



Zaštitite pristup svojim aplikacijama i upravljajte njima putem servisa **Azure Active Directory**



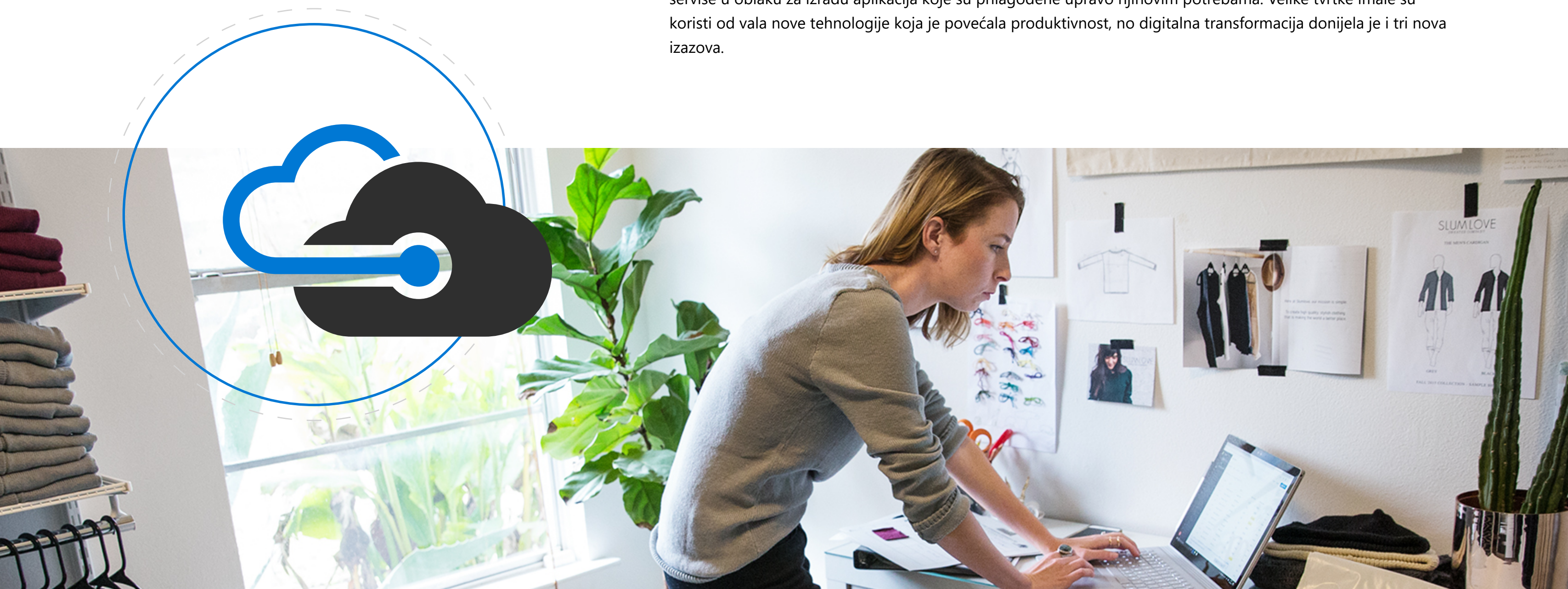
1. dio

Što je upravljanje
identitetima i
pristupom?

Što je upravljanje identitetima i pristupom?

