



Pārvaldiet un drošiniet piekļuvi savām programmām, izmantojot **Azure Active Directory**



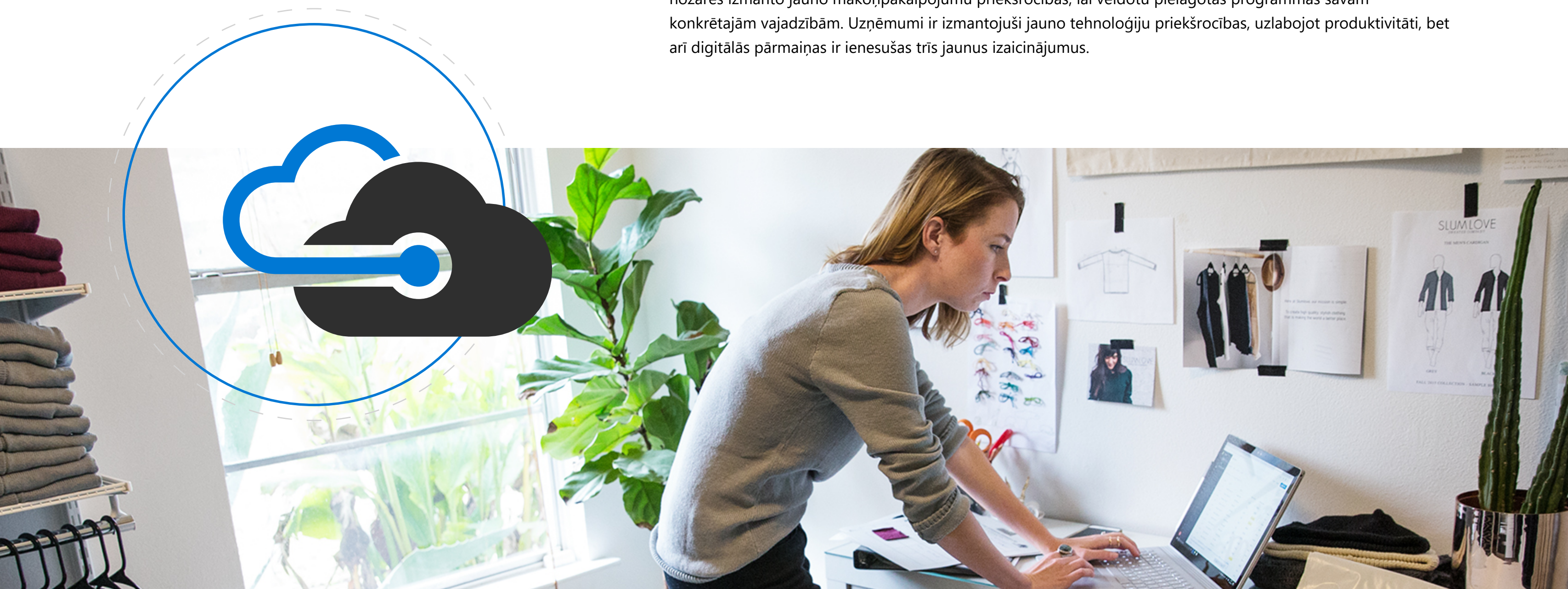
1. sadaļa

Kas ir identitātes un
piekļuves pārvaldība?

Kas ir identitātes un piekļuves pārvaldība?

