evelon

EN INNFØRING I MICROSOFT 365 BUSINESS PREMIUM

Den moderne arbeidsplassen hvor alt er koblet til skyen

Innhold

Innledning

Microsoft 365 Business Premium gir deg den moderne arbeidsplassen, en gjennomgripende forandring i måten du anvender digital teknologi på. Alt er koblet til skyen: brukere, maskiner, applikasjoner og data. Plattformen for produktivitet og samarbeid er overlegen, sikkerheten tilpasset ansatte som jobber når som helst, fra hvor som helst. Enheter og apper kan administreres uansett hvor de befinner seg. Det følger med grunnleggende funksjoner for informasjonsbeskyttelse og hindring av datalekkasje. Business Premium sørger for trygg tilgang, sikrer ansatte og beskytter bedriftsressurser.

Brukere logger på med passordløs godkjenning eller multifaktor-autentisering (MFA) og er umiddelbart produktive. Microsoft 365 Apps og et omfattende sett med nettbaserte verktøy lar dem oppnå «mer med mindre», takket være automatisering og kunstig intelligens. Det gir energi som styrker arbeidslyst og kreativ utfoldelse. Som administrator finner du deg raskt til rette. Admin-portalene er enhetlige og lett å forstå. Du får forenklede prosedyrer beregnet på småbedrifter. For vanskeligere oppgaver er det veivisere. Og du vil alltid få hjelp av oss i Evelon, din Microsoft-partner.

3 forskjellige pakker

Microsoft 365 Business finnes i tre utgaver. De henvender seg til små og mellomstore bedrifter (SMB) med opptil 300 brukere. Alle inneholder samme sikre skytjenester, som inkluderer Teams, Exchange, OneDrive og SharePoint.

Microsoft 365 Business Basic

Basic kommer med nett- og mobilversjoner av Outlook, Word, PowerPoint og Excel.

Microsoft 365 Business Standard

Standard legger til skrivebordsversjonene av Microsoft 365 Apps for Windows og Mac.

Microsoft 365 Business Premium

Premium tilføyer avansert sikkerhet og enhetsadministrasjon, samt Azure Virtual Desktop.

Dette får du med Microsoft 365:

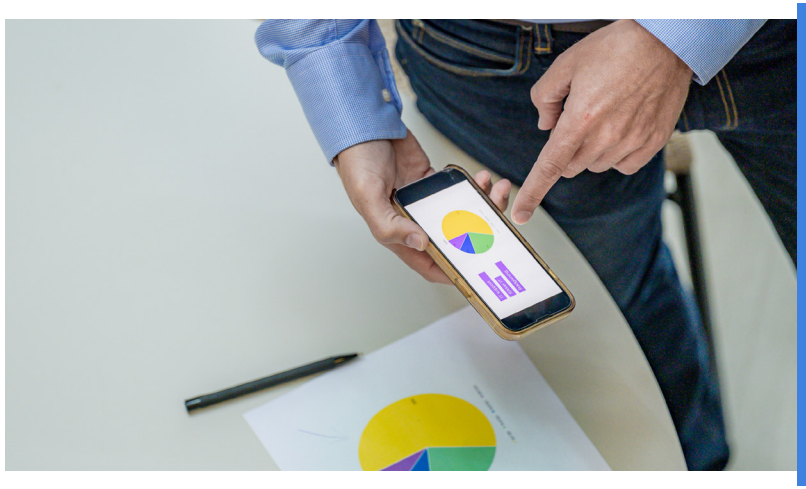
Samarbeid og kommunikasjon

Benytt Teams, en chattbasert arbeidsflate som danner knutepunktet for all intern samhandling i virksomheten. Du kan holde nettmøter og videosamtaler for opptil 300 personer på tvers av avdelinger og organisasjoner. Chat med team fra maskinen din på kontoret eller mens du er på farten. Samle alle chatter, møter, filer og apper til teamet ditt på ett sted, så det blir lett å komme sammen igjen og samarbeide. Du kan arrangere nettseminarer med påmeldingssider for deltakere, e-postbekreftelse og rapportering.