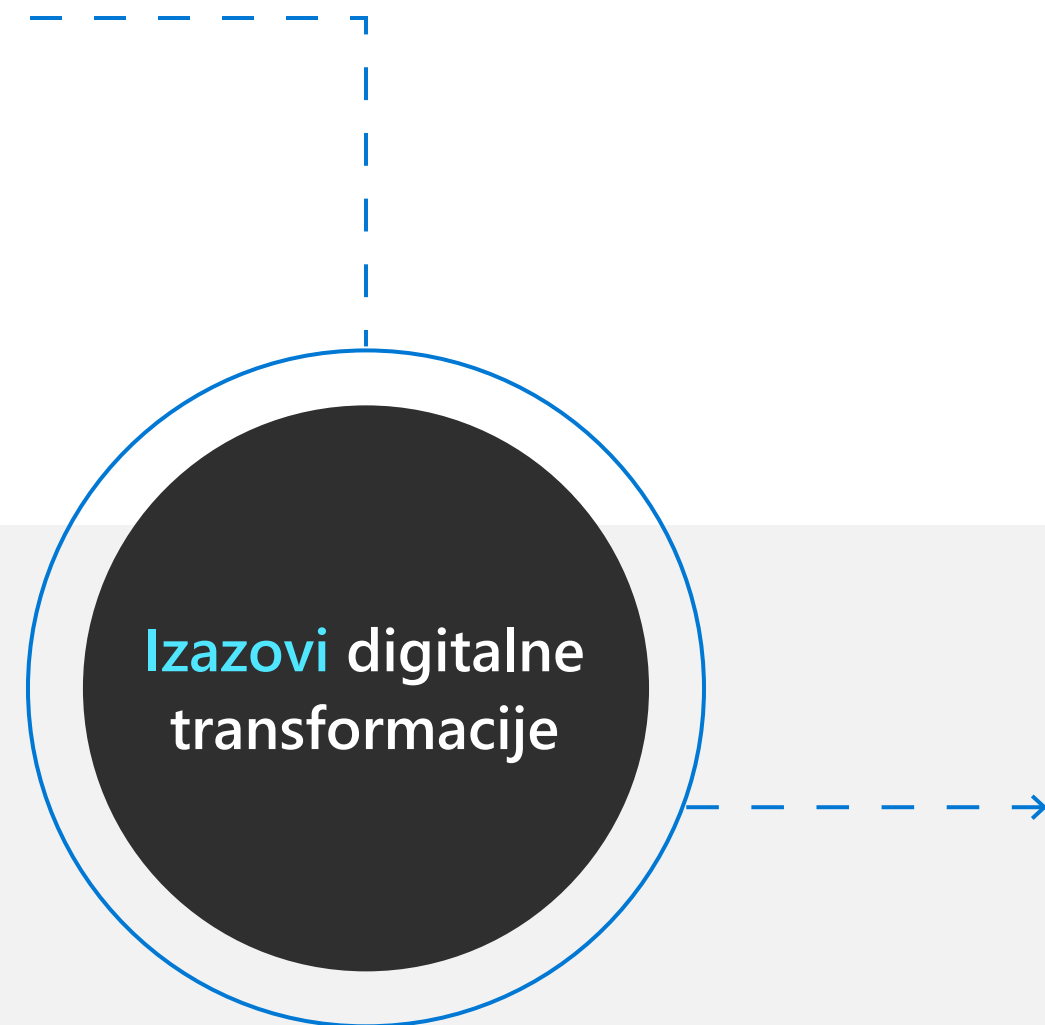
Digitalna transformacija

Računalstvo u oblaku i mobilni uređaji promijenili su način na koji radimo. Svijet rada sve više se globalizira i dovoljno je fleksibilan da se raditi može s bilo kojeg mjesta, pri čemu se izazovi na području produktivnosti i suradnje uspješno rješavaju besplatnim i povoljnim aplikacijama softvera kao servisa (SaaS). Velike tvrtke migriraju aplikacije i računalstvo u oblak da bi osuvremenile svoju arhitekturu, a njihovi odjeli koriste nove servise u oblaku za izradu aplikacija koje su prilagođene upravo njihovim potrebama. Velike tvrtke imale su koristi od vala nove tehnologije koja je povećala produktivnost, no digitalna transformacija donijela je i tri nova izazova.



Što je upravljanje identitetima i pristupom?