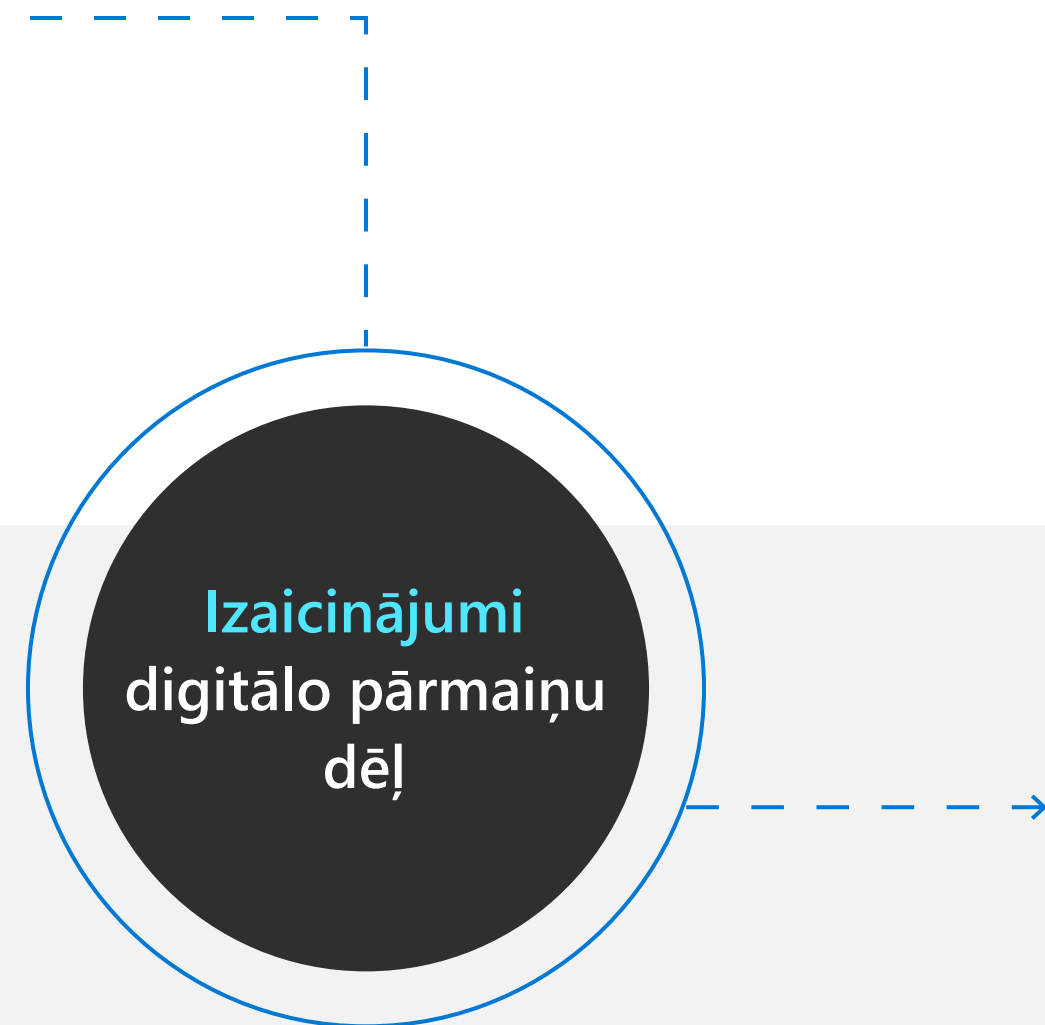
Digitālās pārmaiņas

Mākoņdatošana un mobilās ierīces pārveidoja moderno darbvietu. Arvien lielākai globālā darbaspēka daļai ir elastīga iespēja strādāt neatkarīgi no atrašanās vietas, izmantojot bezmaksas un zemu izmaksu programmatūru pakalpojumu (SaaS) lietojumprogrammu veidā, lai risinātu produktivitātes un sadarbības izaicinājumus. Lielie uzņēmumi migrē programmas un datošanu uz mākonī, lai modernizētu savu arhitektūru, un uzņēmējdarbības nozares izmanto jauno mākoņpakalpojumu priekšrocības, lai veidotu pielāgotas programmas savām konkrētajām vajadzībām. Uzņēmumi ir izmantojuši jauno tehnoloģiju priekšrocības, uzlabojot produktivitāti, bet arī digitālās pārmaiņas ir ienesušas trīs jaunus izaicinājumus.



Kas ir identitātes un piekļuves pārvaldība?

Jauni izaicinājumi



Drošības risks: pirms mākoņa revolūcijas IT darbinieki bija kā tehnoloģiju vārtsargi. Jūsu pārvaldītās un drošinātās programmas un platformas bija iekļautas tīkla perimetrā, un visus, kas pierakstījās jūsu uzņēmuma resursos, vispirms validēja ugunsmūris. Šis laiks ir pagājis. Jūsu darbaspēkam ir lielāka kontrole pār tehnoloģijām, ko tas izmanto, un lielai daļai to tiek piekļūts, izmantojot internetu. Kiberuzbrucēji ir iemācījušies izmantot šīs ievainojamības. Pat tad, ja lietotājs zina pareizo konta paroli, jūs nevarat būt drošs, ka tas ir tas, par kuru uzdodas.

