



Slik administrerer og sikrer du programmene dine med **Azure Active Directory**



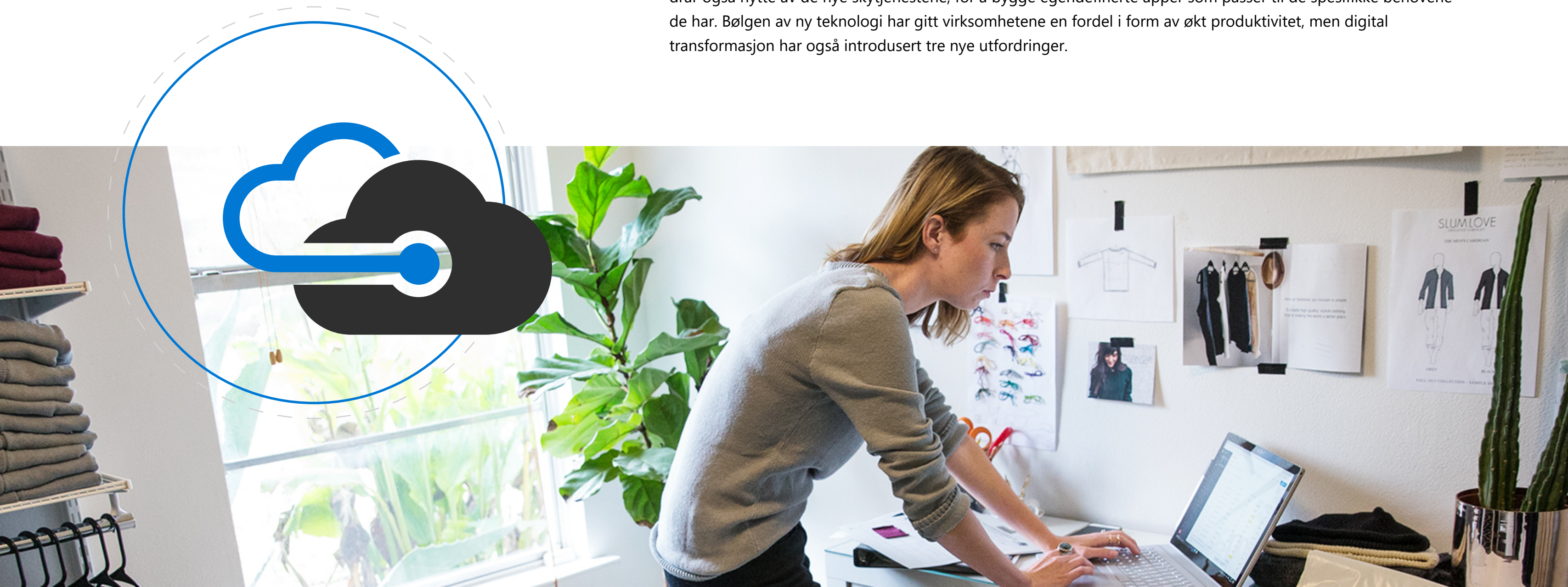
Del 1

Hva er Identitets-
og tilgangsstyring?

Hva er Identitets- og tilgangsstyring?