Novi izazovi



Sigurnosni rizik: Prije revolucije u oblaku IT je služio kao čuvar pristupa tehnologiji. Aplikacije i platforme koje ste štitili i kojima ste upravljali bile su zatvorene u granicama mreže, a sve koji su se prijavili u resurse tvrtke morao je propustiti vatrozid. To je sada prošlost. Vaši zaposlenici imaju veću kontrolu nad tehnologijom koju koriste, a velikom dijelu te tehnologije pristupa se putem interneta. Napadači na internetu naučili su kako iskoristiti te slabosti. Čak i kad korisnik zna pravu lozinku za pristup računu, ne možete uvijek biti potpuno sigurni da se doista radi o osobi koja se kao takva predstavlja.

Administrativno opterećenje: Nevjerojatan rast broja krajnjih točaka korisnicima omogućuje mnogo više načina povezivanja, ali to je istovremeno i administrativna noćna mora. Mnoge tvrtke nisu svjesne koje sve alate zaposlenici koriste, a čak i kada imaju dobar pregled situacije, sama količina aplikacija u oblaku znači da morate upravljati većim brojem sustava identiteta, što povećava troškove te postojećim sigurnosnim rizicima dodaje nove.

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



**Sigurnosni
rizik**



**Administrativno
opterećenje**



**Loše korisničko
iskustvo**

Što je upravljanje identitetima i pristupom?

Upravljanje identitetima i pristupom kao središnja upravljačka ravnina

Zajednički nazivnik navedenih problema neučinkoviti su sustavi provjere identiteta. Nekada je kao upravljačka ravnina služila granica mreže, a sada tu ulogu preuzima identitet. Potrebna su vam rješenja kojima se povezuju različiti alati, arhitektura, uređaji i servisi na razini tvrtke da bi organizacija bila zaštićenija i da bi se moglo upravljati pristupom zaposlenika i vanjskih suradnika. Sustavi za upravljanje identitetima i pristupom (IAM) objedinjuju pristupe, što omogućuje bolju kontrolu. Oni vam omogućuju neometanu suradnju izvan granica tvrtke ili ustanove uz unaprjeđenje zaštite poslovnih resursa. Dobro rješenje za IAM omogućuje vam da povežete korisnike sa svim njihovim aplikacijama za rad (bez obzira jesu li one dostupne u oblaku ili lokalno) jednim skupom vjerodajnica. Rješenja za IAM osmišljena su tako da korisnicima omogućuju pristup samo resursima koji su im potrebni, a onemogućuju korisnicima pristup podacima za koje nemaju ovlasti. Pravima za pristup i dozvolama za pristup upravlja se sa središnjeg portala, čime se smanjuje broj postupaka omogućivanja i onemogućivanja korištenja korisničkih računa koji se moraju obaviti ručno. Rješenja za IAM sadrže i alate za upravljanje sigurnosnim pravilnicima primjenjive za sve identitete i aplikacije. Najbolja rješenja za IAM bolje štite identitete, poboljšavaju korisnički rad i povećavaju administrativnu učinkovitost.

Rješenjima za IAM
odgovorite na ove
izazove



**Bolje
zaštitite
identitete**



**Poboljšajte
korisnički
rad**



**Povećajte
administrativnu
učinkovitost**

2. dio

Pregled servisa Azure AD

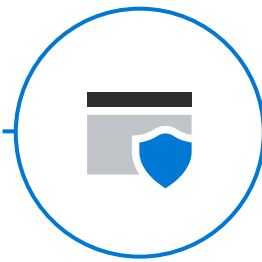
Sveobuhvatno rješenje

Microsoft Azure Active Directory (Azure AD) sveobuhvatno je rješenje u oblaku, vodeće na tržištu upravljanja direktorijima, pristupa aplikacijama i napredne zaštite identiteta. Azure AD omogućuje tvrtkama i ustanovama upravljanje identitetima te njihovu zaštitu kako bi zaposlenici, partneri i klijenti mogli pristupiti aplikacijama i servisima koji su im potrebni. Azure AD omogućuje milijunima tvrtki i ustanova zaštitu više od milijardu identiteta i upravljanje njima.