Administratīvais slogs: galapunktu eksplozija nodrošina lietotājus ar papildu savienojuma veidiem, bet rada arī administratīvu murgu. Daudzi uzņēmumi nav informēti par visiem rīkiem, ko darbinieki izmanto, un pat tad, ja tiem ir laba inventāra uzskaitē, lielais mākoņa programmu skaits nozīmē to, ka jums ir jāpārvalda vairākas identitātes sistēmas, kas palielina izmaksas un sarežģī esošos drošības riskus.

Slikta lietotāju pieredze: arī lietotājiem ir problēmas. Tiem patīk elastība, bet neapmierinātību rada daudzie akreditācijas dati, kas ir jāiegaumē.



Drošības risks



Administratīvais
slogs



Slikta lietotāju
pieredze

Kas ir identitātes un piekļuves pārvaldība?

Identitātes un piekļuves pārvaldība kā centrālā vadības plakne

Visu šo sāpju punktu kopsaucējs ir neefektīvas identitātes pārbaudes sistēmas. Identitāte ir aizstājusi tīkla perimetru kā jaunā vadības plakne. Jums ir nepieciešami risinājumi, kas visā uzņēmumā savieno atšķirīgos rīkus, arhitektūras, ierīces un pakalpojumus, lai labāk aizsargātu organizāciju un pārvaldītu piekļuvi gan darbiniekiem, gan ārējiem partneriem. Identitātes un piekļuves pārvaldības (IAM) sistēmas apvieno piekļuvi vienā sistēmā, sniedzot jums lielāku kontroli. Tās piedāvā nevainojamu sadarbību pāri jūsu organizācijas robežām, vienlaikus uzlabojot uzņēmuma resursu drošību. Labs IAM risinājums ļauj, izmantojot vienu akreditācijas datu kopu, savienot lietotājus ar visām to darba programmām neatkarīgi no tā, vai tās atrodas mākonī vai lokāli. IAM risinājumi ir paredzēti, lai lietotājiem piešķirtu piekļuvi tikai nepieciešamajiem resursiem un bloķētu nepilnvarotu lietotāju piekļuvi datiem, kuriem tiem nebūtu jāpiekļūst. Jūs pārvaldāt lietotāju piekļuves tiesības un atļaujas no centralizēta portāla, kas samazina lielu daļu manuālo procesu, kas jāveic saistībā ar lietotāju kontu nodrošināšanu un nodrošinājuma atcelšanu. IAM risinājumi nodrošina arī rīkus drošības politiku pārvaldībai visās jūsu identitātēs un programmās. Vislabākie IAM risinājumi labāk aizsargā identitātes, uzlabo lietotāju pieredzi un palielina administratīvo efektivitāti.

IAM risinājumi
risina šos
izaicinājumus



Labāka identitāšu
aizsardzība



Lietotāju pieredzes
uzlabošana



Administratīvo
efektivitātes palielināšana

2. sadaļa

Azure AD pārskats

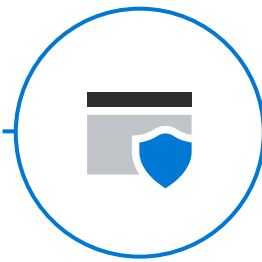
Visaptverošs risinājums

Microsoft Azure Active Directory (Azure AD) ir visaptverošs IAM risinājums mākonī, kā arī direktoriju pārvaldības, programmu piekļuves un uzlabotas identitātes aizsardzības tirgus līderis. Azure AD sniedz organizācijām iespēju pārvaldīt un aizsargāt darbinieku, partneru un klientu identitātes, lai piekļūtu nepieciešamajām programmām un pakalpojumiem. Azure AD palīdz miljoniem organizāciju pārvaldīt un drošināt vairāk nekā miljardu identitāšu.



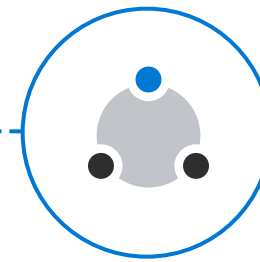
Piekļuves modernizēšana

Pārvaldiet un drošiniet piekļuvi savas organizācijas datiem un resursiem lokāli un mākonī. Savienojiet visus lietotājus, programmas un ierīces ar mākonī, lai nodrošinātu nemanāmu, drošu piekļuvi un uzlabotu redzamību un kontroli. Automatizējiet darbplūsmas un iespējotiet patstāvīgi izmantojamās iespējas, kas palīdz samazināt izmaksas un uzlabot lietotāju produktivitāti.



