigurniji pristup svim aplikacijama

Azure AD omogućava sveobuhvatnu zaštitu identiteta u svim aplikacijama – kako aplikacijama SaaS-a tako i lokalno instaliranim aplikacijama iz određene oblasti poslovanja. Bez obzira na to da li korisnik zahteva pristup programu Microsoft Word ili Box, Azure AD osigurava da se identitet potvrdi pre dodeljivanja pristupa. Takođe možete da obezbedite pristup smernicama upravljanja da biste se uverili da korisnici imaju pristup samo onome što im je potrebno, kada im je to potrebno. Možete zahtevati od korisnika da zatraže dozvolu za pristup i možete da podesite vremensko ograničenje za trajanje pristupa aplikaciji i vođenje regularnih pregleda usaglašenosti pristupa.

Azure AD koristi i snagu sistema Microsoft Intelligent Security Graph i mašinskog učenja da bi u svim našim proizvodima i uslugama analizirao milijarde signala koji otkrivaju netipična ponašanja i dodeljuju ocenu relativnog rizika svakoj sesiji. Azure AD uzima u obzir uređaj, lokaciju i druge kontekstne informacije da bi procenio rizik povezan s određenom prijavom. Možete utvrditi pravila uslovnog pristupa za Azure AD koja automatski primenjuju bezbednosne mere, kao što je blokiranje zahteva za pristup ili traženje ponovnog postavljanja lozinke kada se prijava smatra rizičnom ili su ispunjeni uslovi predviđeni nekim pravilom.



**Mere zaštite
aplikacija**



**Zaštita
identiteta**



**Upravljanje
pristupom**



**Smernice
uslovnog pristupa**

4. deo

Zaštita aplikacija i upravljanje njima pomoću usluge Azure AD

Azure AD omogućava bolju kontrolu i smanjuje troškove zahvaljujući automatizaciji, samousluživanju i sprovođenju pravila.

Zaštita aplikacija i upravljanje njima pomoću usluge Azure AD

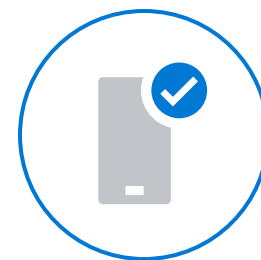


Integracije aplikacija za Azure AD

Galerija aplikacija usluge Azure AD omogućava jednostavnu konfiguraciju bilo koje od hiljadu unapred integrisanih aplikacija za vašeg klijenta i njihovo povezivanje. Sve te aplikacije podržavaju jedinstvenu prijavu, a za uslovni pristup usluge Azure AD aplikacije se mogu jednostavno konfigurisati, bilo svaka zasebno ili u skladu s pravilima koja važe za celu organizaciju. Kad dodate aplikaciju i konfigurirate je u skladu sa svojim potrebama, korisnici s ovlašćenjima za pristup mogu je lako pronaći na portalu My Apps usluge Azure AD, središnjem portalu na kojem krajnji korisnici mogu pronaći i pokrenuti aplikacije.

Ako ste izradili aplikaciju ili je vašoj organizaciji potrebna njena integracija, možete zatražiti da bude na listi u galeriji aplikacija usluge Azure AD.

[Pregledajte hiljade unapred integrisanih aplikacija >](#)



Obezbeđivanje hibridnog pristupa

Proxy za aplikacije servisa Azure AD omogućava vam siguran udaljeni pristup veb aplikaciji u lokalnom okruženju koja podržava tvrdnje bez potrebe za VPN-om. Za rad proxy servera za aplikacije potrebna je instalacija s lakim konektorom, a on omogućava način rada koji je za IT i za krajnjeg korisnika isti kao rad aplikacija SaaS-a povezanih putem galerije aplikacija usluge Azure AD.

A ako želite iskoristiti dostupnost postojećih infrastrukturnih ulaganja, na primer, s partnerima kao što su F5 ZScaler, SAP, Oracle ili Ping Identity, da biste povezali druge vrste aplikacija, kao što su one koje koriste protokole za proveru identiteta na osnovu zaglavlja ili Kerberos, možete i to da uradite, a pritom i dalje da uživate u pogodnostima centralizacije i zaštite koje nudi Azure AD.