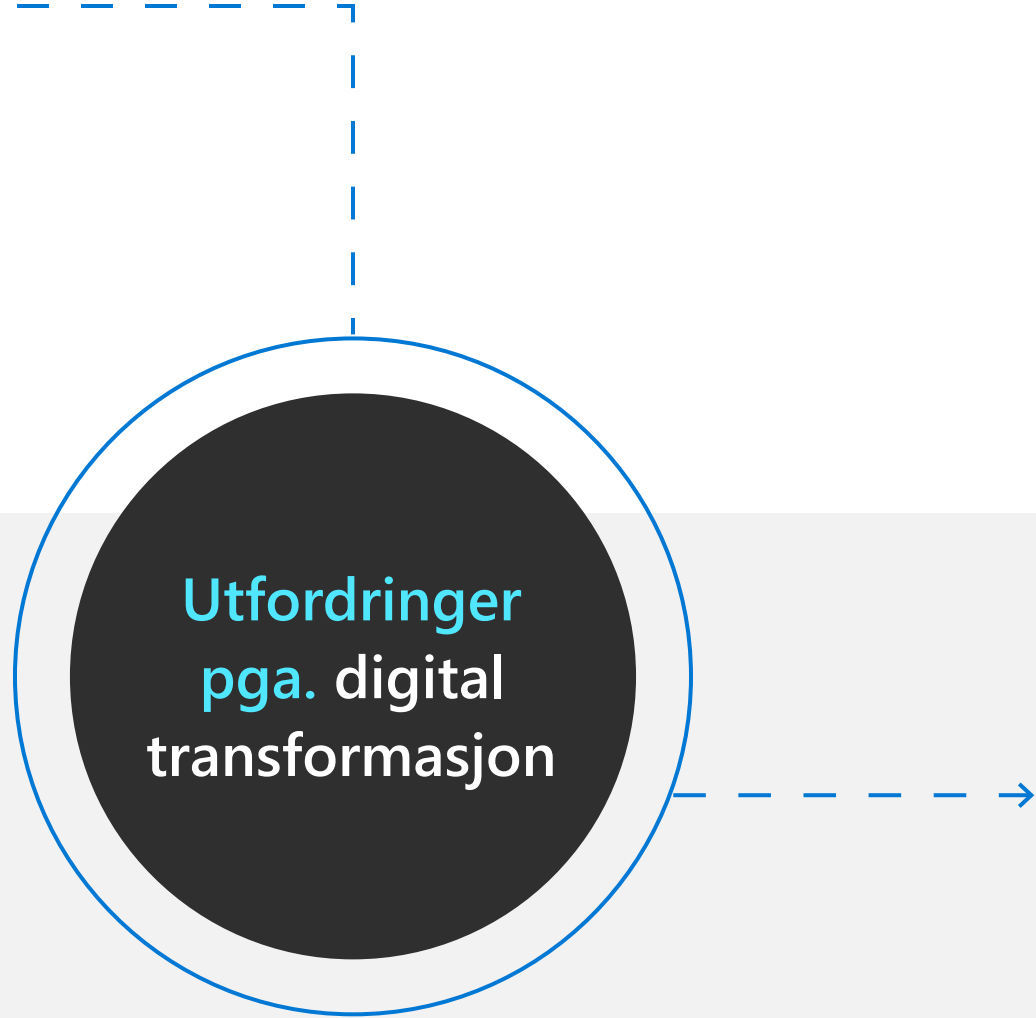
Digital transformasjon

Databehandling i skyen og mobile enheter har transformert den moderne arbeidsplassen. En stadig voksende global arbeidsstyrke har fleksibiliteten til å jobbe fra hvor som helst og bruke gratis og rimelig programvare, som tjenesteprogrammer (SaaS), for å løse produktivets- og samarbeidsutfordringer. Store virksomheter overfører programmer og behandling til skyen for å modernisere arkitekturen sin, og en rekke virksomhetslinjer drar også nytte av de nye skytjenestene, for å bygge egendefinerte apper som passer til de spesifikke behovene de har. Bølgen av ny teknologi har gitt virksomhetene en fordel i form av økt produktivitet, men digital transformasjon har også introdusert tre nye utfordringer.



Hva er Identitets- og tilgangsstyring?

Nye utfordringer



Utfordringer
pga. digital
transformasjon

Sikkerhetsrisiko: Før den skybaserte revolusjonen, fungerte IT som en teknisk portvakt. Appene og plattformene du administrerte og sikret, befant seg inne i perimeternettverket, og alle som logget seg på firmaets ressurser ble validert av brannmuren først. De dagene er over. Arbeidsstyrken din har nå mer kontroll over teknologien de bruker selv, og mye av dette er tilgjengelig via internett. Disse sårbarhetene har cyberangriperne lært seg å utnytte. Selv når en bruker vet det riktige passordet til en konto, kan du ikke alltid være sikker på at de er den de sier at de er.

Administrativ byrde: Eksplosjonen av sluttpunkter gir brukerne flere måter å koble seg til på, men dette skaper også et administrativt mareritt. Mange virksomheter er ikke klar over alle verktøyene de ansatte bruker, og selv om de har et godt utvalg verktøy selv, betyr likevel det store antallet skyapper at du må administrere flere identitetssystemer, øke kostnadene og behandle eksisterende sikkerhetsrisikoer.

Dårlig brukeropplevelse: Brukerne føler også denne smerten. De elsker fleksibiliteten det gir dem, men er frustrerte over alle påloggingslegitimasjonene de må å huske.



Sikkerhetsrisiko



Administrativ
byrde



Dårlig
brukeropplevelse

Hva er Identitets- og tilgangsstyring?