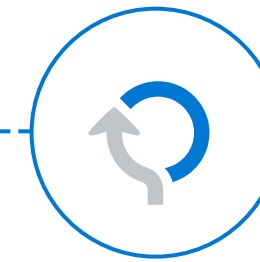
Drošība un regulējumi

Katru dienu notiek ļoti daudz uzbrukumu lietotāju akreditācijas datiem, tāpēc veids, kā nepieļaut kompromisu, ir nepārtraukti sekot līdzi parastajai un nenormālajai darbībai visplašāk iespējamajā signālu klāstā, lietojot mākslīgo intelektu un automatizējot atbildes. Balansējiet produktivitāti un drošību ar savlaicīgu piekļuvi pareizajiem resursiem, kā arī regulāru piekļuves pārskatīšanu un politiku ieviešanu.



Saziņa un sadarbība

Attīstiet savu uzņēmumu, izmantojot uzticamu mākoņpakalpojumu, kas ļauj apkalpot miljoniem lietotāju ar nozarē vadošo drošību un elastību. Veidojiet savienojumu ar ārējiem lietotājiem un ļaujiet tiem būt produktīviem, izmantojot lietotājam draudzīgu, patstāvīgi izmantojamu pieredzi un iebūvētas drošības vadīklas.



Izstrāde un integrācija

Būvējiet programmas, kas lietotājiem ļauj ērti pierakstīties ar savu Microsoft personisko, darba vai mācību kontu vai sociālo kontu. Sāciet, veidojot savienojumu ar Microsoft Graph, vārteju uz datiem un informāciju pakalpojumā Microsoft 365, un būvējiet bagātīgas programmas. Iespējotiet vienoto pierakstīšanos un automatizējiet lietotāju nodrošināšanu un panāciet pasaules lielākās organizācijas.

3. sadaļa

Azure AD jūsu
programmām

Azure AD jūsu programmām

Universāla platforma

Azure AD ļauj pārvaldīt vispārēju identitāti katram lietotājam visā jūsu hibrīdajā infrastruktūrā, lai piekļūtu visām tam nepieciešamajām programmām, tostarp arī mākoņa un lokālajā biznesa programmām. Pārvaldiet visas savas identitātes no universālas platformas, palielinot administratīvo efektivitāti un nodrošinot sev lielāku kontroli. Lietojiet granuļveida drošības politikas katrai programmai, kas tiek izmantota jūsu organizācijā.



Ietaupiet laiku un līdzekļus

Azure AD ir sākotnēji integrēts ar tūkstošiem programmu, tostarp tādu populāru iespēju kā Workday, ServiceNow, SuccessFactors, Adobe, un Concur, atvieglojot šo programmu nodrošināšanu saviem lietotājiem. Izmantojot vienu konsoli, izvietojiet konsekventas politikas un pārbaugiet piekļuves tiesības. Varat automatizēt lietotāju nodrošināšanas un dzīves cikla pārvaldības darbplūsmas un taupīt laiku un resursus, izmantojot patstāvīgi izmantojamu konta pārvaldību. Varat arī saņemt informāciju par lietotājiem no cilvēkresursu rīkiem kā patiesas informācijas avota, lai lietotāju atribūtu pārvaldībai nebūtu jālieto pielāgoti skripti vai manuāli procesi.

Programmas, kas konfigurētas, izmantojot Azure AD, iespējot vienoto pierakstīšanos (SSO) nemanāmai piekļuvei, kas nozīmē to, ka lietotājiem nav jāatceras katras programmas konta akreditācijas dati vai atkārtoti jāizmanto vājas paroles un jāriskē ar datu pārkāpumu. Konti, kas ir konfigurēti automatiskajai nodrošināšanai, lietotājiem sniedz piekļuvi jaunajiem resursiem, tiklīdz tas ir iespējams. Ienākošajai nodrošināšanai Azure AD nodrošina, ka jaunajiem darbiniekiem ir piekļuve visiem atbilstošajiem resursiem jau pirmajā dienā.



**Laika un līdzekļu
taupīšana**



**Iebūvētas SaaS
integrācijas**



**Vienotā
pierakstīšanās**



**Lietotāju piekļuve
jau pirmajā dienā**

Azure AD jūsu programmām

Sniedziet drošāku piekļuvi visām savām programmām

Azure AD nodrošina visaptverošu identitātes aizsardzību visās jūsu programmās — gan SaaS, gan jūsu lokālajās biznesa programmās. Neatkarīgi no tā, vai lietotājs pieprasa piekļuvi programmai Microsoft Word vai Box, Azure AD pirms piekļuves piešķiršanas pārlicinās par tā identitātes apstiprinājumu. Varat arī ieviest piekļuves pārvaldības politikas, lai nodrošinātu lietotāju piekļuvi tikai tam, kas tiem ir nepieciešams, un tad, kad tas ir nepieciešams. Varat pieprasīt lietotājiem pieprasīt atļauju piekļuvei un varat iestatīt laika ierobežojumu, cik ilgi tie var piekļūt programmai, kā arī veikt regulāru piekļuvi atbilstības pārskatīšanu.