[Pročitajte kako dodati lokalnu aplikaciju putem proxy servera za aplikacije >](#)

[Povezivanje drugih partnerskih aplikacijskih mreža i oblaka >](#)

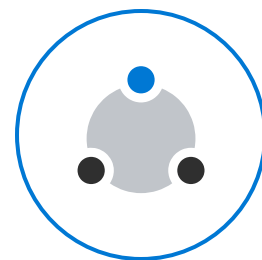
Zaštita aplikacija i upravljanje njima pomoću usluge Azure AD



Automatizovano obezbeđivanje

Azure AD omogućava automatizovanje kreiranja, održavanja i uklanjanja korisničkih identiteta u popularnim aplikacijama SaaS-a. Kad se nove osobe priključe vašem timu ili organizaciji, možete automatski kreirati nove naloge u odgovarajućim sistemima. Kada osoba napusti tim ili organizaciju, možete da postavite smernice koje će automatski deaktivirati naloge u odgovarajućim sistemima. Automatizacijom tih zadataka možete obezbediti da identiteti u aplikacijama i sistemima budu ažurirani u skladu s promenama u direktorijumu ili sistemu ljudskih resursa, smanjujući tako greške i štedeći vreme.

[Saznajte više o postavljanju automatske dodele i uklanjanja identiteta za aplikacije SaaS-a >](#)



Grupno upravljanje

Azure AD omogućava pristup resursima organizacije pružajući pravo pristupa jednom korisniku ili celoj grupi usluge Azure AD. Grupe omogućuju vlasniku resursa da postavi dozvole za pristup za sve članove grupe odjednom umjesto da dodeljuje prava jednom po jednom članu. To je sigurniji način jer je manje verovatno da će nekome slučajno biti dodeljen neprimeren pristup, a njime se i štedi vreme. Upravljanje grupom može se i dinamički prilagoditi automatizacijom primanja članova na osnovu pravila zasnovanih na atributima identiteta.

[Naučite kako da kreirate grupu na Azure portalu >](#)

Zaštita aplikacija i upravljanje njima pomoću usluge Azure AD



Samousluživanje korisnika

Za obavljanje nekih zadataka nije potreban IT stručnjak, a Azure AD omogućuje vam da ih dodelite drugim osobama u organizaciji. Možete da omogućite korisnicima da kreiraju sopstvene bezbednosne grupe i da upravljaju njima u usluzi Azure AD. Vlasnici grupa mogu odobravati ili odbijati zahteve za članstvo ili mogu delegirati kontrolu članstva u grupi.

[Postavljanje grupa koje mogu upravljati same sobom >](#)

Samousluživanje se odnosi i na korisnike. Korisnici se mogu registrovati na nalog putem portala za samousluživanje ako imaju proverenu e-poštu i mogu koristiti portal za ponovno postavljanje lozinke. To može znatno doprineti uštedi vremena i novca vašoj službi za korisnike.

[Konfigurisanje samoouslužnog ponovnog postavljanja lozinke >](#)



Modernizacija potvrde identiteta

Ako trenutno koristite lokalnu potvrdu identiteta kao što je Active Directory Federation Services (AD FS) mogli biste imati koristi od migriranja aplikacija u Azure AD. Njime zadržavate prednosti za korisnika kao što je jedinstvena prijava, a dobijate skalabilnost i sigurnosne prednosti koje su dostupne u oblaku, kao što je primjena granularnih kontrola pristupa pojedinoj aplikaciji pomoću uslovnog pristupa usluge Azure AD ili dodeljivanje pristupa resursima partnerima putem B2B suradnje servisa Azure AD. Sve aplikacije koje za spoljašnje prijave koriste standarde SAML 2.0, WS-Federation, OAuth ili OpenID Connect mogu se migrirati.

[Stvaranje pravila uslovnog pristupa usluge Azure AD za zaštitu pristupa aplikacijama >](#)

[Koristite Azure AD B2B za neometanu saradnju sa spoljnim partnerima >](#)

Bezbedno povežite bilo koju aplikaciju, na bilo kom oblaku ili serveru sa uslugom Azure AD.

Povezano je čak **milion** aktivnih jedinstvenih aplikacija.

Počnite da ga koristite već danas.

[Započnite besplatno jednomesečno probno korišćenje usluge Azure AD](#) da biste se uverili kako je jednostavno upravljati korisničkim pristupom svim aplikacijama i zaštititi svoje preduzeće.