E-post og kalender

Hver bruker får en postboks på 50 GB pluss et arkiv på opptil 1,5 TB for langsiktig oppbevaring, med et regelsett for å overføre elementer som er eldre enn to år. Benytt egendefinerte domenenavn. Sett opp e-post for nye brukere, gjenopprett slettede kontoer. Bruk delte postbokser som er tilgengelig for flere, og rom- og ressurspostbokser for booking med automatiserte svar for ledig og opptatt tid. Administrer kalenderen, del tilgjengelige tidspunkter, planlegg møter og få påminnelser.

Filområder og intranett



Med SharePoint får du et system for å håndtere dokumenter som kan erstatte delte områder på en filserver og bidra til informasjonsflyt via kommunikasjonssider og nyheter. Opprett gruppe-områder med SharePoint for å dele informasjon, innhold og filer på intranettet. Samarbeid om prosjekter. Du får tilgang til dokumentene fra en hvilken som helst enhet.

Skylagring- og deling

OneDrive for Business dekker behovet for hjemmeområder og synkroniserer filer mellom sky og enheter. Du kan dele dokumenter internt og eksternt på en trygg måte. Det er 1 TB lagring per bruker. Jobb på filer, og lagre dem direkte i OneDrive eller SharePoint. Endringer oppdateres på tvers av synkroniserte enheter. Forsyn eksterne kontakter med gjestekoblinger til dokumenter. Del filer og send e-post på en sikker måte, så bare personer med riktige tillatelser får tilgang.

Microsoft 365 Apps

Skrivebordsversjonene er Office-pakken i skytilkoblet utgave med forbedret brukeropplevelse. Du får ferdig oppsatte og alltid oppdaterte versjoner av Word, Excel, PowerPoint, Outlook og OneNote for Windows eller Mac (også Access og Publisher på PC). Hver bruker kan installere Office-appene på opptil fem PCer eller Macer. Alle har tilgang til nettutgavene og kan installere mobilappene på opptil fem mobiler og fem nettbrett. Det er støtte for samtidig sanntidsredigering.

Andre inkluderte apper

Stream er bedriftens tjeneste for å lage videoer, ta opp Teams-møter og holde direktesendinger. Yammer gir muligheten til å formidle ideer, stille spørsmål og føre diskusjoner på en sosial nettverkstjeneste. Bookings lar deg lage en landingsside hvor (mulige) kunder kan velge ulike tjenester og bestille en avtale eller avtale tid for en samtale. I tillegg finner du et 20-talls nettbaserte apper, som Whiteboard (lerret i friform) og Planer (prosjektstyring).

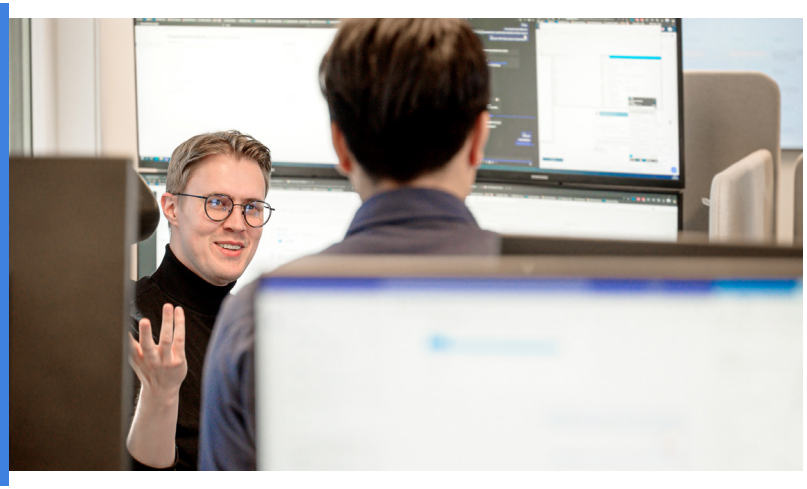
evelon

Verktøy for å bygge og administrere bedriften

Bruk Microsoft Forms til å samle tilbakemeldinger fra kunder og medarbeidere. Bruk Visio på nettet til å opprette profesjonelle diagrammer og flytskjemaer som kan deles og redigeres samtidig. Bruk Teams til å planlegge tidsplaner og daglige gjøremål. Med Microsoft Lister kan du spore informasjon og arbeid som er av størst betydning for teamet. Sørg for personlig vekst hos dine ansatte og styrk mennesker og team til å være på sitt beste med Viva.