Azure AD izmanto arī Microsoft Intelligent Security Graph un mašīnmācīšanos, lai analizētu triljonus signālu visos mūsu produktos un pakalpojumos, kas ļauj atklāt netipisku uzvedību un piešķirt relatīvā riska novērtējumu katrai sesijai. Azure AD analizē informāciju par ierīci, atrašanās vietu un citu kontekstinformāciju, lai novērtētu pierakstīšanās risku. Varat izveidot Azure AD nosacītās piekļuves politikas, kas automātiski lieto drošības līdzekļus, piemēram, piekļuves pieprasījumu bloķēšanu vai paroles atiestatīšanu, ja pierakstīšanās tiek uzskatīta par riskantu vai ja izpildās noteikti politikas nosacījumi.



Programmu
drošības līdzekļi



Identitātes
aizsardzība



Piekļuves
pārvaldība



Nosacītās
piekļuves
politikas

4. sadaļa

Kā pārvaldīt un drošināt programmas, izmantojot Azure AD

Azure AD vienkāršo kontroli un samazina izmaksas, izmantojot automatizāciju, patstāvīgi izmantojamus pakalpojumus un politiku ieviešanu.

Kā pārvaldīt un drošināt programmas, izmantojot Azure AD

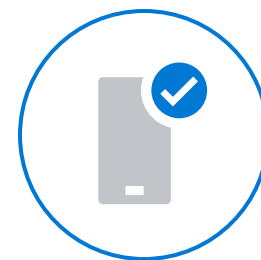


Azure AD programmu integrācija

Azure AD programmu galerija ļauj ērti konfigurēt un ar jūsu nomnieku savienot jebkuru no tūkstošiem sākotnēji integrēto programmu. Visas šīs programmas atbalsta SSO līdzekļus, kā arī programmas var ērti konfigurēt Azure AD nosacītajai piekļuvei, izmantojot programmas vai uzņēmuma līmeņa politiku. Tiklīdz esat pievienojis programmu un konfigurējis to savām vajadzībām, lietotāji ar pilnvarotu piekļuvi var ērti to atrast portālā Azure AD manas programmas, kas ir centralizēts portāls lietotāju programmu atklāšanai un palaišanai.

Ja jūsu organizācijai ir kāda iebūvēta programma vai ir nepieciešama kādas programmas integrācija, varat arī pieprasīt tās iekļaušanu Azure AD programmu galerijā.

[Izpētiet tūkstošiem sākotnēji integrētu programmu >](#)



Droša hibrīdā piekļuve

Izmantojiet Azure AD programmu starpniekserveri, lai nodrošinātu drošu, attālu piekļuvi uz prasībām balstītai lokālai tīmekļa programmai bez nepieciešamības izmantot VPN. Programmu starpniekserverim ir nepieciešama neliela savienotāja instalācija, un tas nodrošina to pašu IT un lietotāju pieredzi, ko sniedz SaaS programmas, kuras ir savienotas, izmantojot Azure AD programmu galeriju.

Vai arī, ja vēlaties izmantot esošās infrastruktūras investīcijas, piemēram, ar tādiem partneriem kā F5 ZScaler, SAP, Oracle vai Ping Identity, lai izveidotu savienojumu ar citu veidu programmām, piemēram, tādām, kas izmanto iesākumos norādītos vai Kerberos autentifikācijas protokolus, varat izdarīt arī to un joprojām gūt Azure AD centralizācijas un drošības priekšrocības.