Identitets- og tilgangadministrasjon som det sentrale kontrollplanet

Fellesnevneren på tvers av disse smertepunktene er ineffektive systemer for å bekrefte identitet. Identitet har erstattet perimeternettverket som det nye kontrollplanet. Du trenger løsninger som kobler sammen forskjellige verktøy, arkitektur, enheter og tjenester i hele virksomheten, for å kunne beskytte organisasjonen bedre og administrere tilgangen for både ansatte og eksterne partnere. Dette er identitets- og tilgangs (IAM) -systemer som forener tilgang under ett system, noe som gir deg mer kontroll. De gir sømløst samarbeid på tvers av organisasjonens grenser, mens de forbedrer sikkerheten til firmaets ressurser. En god IAM-løsning lar deg koble brukerne dine til alle arbeidsprogrammene sine – enten de er i skyen eller på lokalt – via et sett med påloggingslegitimasjoner. IAM-løsninger er designet for å gi brukerne tilgang til bare de ressursene de trenger, og blokkere uautoriserte brukere fra å få tilgang til data de ikke burde ha. Du administrerer brukernes rettigheter og tillatelser fra en sentralisert portal, og reduserer mange av de manuelle prosessene som er involvert i klargjøring og avskaffing av brukerkontoer. IAM-løsninger gir også verktøy for å administrere sikkerhetspolicyer på tvers av identiteter og apper. De beste IAM-løsningene sikrer bedre identiteter, forbedrer brukeropplevelsen og øker administrativ effektivitet.

IAM-løsningene
løser disse
utfordringene



Bedre sikring
av identiteter



Forbedrer
brukeropplevelsen



Øker administrativ
effektivitet

Del 2

Oversikt over Azure AD

Oversikt over Azure AD

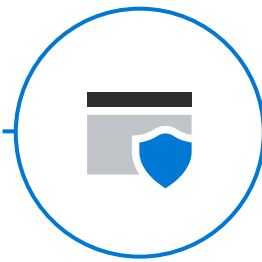
En omfattende løsning

Microsoft Azure Active Directory (Azure AD) er en omfattende IAM-løsning i skyen, og ledende på markedet for å administrere kataloger, gi tilgang til programmer og gi avansert identitetsbeskyttelse. Azure AD styrker organisasjonenes mulighet til å administrere og sikre identiteten til de ansatte, partnerne og kundene sine, slik at de alle får tilgang til appene og tjenestene de trenger. Azure AD hjelper millioner av organisasjoner med å administrere og sikre over en milliard identiteter.



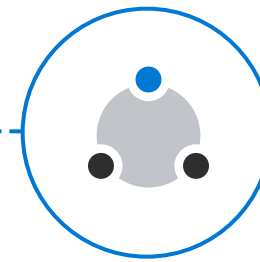
Moderniser tilgangen

Administrer og sikre tilgang til organisasjonens data og ressurser, lokalt og i skyen. Koble alle brukerne, applikasjonene og enhetene dine til skyen, for en sømløs, sikker tilgang og større synlighet og kontroll. Automatiser arbeidsflyter og aktiver selvbetjeningsalternativer for å holde kostnadene nede og forbedre produktiviteten for brukerne dine.



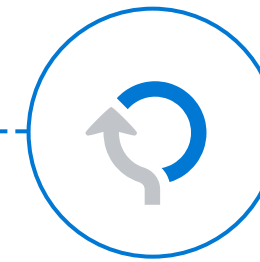
Sikre og styre

Med det høye volumet av angrep som skjer på påloggingslegitimasjonene hver dag, er måten å forhindre et sikkerhetsbrudd på, å kontinuerlig spore normal og unormal atferd på tvers av det bredeste settet av signaler som mulig, anvende kunstig intelligens og automatisere svarene. Balanser produktivitet og sikkerhet, med tidsstyrt tilgang til de riktige ressursene og regelmessige, åpne gjennomganger og håndhevelse av policyer.



Koble til og samarbeide

Utvid bedriften din med en pålitelig skytjeneste, som kan skalere bruken til millioner av brukere, med bransjeledende sikkerhet og fleksibilitet. Ta kontakt med de eksterne brukerne dine og styrk produktiviteten deres, med brukervennlige selvbetjeningsopplevelser og innebygde sikkerhetskontroller.



Utvikle og integrere

Bygg programmer som gir brukerne en enkel måte å logge på, enten ved hjelp av Microsofts personlige, arbeids- eller skolekonto eller via kontoen til de sosiale nettverkene deres. Begynn å koble til Microsoft Graph, porten til data og intelligens i Microsoft 365, og bygg opp rike programmer. Aktiver enkelt pålogging, automatiser brukerklargjøring og nå ut til verdens største organisasjoner.