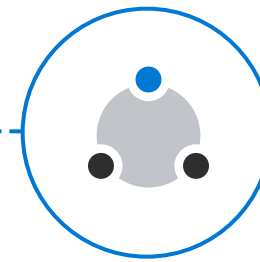
Modernizacija pristupa

Zaštitite pristup podacima i resursima tvrtke ili ustanove lokalno i u oblaku te upravljajte njima. Povežite sve svoje korisnike, aplikacije i uređaje s oblakom da biste omogućili neometan i siguran pristup te veću vidljivost i kontrolu. Automatizirajte tijekove rada i omogućite samoposluživanje da biste smanjili troškove i poboljšali produktivnost svojih korisnika.



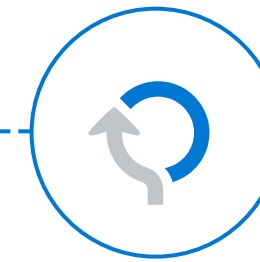
Zaštita i kontrola

Uz velik broj svakodnevnih napada na vjerodajnice korisnika, da bi se spriječilo ugrožavanje sustava potrebno je kontinuirano praćenje normalnog i abnormalnog ponašanja uz najširi mogući raspon signala, primjenu umjetne inteligencije i automatiziranje odgovora. Održite ravnotežu između produktivnosti i sigurnosti pravovremenim pristupom odgovarajućim resursima te redovnim ocjenjivanjem pristupa i provedbom pravilnika.



Povezivanje i suradnja

Proširite svoje poslovanje pouzdanim servisom u oblaku koji mogu koristiti milijuni korisnika i čije su sigurnost i fleksibilnost najbolje na tržištu. Povežite se s vanjskim korisnicima i omogućite im produktivnost zahvaljujući jednostavnom sučelju kojim se mogu sami služiti i ugrađenim sigurnosnim kontrolama.



Razvoj i integracija

Izradite aplikacije koje korisnicima omogućuju jednostavnu prijavu na Microsoftov osobni račun, račun tvrtke ili obrazovne ustanove ili pak račun za društvene mreže. Povezujte se u Microsoft Graph, pristupnik za podatke i poslovno obavješćavanje u okruženju Microsoft 365, te razvijte obogaćene aplikacije. Omogućite jedinstvenu prijavu i automatizirajte dodjelu korisničkih ovlasti da biste doprli do najvećih svjetskih tvrtki ili ustanova.

3. dio

Azure AD za vaše
aplikacije

Azure AD za vaše aplikacije

Univerzalna platforma

Azure AD omogućuje vam upravljanje zajedničkim identitetima pomoću kojih svaki korisnik vaše hibridne infrastrukture može pristupiti svim aplikacijama koje su mu potrebne, što obuhvaća i aplikacije karakteristične za njegovo područje rada, lokalne i u oblaku. Upravljajte svim identitetima putem univerzalne platforme da biste povećali administrativnu učinkovitost i imali bolju kontrolu. Primijenite granularne sigurnosne pravilnike na svaku aplikaciju koju koristite u svojoj tvrtki ili ustanovi.



Ušteda vremena i novca

Azure AD unaprijed je integriran s tisućama 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 dosljedno provodili pravilnike i nadzirali pristupna prava. Tijekove rada za dodjelu korisničkih ovlasti i upravljanje životnim ciklusima možete automatizirati te uštedjeti vrijeme i resurse pomoću samoposlužnog upravljanja računom. Možete koristiti i dolazne informacije o korisnicima iz alata za upravljanje ljudskim resursima kao izvor točnih podataka, pa nema potrebe za prilagođenim skriptama ili ručnim postupcima za upravljanje korisničkim atributima.

Aplikacije konfigurirane putem servisa Azure AD omogućuju jedinstvenu prijavu za neometan pristup, što znači da korisnici ne moraju zapamtiti vjerodajnice za svaki račun aplikacije ni višekratno koristiti slabe lozinke i riskirati ugrožavanje sigurnosti podataka. Računi konfigurirani za automatsku dodjelu ovlasti omogućuju korisnicima što brži pristup novim resursima. Na području ulazne dodjele ovlasti Azure AD omogućuje novim zaposlenicima pristup svim potrebnim resursima od prvog dana.