[Lasiet, kā pievienot lokālo programmu, izmantojot programmu starpniekserveri >](#)

[Savienojuma izveide ar citiem partneru programmu tīkliem un mākoņiem >](#)

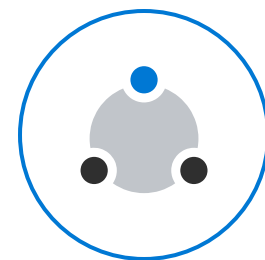
Kā pārvaldīt un drošināt programmas, izmantojot Azure AD



Automatizēta nodrošināšana

Azure AD ļauj automatizēt lietotāju identitāšu izveidi, uzturēšanu un noņemšanu populārās SaaS programmās. Varat automātiski izveidot jaunus kontus pareizajās sistēmās jauniem lietotājiem, kad tie pievienojas jūsu komandai vai organizācijai. Kad lietotāji pamet komandu vai organizāciju, varat iestatīt politikas, kas automātiski deaktivizē to kontus pareizajās sistēmās. Automatizējot šos uzdevumus, varat nodrošināt, lai identitātes jūsu programmās un sistēmās tiktu uzturētas atjauninātas atbilstoši izmaiņām direktorijā vai cilvēkresursu sistēmā, tā samazinot kļūdas un taupot laiku.

[Papildinformācija par automatizētas nodrošināšanas un nodrošinājuma atcelšanas iestatīšanu SaaS programmām >](#)



Grupu pārvaldība

Azure AD palīdz piešķirt piekļuvi organizācijas resursiem, nodrošinot piekļuves tiesības atsevišķam lietotājam vai veselai Azure AD grupai. Grupu lietošana resursa īpašniekam ļauj iestatīt piekļuves atļaujas visiem grupas dalībniekiem, nevis nodrošināt tiesības katram lietotājam atsevišķi. Šī ir drošāka metode, jo jums ir mazāk iespēju nejauši piešķirt individuālu neatbilstošu piekļuvi, kā arī tā var palīdzēt taupīt laiku. Varat arī dinamiski mērogot grupas pārvaldību, automatizējot reģistrēšanu ar identitātes atribūtu politikām.

[Uzziniet, kā Azure portālā izveidot grupu >](#)

Kā pārvaldīt un drošināt programmas, izmantojot Azure AD



Lietotāju patstāvīgi izmantojamie pakalpojumi

Dažu uzdevumu veikšanai nav nepieciešams IT speciālists, un Azure AD ļauj uzticēt tos citiem lietotājiem jūsu organizācijā. Varat piešķirt lietotājiem iespējas direktorijā Azure AD veidot un pārvaldīt savas drošības grupas. Grupu īpašnieki var apstiprināt vai noraidīt dalības pieprasījumus, kā arī tie var deleģēt grupas dalības kontroli.

[Patstāvīgi pārvaldītu grupu iestatīšana >](#)

Patstāvīgi izmantojamie pakalpojumi ir pieejami arī lietotājiem. Lietotāji var reģistrēties kontam, izmantojot patstāvīgi izmantojamu pakalpojumu portālu, ja viņiem ir verificēta e-pasta adrese, un tie var izmantot šo portālu, lai atiestatītu savu paroli. Šādi neskaitāmas reizes varat ietaupīt sava palīdzības dienesta laiku un līdzekļus.

[Patstāvīgi izmantojamas paroles atiestatīšanas konfigurēšana >](#)



Autentifikācijas modernizēšana

Ja pašlaik izmantojat lokālu autentifikāciju, piemēram, Active Directory federācijas pakalpojumu (AD FS), varat apsvērt iespēju migrēt programmas uz Azure AD. Jūs saglabājat tās pašas lietotāju priekšrocības, piemēram, SSO, taču iegūstat mērogojamību un drošības priekšrocības, kas ir pieejamas mākonī, piemēram, granuluveida piekļuves vadīklu lietošanu katrai programmai atsevišķi, izmantojot Azure AD nosacīto piekļuvi, vai piekļuves resursiem piešķiršanu partneriem, izmantojot Azure AD B2B sadarbību. Var migrēt visas programmas, kas federatīvās pierakstīšanās vajadzībām izmanto standartu SAML 2,0, WS-Federation, OAuth vai OpenID Connect.

[Azure AD nosacītās piekļuves politikas izveide, lai drošinātu piekļuvi programmām >](#)

[Azure AD B2B izmantošana, lai nemanāmi sadarbotos ar ārējiem partneriem >](#)

Droši veidojiet jebkuras programmas (jebkurā mākonī vai serverī) savienojumu ar Azure AD.

1 miljons aktīvu, unikālu savienotu programmu.

Sāciet darbu jau šodien.

[Sāciet Azure AD 1 mēneša bezmaksas izmēģināšanu](#), lai uzzinātu, cik vienkārši ir pārvaldīt lietotāju piekļuvi visām savām programmām un aizsargāt savu uzņēmumu.