Del 3

Azure AD for
programmene dine

Azure AD for programmene dine

En universell plattform

Azure AD lar deg administrere en felles identitet for hver bruker på tvers av hybridinfrastrukturen din, for å få tilgang til alle programmene de trenger, inkludert sky og lokale bedriftsprogrammer. Den administrerer alle identitetene dine fra en universell plattform, øker den administrative effektiviteten og gir deg mer kontroll. Den bruker detaljert sikkerhetspolicy på alle programmene som brukes i organisasjonen din.



Azure AD for programmene dine

Spas tid og penger

Azure AD er forhåndsintegrert med tusenvis av programmer, inkludert populære alternativer som Workday, ServiceNow, SuccessFactors, Adobe og Concur, noe som gjør det enklere for deg å gjøre disse appene tilgjengelige for brukerne dine. Med en konsoll, kan du distribuere konsekvente policyer og overvåke tilgangsrettighetene. Du kan automatisere arbeidsflyter for brukerklargjøring og livssyklusadministrasjon, og spare tid og ressurser med selvbetjening av kontoadministrasjon. Du kan også inkludere brukerinformasjonen fra HR-verktøyene som en kilde til sannhet, og eliminere behovet for tilpassede skript eller manuelle prosesser for å administrere brukeregenskapene.

Apper som er konfigurert gjennom Azure AD, aktiverer enkel pålogging (SSO) for sømløs tilgang, noe som betyr at brukerne ikke trenger å huske påloggingslegitimasjon for hver eneste appkonto, og heller ikke trenger å bruke svake passord om igjen, for slik å risikere et datainnbrudd. Kontoer som er konfigurert for automatisk klargjøring, gir brukere tilgang til nye ressurser så snart som mulig. Azure AD sikrer at de nyansatte har tilgang til alle relevante ressurser for den innkommende klargjøringen fra dag én.



**Sparing av tid
og penger**



**Innebygde SaaS-
integreringer**



Enkel pålogging



**Brukertilgang
fra dag én**

Azure AD for programmene dine

Skaffer deg den sikreste tilgang til alle appene dine

Azure AD gir deg omfattende identitetsbeskyttelse i alle appene dine – både SaaS-appene og de lokale bedriftsappene. Om brukeren ber om tilgang til Microsoft Word eller Box, spiller det ingen rolle, Azure AD sørger for at identiteten deres blir bekreftet før den gir tilgang. Du kan også innføre retningslinjer for tilgangspolicyer for å sikre at brukere bare har tilgang til det de trenger, når de trenger det. Du kan kreve at brukerne ber om tilgangstillatelse, du kan angi tidsbegrensning på hvor lenge de kan få tilgang til programmet og du kan gjennomføre regelmessige samsvarsvurderinger av tilgangen.

Azure AD utnytter også kraften fra Microsoft Intelligent Security Graph og maskinlæring for å analysere billioner av signaler på tvers av alle produktene og tjenestene våre, dette er for å avdekke atypisk oppførsel og tildele relativ risiko for hver økt. Azure AD ser på enheten, plasseringen og annen kontekstuell informasjon, for å evaluere risikoen for pålogging. Du kan opprette policyer for Azure AD Conditional Access, som automatisk tar i bruk sikkerhetstiltak, for eksempel å blokkere en tilgangsforespørsel eller kreve tilbakestilling av passord, når en pålogging anses som risikabel eller spesielle policyer for betingelser ikke er oppfylt.



**Sikkerhetstiltak
for søknader**



Identitetsbeskyttelse



**Få tilgang
til styring**



**Retningslinjer for
betinget tilgang**

Del 4

Hvordan administrere og sikre apper med Azure AD

Azure AD gjør det enkelt å holde kontroll og redusere kostnadene ved hjelp av automatisering, selvbetjening og håndhevelse av policy.

Hvordan administrere og sikre apper med Azure AD



Azure AD integrasjoner med apper

Programgalleriet til Azure AD, gjør det enkelt å konfigurere og koble til hvilken som helst av de tusenvis pre-integrerte appene til leietakeren din. Disse appene støtter alle en SSO-opplevelse, og det er enkelt å konfigurere appene for Azure AD Conditional Access, enten per app eller per virksomhetsdekkende policy. Når du har lagt til appen og konfigurert den etter dine behov, kan brukere med autorisert tilgang lett finne den i Azure AD My Apps-portalen, en sentralisert portal for oppdagelse og lansering av apper for sluttbrukere.

Hvis du har bygd en app eller trenger å integrere en for organisasjonen din, kan du også be om å få den oppført i programgalleriet for Azure AD.

[Utforsk tusenvis av forhåndsintegrerte apper >](#)



Sikker hybrid tilgang

Bruk Azure AD Application Proxy for å tilby en sikker, ekstern tilgang til kravbaserte lokale nettprogrammer, uten behov for VPN. App Proxy krever en enkelt installasjon av kontakten, og gir den samme IT- og sluttbrukeropplevelsen som SaaS-apper, koblet gjennom programgalleriet for Azure AD.