**Ušteda vremena
i novca**



**Ugrađene SaaS
integracije**



**Jedinstvena
prijava**



**Korisnički pristup
od prvog dana**

Omogućite sigurniji pristup svim aplikacijama

Azure AD omogućuje sveobuhvatnu zaštitu identiteta u svim aplikacijama, i SaaS aplikacijama i lokalno instaliranim aplikacijama pojedinog odjela. Neovisno o tome zatraži li korisnik pristup u Microsoft Word ili Box, Azure AD jamči da će njegov identitet biti potvrđen prije odobravanja pristupa. Možete i stvoriti pravilnike kojima se uređuje pristup tako da korisnici mogu pristupati samo onome što im je potrebno i kada im je potrebno. Možete odrediti da korisnici moraju zatražiti dozvolu za pristup i postaviti vremensko ograničenje pristupa aplikaciji te provoditi redovne provjere pravilnosti pristupa.

Azure AD koristi i snagu sustava Microsoft Intelligent Security Graph te strojnog učenja da bi u svim našim proizvodima i uslugama analizirao bilijune signala koji otkrivaju netipična ponašanja i dodjeljuju ocjenu relativnog rizika svakoj sesiji. Azure AD uzima u obzir uređaj, lokaciju i druge kontekstne informacije da bi procijenio rizik povezan s određenom prijavom. Možete stvoriti pravilnike o uvjetnom pristupu za Azure AD koja automatski primjenjuju sigurnosne mjere, kao što je blokiranje zahtjeva za pristup ili traženje ponovnog postavljanja lozinke kada se prijava smatra rizičnom ili su ispunjeni uvjeti predviđeni nekim pravilnikom.



**Mjere zaštite
aplikacija**



**Zaštita
identiteta**



**Uređivanje
pristupa**



**Pravilnici o
uvjetnom
pristupu**

4. dio

Zaštita aplikacija i upravljanje njima putem servisa Azure AD

Azure AD omogućuje bolju kontrolu i smanjuje troškove zahvaljujući automatizaciji, samoposluživanju i provedbi pravilnika.

Zaštita aplikacija i upravljanje njima putem servisa Azure AD



Integracije aplikacija za Azure AD

Galerija aplikacija servisa Azure AD omogućuje jednostavnu konfiguraciju bilo koje od tisuća unaprijed integriranih aplikacija za vašeg klijenta i njihovo povezivanje. Sve te aplikacije podržavaju jedinstvenu prijavu, a za uvjetni pristup za Azure AD aplikacije se mogu jednostavno konfigurirati, svaka zasebno ili u skladu s pravilnicima koji vrijede za cijelu tvrtku. Kad dodate aplikaciju i konfigurirate je u skladu sa svojim potrebama, korisnici s ovlastima za pristup mogu je lako pronaći na portalu Moje aplikacije servisa Azure AD, središnjem portalu na kojem krajnji korisnici mogu pronaći i pokrenuti aplikacije.

Ako ste izradili aplikaciju ili je vašoj tvrtki ili ustanovi potrebna njezina integracija, možete zatražiti da bude na popisu u galeriji aplikacija servisa Azure AD.

[Pregledajte tisuće unaprijed integriranih aplikacija >](#)



Siguran hibridni pristup

Proxy za aplikacije servisa Azure AD omogućuje vam siguran daljinski pristup bez VPN-a web-aplikaciji u lokalnom okruženju utemeljenoj na slanju zahtjeva. Za rad proxyja za aplikacije potrebna je instalacija s jednostavnim poveznikom, a on omogućuje način rada koji je za IT i za krajnjeg korisnika isti kao rad SaaS aplikacija povezanih putem galerije aplikacija servisa Azure AD.

A ako želite iskoristiti dostupnost postojećih infrastrukturnih ulaganja, primjerice 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 provjeru autentičnosti na temelju zaglavlja ili Kerberos, možete i to učiniti, a pritom i dalje koristiti pogodnosti centralizacije i zaštite koje nudi servis Azure AD.