Azure Active Directory

Det er det skybaserte motstykket til Windows AD og inneholder en rekke avanserte sikkerhetsmekanismer som beskytter mot identitetsangrep, så som passordbeskyttelse, multifaktor-autentisering (MFA) og passordløs godkjenning, samt selvbetjent tilbakestilling av passord. Betinget tilgang lar deg angi hvem som skal ha adgang inn i organisasjonen din, basert på bruker og gruppetilhørighet, enhet og helsetilstand, geolokasjon og sted pluss applikasjon. Du kan synkronisere lokalt AD mot Azure AD, så brukere autentiserer seg med samme legitimasjon og engangspålogging.

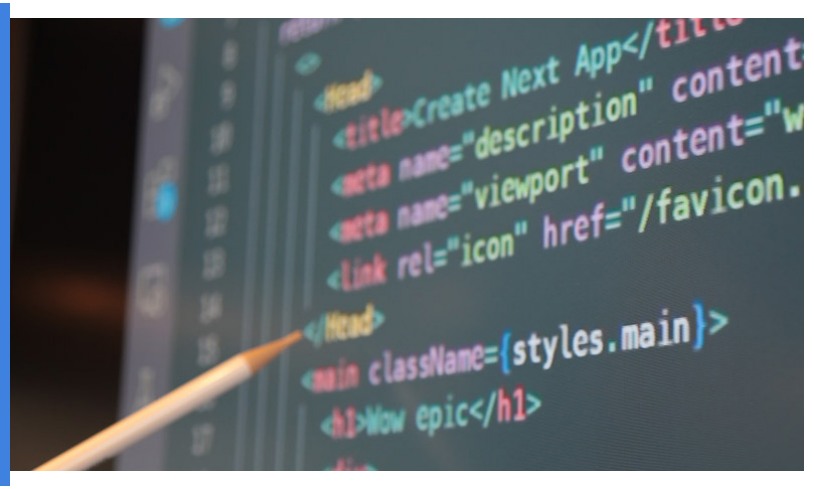


Administrasjon av datamaskiner og mobilenheter

Microsoft Intune bidrar med mobil enhets- og applikasjonsbehandling. Alle enheter bør innrulleres her, så du kan administrere og sikre dem med bunnlinjer for sikkerhet, konfigurasjonsprofiler og policyer for samsvar. Du kan rulle ut programvare og holde den oppdatert. Du kan fjernslette bedriftsdata og -apper om enheter går tapt. Det er støtte for både bedriftseide og private mobilenheter (BYOD).

Avansert trusselbeskyttelse

Exchange Online Protection avviser hovedtyngden av uønsket e-post ved inngangsdøren, skanner meldinger med tre virusmotorer og beskytter mot utbredte phishing-angrep. Defender for Office 365 forbedrer phishing-beskyttelsen med maskinlæring, undersøker koblinger idet du klikker på dem, og analyserer vedlegg før de ender opp i innboksen. Defender for Business sørger for markedsledende endepunktsbeskyttelse på tvers av datamaskiner og mobilenheter (EDR). Cloud App Discovery lar deg oppdage skygge-IT.



Informasjonsbeskyttelse og hindring av datatap

Med Microsoft Purview kan du manuelt klassifisere, merke og kryptere dokumenter og e-post. Du kan blokkere for utilsiktet og tilsiktet datalekkasje. Det er funksjoner for automatisert oppbevaring og sletting av data, eDiscovery og rettslig sperre.