Eller hvis du vil utnytte eksisterende infrastrukturinvesteringer, for eksempel med partnere som F5 ZScaler, SAP, Oracle eller Ping Identity, for å koble til andre typer apper som de som bruker vertshodebasert eller Kerberos-godkjenningsprotokoller. Dette kan du fint gjøre, og du vil fortsatt oppnå de samme sentraliserings- og sikkerhetsfordelene som med Azure AD.

[Les hvordan du legger til en lokalt program gjennom App Proxy >](#)

[Koble til andre nettverk for partnerapper og skyer >](#)

Hvordan administrere og sikre apper med Azure AD



Automatisert klargjøring

Azure AD lar deg automatisere opprettelsen, vedlikeholdet og fjerningen av brukeridentiteter i populære SaaS-programmene. Når noen blir med i teamet eller organisasjonen din, kan du automatisk opprette nye kontoer for nye personer i de riktige systemene. Når personer forlater et team eller en organisasjon, kan du angi policyer som automatisk vil deaktivere kontoene deres fra de riktige systemene. Ved å automatisere disse oppgavene, kan du sikre deg at identitetene i appene og systemene dine alltid holdes oppdatert, enten basert på endringer i katalogen, eller via det menneskelige ressurssystemet, noe som reduserer feil og unødig tidsbruk.

[Finn ut mer om hvordan du konfigurerer automatisert levering og avskaffing av dette i SaaS-appene >](#)



Gruppeadministrasjon

Azure AD hjelper deg med å gi tilgang til organisasjonens ressurser. Dette gjøres ved å gi tilgangsrettigheter til enkelte brukere eller til hele Azure AD-grupper. Ved å bruke grupper, kan ressurseieren gi tilgangstillatelser for alle medlemmene i gruppen på én gang, i stedet for å måtte oppgi alle rettighetene en for en. Dette er en sikrere metode, ettersom det slik er mindre sannsynlighet for at du ved et uhell gir en individuell upassende tilgang, i tillegg til at det sparer deg for tid. Du kan også dynamisk skalere gruppeadministrasjonen din ved å få påmelding automatisert gjennom identitets- og attributtbaserte policyer.

[Lær hvordan du oppretter en gruppe i Azure-portalen >](#)

Hvordan administrere og sikre apper med Azure AD



Brukerbasert selvbetjening

Noen oppgaver krever ikke en IT-profesjonell for å fullføre, og Azure AD lar deg delegere disse til andre i organisasjonen. Du kan gi brukerne styrket mulighet til å opprette og administrere sine egne sikkerhetsgrupper i Azure AD. Gruppeeiere kan godkjenne eller avslå forespørsler om medlemskap, eller de kan delegere kontroll over gruppemedlemskapene.

[Konfigurer selvadministrerte grupper >](#)

Selvbetjening strekker seg også ut til brukerne. Brukere som har en bekreftet e-postadresse, kan registrere seg for en konto via selvbetjeningsportalen, denne portalen kan de senere bruke til å tilbakestille passordet. Dette kan spare brukerstøtteavdelingen din for utallige tid og penger.

[Konfigurer selvbetjening for tilbakestilling av passord >](#)



Moderniser autentisering

Hvis du for øyeblikket bruker en lokal godkjenning, som for eksempel Active Directory Federation Services (AD FS), kan du vurdere å overføre appene dine til Azure AD. Du beholder de samme brukerfordelene som ved SSO, men får skalerbarhet og sikkerhetsfordeler tilgjengelig fra skyen. Dette betyr for eksempel å bruke granulære tilgangskontroller per program ved bruk av Azure AD Conditional Access, eller å gi partnere tilgang til ressurser med Azure AD B2B-samarbeid. Apper som bruker SAML 2.0, WS-Federation, OAuth eller OpenID Connect-standarder for føderal pålogging, kan overføres.

[Bygg policyer for betinget tilgang til Azure AD, dette sikrer tilgang til appene dine >](#)

[Bruk Azure AD B2B for å samarbeide sømløst med de eksterne partnerne dine >](#)

Koble enhver app, uansett hvilken sky eller server de er på, til Azure AD på en sikker måte.

Én million aktive,
unike apper tilkoblet.

Kom i gang nå.

Start den én-månedes kostnadsfrie prøveperioden med Azure AD for å se hvor enkelt det er å administrere brukertilgang til alle appene dine og sikre virksomheten din.