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

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

Zaštita aplikacija i upravljanje njima putem servisa Azure AD



Automatsko dodjeljivanje identiteta

Azure AD omogućuje automatizaciju stvaranja, održavanja i uklanjanja korisničkih identiteta u popularnim SaaS aplikacijama. Kad se nove osobe priključe vašem timu, tvrtki ili ustanovi, možete automatski stvoriti nove račune u odgovarajućim sustavima. Kada netko napusti tim, tvrtku ili ustanovu, možete postaviti pravilnike koji će automatski deaktivirati njegov račun u odgovarajućim sustavima. Automatizacijom tih zadataka omogućujete ažurnost identiteta u aplikacijama i sustavima u skladu s promjenama u direktoriju ili sustavu ljudskih resursa, smanjujući tako pogreške i štedeći vrijeme.

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



Grupno upravljanje

Azure AD omogućuje pristup resursima tvrtke ili ustanove dajući pravo pristupa jednom korisniku ili cijeloj grupi servisa Azure AD. Grupe omogućuju vlasniku resursa da postavi dozvole za pristup za sve članove grupe odjednom umjesto da dodjeljuje prava jednom po jednom članu. To je sigurniji način jer je manje vjerojatno da će nekome nehotice biti dodijeljen neodgovarajući pristup, a njime se i štedi vrijeme. Upravljanje grupom može se i dinamički prilagoditi automatizacijom primanja članova na temelju pravilnika zasnovanih na atributima identiteta.

[Saznajte kako stvoriti grupu na portalu za Azure >](#)

Zaštita aplikacija i upravljanje njima putem servisa Azure AD



Samoposluživanje korisnika

Za obavljanje nekih zadataka nije potreban IT stručnjak, a Azure AD omogućuje vam da ih dodijelite drugim osobama u tvrtki ili ustanovi. Korisnicima možete omogućiti stvaranje vlastitih sigurnosnih grupa u servisu Azure AD i upravljanje njima. Vlasnici grupa mogu odobravati ili odbijati zahtjeve za članstvo ili pak delegirati kontrolu članstva u grupi.

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

Samoposluživanje se odnosi i na korisnike. Korisnici se mogu registrirati za račun putem portala za samoposluživanje ako imaju provjerenu e-poštu te mogu koristiti portal za ponovno postavljanje lozinke. To može znatno pridonijeti uštedi vremena i novca službi za korisnike.

[Konfiguriranje samoposlužnog ponovnog postavljanja lozinke >](#)



Modernizacija provjere autentičnosti

Ako trenutno koristite lokalnu provjeru autentičnosti kao što je Active Directory Federation Services (AD FS), mogli biste imati koristi od migracije aplikacija na Azure AD. Njime zadržavate prednosti za korisnike, npr. jedinstvenu prijavu, a dobivate skalabilnost i sigurnosne prednosti dostupne u oblaku, kao što je primjena granularnih kontrola pristupa pojedinoj aplikaciji pomoću uvjetnog pristupa za Azure AD ili dodjela partnerima pristupa resursima putem B2B suradnje putem servisa Azure AD. Sve aplikacije koje za vanjske prijave koriste standarde SAML 2,0, WS-Federation, OAuth ili OpenID Connect mogu se migrirati.

[Stvaranje pravilnika o uvjetnom pristupu za Azure AD radi zaštite pristupa aplikacijama >](#)

[Koristite servis Azure AD B2B za neometanu suradnju s vanjskim partnerima >](#)

Na siguran način povežite bilo koju aplikaciju na bilo kojem oblaku ili poslužitelju sa servisom Azure AD.

Povezano je čak milijun aktivnih
jedinstvenih aplikacija.

Započnite s radom već danas.

Započnite besplatno jednomjesečno probno korištenje servisa Azure AD da biste se uvjerali kako je jednostavno upravljati korisničkim pristupom svim aplikacijama i zaštititi svoju tvrtku.