Azure Virtual Desktop

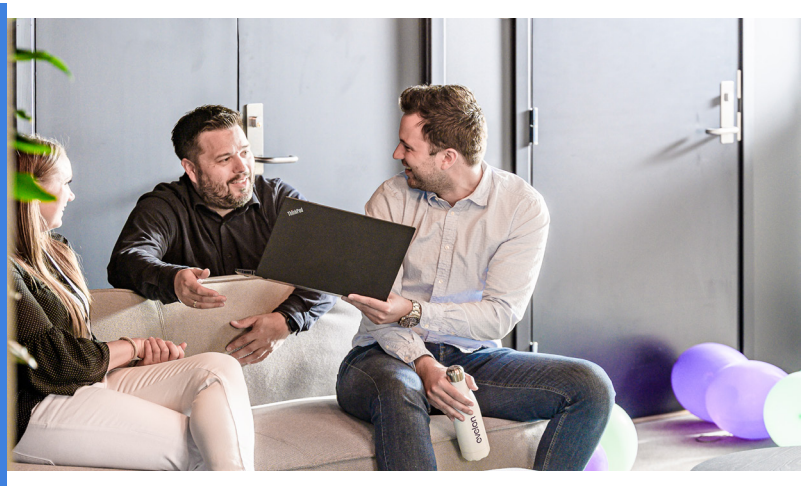
La dine ansatte jobbe på virtualiserte Windows 11-skrivebord i skyen i stedet for på usikrede maskiner. Klientstøtten inkluderer Windows, Mac, iOS, Android og HTML5. Det er innebygd intelligent sikkerhet. Hold programmer og data trygge og i samsvar med funksjoner som proaktivt oppdager trusler og foretar korrigerende tiltak.

Universell utskrift

Ta i bruk en skybasert utskriftsløsning som muliggjør enkle, omfattende og sikre utskrifter. Den sparer tid og arbeid for IT-avdelingen. IT registrerer skrivere i Azure AD og publiserer egenskaper og lokasjon. Brukere kan få opp forhåndskonfigurerte utskriftsenheter som er i nærheten, legge til ønsket skriver og skrive ut. IT administrerer enhetene og mottar rapporter og innsikt i bruk.

Støtte og distribusjon

Microsoft gir kundestøtte via nett og telefon døgnet rundt, men du vil som regel være bedre ute ved å ha en avtale med Evelon, din lokale Microsoft-partner som kjenner miljøet ditt og er i din geografiske nærhet på Østlandet. Det vil gå kjappere og foregå på norsk. Selskapets økonomisk understøttede oppetidsgaranti er 99,9 %. Business Premium kan innenfor virksomheten kombineres med andre abonnementer. Du kan for eksempel sette opp 300 brukere med Business Premium og 100 med Microsoft 365 E5.



01

Samarbeid i sanntid

Microsoft 365 er verdens produktivitetssky. Visjonen er å få hver person og hver organisasjon på kloden til å oppnå mer. Det omfatter oppgaver du utfører i dag og ting du aldri har gjort før. Med Microsofts egne ord: Plattformen kan bidra til å gjøre små bedrifter og større konserner mer produktive og konkurransedyktige, ideelle foreninger og offentlige kontorer mer effektive og responsive. Den kan styrke læring i skolen og på universiteter og åpne for nye muligheter innen helsevesen og forskning.

Microsoft 365 Apps

Skrivebordsversjonene av Microsoft 365 Apps deler kodebase med Office 2021, men er forskjellige ved å være skytilkoblet. Samtidig vil Office-brukere umiddelbart finne seg til rette. Mens Office 2021 bare oppdateres med sikkerhetsfikser og feilrettinger, er Microsoft 365 Apps «evig grønne», stadig forbedret med nye funksjoner og verktøy. Dokumenter i Word, Excel og PowerPoint som ligger i OneDrive eller SharePoint, lagres automatisk. Du angrer endringer ved å klikke på den avrundede pilen til høyre for lagringsikonet eller ved å gå tilbake i versjonshistorikken. Du sender ikke lenger dokumenter som vedlegg, men deler dem, i hvert fall internt. Og du kan redigere filer i sanntid sammen med andre.

Word, Excel, PowerPoint og Outlook har følsomhetsetiketter for å klassifisere, merke og kryptere data. Oppbevaringsetiketter angir retningslinjer for å håndheve innstillinger for oppbevaring og sletting. OneDrive brukes som hjemmeområde, SharePoint til delte prosjekter. Med sentralisert skylagring kan du bli fleksibel og produktiv i en hybrid hverdag. Opprett og skriv på et dokument på PCen din på kontoret, jobb videre med det på din Mac hjemme. Sett deg i godstolen og les det igjennom på et nettbrett. Foreta siste redigeringer på mobilen mens du sitter på bussen neste morgen.

Kunstig intelligens (KI) med maskin- og dyplæring gjennomsyrer i stadig høyrere grad miljøet. Det finner nedslag i Microsoft 365 Apps, tjenester og sikkerhetsfunksjoner. Stavekontrollen er kraftig forbedret ved å bruke KI for å gjenkjenne og tilby rettelser for stave- og grammatikkfeil. I flere Office-apper kan du diktere. Word oversetter mellom ulike språk. PowerPoint kan lære deg opp i å holde mer effektive presentasjoner og har KI-medhjelpere for profesjonelle forslag til plassering av tekst og billedstoff. Stream har tale-til-tekst-transkripsjon og analyserer lydfrekvenser for å skille ut bakgrunnsstøy.

Microsoft Edge

Microsoft Edge fungerer like godt på en Mac som på Windows, Android, iOS/iPadOS og Linux. Edge er basert på samme Chromium-motor som i Chrome, men bruker markant mindre minne. Nettleseren er godt integrert i Microsoft 365. For Windows kan du konfigurere den ved hjelp av Intune med anbefalte sikkerhetsinnstillinger. Du kan kjøre Edge i en virtuell maskin mot utrygge nettsteder, som beskytter mot skadevare som lastes ned i bakgrunnen. Klikk på terningen til venstre for å få frem nettappene. For adressefeltet kan du endre søkemotoren til Google. Men i søkeboksen må du holde deg til Bing. Der kan du til gjengjeld også lete etter intern informasjon i bedriften, en funksjon mange har savnet.

Visste du at

Microsoft..

.. har utviklet seg fra skyleverandør med enkelte sikkerhetsløsninger til ett av verdens ledende sikkerhetsselskap.

Microsoft Teams

Teams er egentlig ikke en applikasjon i seg selv. Den består av et flettverk av mikrotjenester som kjører oppå Exchange og SharePoint, grunnsøylene for samarbeidsplattformen i Microsoft 365, med en Skype-motor i bakgrunnen. Derfor vil du aldri kunne få en lokal Teams-server. Filer peker på OneDrive og SharePoint, Wiki på en integrert app, Kalender på Outlook med Exchange og Møteopptak på Stream. Nye hybride arbeidsmønstre gjør det utenkelig å gå bort fra all funksjonalitet Teams gir. Det naturlige stedet å starte dagen på er i Teams. Se hva som står på i kalenderen, som er synkronisert med Outlook (og Exchange). Sjekk om det er noen svar i chattene du deltar i, som kan være én-til-én-kommunikasjon eller i grupper. Det kan ha dukket opp offentlige kunngjøringer som angår hele virksomheten, eller nye meldinger i teamene du er medlem av. Videomøter er en del av hverdagen, og det er ikke alltid tidspunktet passer. Spill av møteopptaket om det er informasjon der som du trenger.

Du kan ha et samarbeidsprosjekt som involverer flere filer som lagres i en Teams-kanal, med research der dere benytter wikier og en delt OneNote. Dere kan være flere om å redigere samme dokument samtidig. Chatter kan lett gå over i video-anrop og skjermdelinger. Teams kan integreres med innebygde apper som Planer for prosjektstyring, tredjepartsapper fra et stadig økende galleri og egenutviklede applikasjoner i Power Platform som krever ingen eller lite kode. Teams kan kort og godt tilpasses virksomhetens behov. Den kan faktisk erstatte ditt telefonisystem.

Visste du at

Microsoft Teams..

..er den raskest voksende forretningsappen i Microsofts historie. Antallet aktive brukere steg fra 20 millioner i november 2019 til 75 millioner i april 2020 som følge av korona og nedstengning.

Exchange Online og Outlook

Exchange sammen med Outlook lar deg administrere din tid og føre en målrettet kommunikasjon. Planlegg og delta i møter enten via Outlook eller Microsoft Teams. Send beskyttet e-post. Dra nytte av et avansert og omfattende sett med sikkerhets- og samsvarsfunksjoner for e-post og vedlegg. Microsoft refererer til Outlook og Teams som de to knutepunktene for kommunikasjon og samarbeid. Begge er barn av sin tid. Outlook er eldre og skapt for å ta seg av mer formell og strukturert e-post. Den har funksjoner som kalendere, møtebooking, kontakter, oppgaver og notater – mens delte postbokser og fellesmapper sørger for informasjonsdeling og arbeidsflyt.

Teams representerer en ungdommelig livsfølelse, tydelig inspirert av ledigere omgangsformer på sosiale medier og direktemeldingsapper. Programmerbare fellesmapper i Outlook har utspilt sin rolle. Teams kan ikke sende e-post, bare motta dem i kanaler. Dermed blir det lite eller ingen overlapp mellom Outlook og Teams. Outlook fortsetter som e-postklient og personlig informasjonsmanager. Teams benyttes til uformell internkommunikasjon, gruppearbeid og det du ellers har brukt Skype for Business til. Samtidig vil du oppdage at innboksen din fylles opp med langt færre interne meldinger.

Visste du at

Exchange Online og Outlook ..

.. i hovedsak er din e-post og kalender? Exchange Online konfigurerer e-post i transitt, inkludert DLP-policyer, justerer beskyttelsen mot spam, skadelig programvare, phishing og forfalskning, og konfigurerer avansert trusselbeskyttelse- og intelligens.

SharePoint Online

SharePoint er et effektivt system for å håndtere dokumenter og interne nettsteder. Det har to primære formål. Du kan opprette gruppeområder som kobler deg og grupper til delt innhold og ressurser, så dere kan samarbeide om prosjekter og ha filområder som erstatter lagring på en lokal filserver. Du kan bygge kommunikasjonsområder for å formidle og kringkaste informasjon, så som nyheter, rapporter og statusoppdateringer. Sikkerheten er robust nok til å ta hånd om sensitive og sterkt klassifiserte data.

Du kan koble til en Microsoft 365-gruppe for å gi tilgang til grupperessurser, som en felles postboks og kalender, en OneNote med mer. For hvert nettsted opprettes det et dokumentbibliotek. Det gjør det lettvint å organisere og finne frem til innhold, samtidig som det er gode søkemuligheter takket være indeksering i bakgrunnen. Å legge til filer eller flytte dem mellom mapper er like enkelt som å dra og slippe dem fra ett sted til et annet. Du får tilgang til dokumentene fra en hvilken som helst enhet.

Visste du at

med SharePoint..

.. så kan du lage attraktive, funksjonsrike nettsider direkte i Sharepoint for team og kommunikasjon. Bruk samme sikkerhets- og samsvarsfunksjoner på tvers av filer, enten de er opprettet gjennom Teams eller direkte i SharePoint.

OneDrive for Business

OneDrive for Business er hjemmeområdet for alle brukere og erstatter fullt og helt din gammeldagse filserver med funksjoner du bare kunne drømt om. OneDrive lagrer og synkroniserer filer i skyen. Det gir deg tilgang fra PC, Mac, mobil eller nettbrett. Uten en Internett-forbindelse kan du jobbe med lokale filer. Straks du er tilkoblet igjen, samkjøres endringene med skylageret. Du vil typisk sette opp OneDrive til automatisk å laste ned filer ved behov. Da har du dokumentene du arbeider med, og du får frigjort diskplass. En annen mulighet, som ikke er anbefalt, er å laste ned alle filer og alltid beholde dem på enhetene. Du kan også sikkerhetskopiere lokale data til OneDrive.

OneDrive og OneDrive for Business har felles navn. Begge sørger for skylagring. Men der slutter også likhetspunktene. OneDrive er konsumentversjonen som benyttes til personlige data, og som brukere har full kontroll over. OneDrive for Business kontrolleres av virksomheten og er fullstendig forskjellig i funksjonalitet. Den er ment å gjøre det mulig for ansatte å dele og samarbeide om dokumenter med andre medarbeidere og administreres av organisasjonen. Du har mer detaljert styring over hvem som har tilgang til hvilke dokumenter, og handlingene som kan utføres på dem.

Visste du at

OneDrive for Business..

..er individuell skybasert fillagring? Brukere kan få tilgang til OneDrive-mappene sine fra mange steder, inkludert Microsoft Teams.

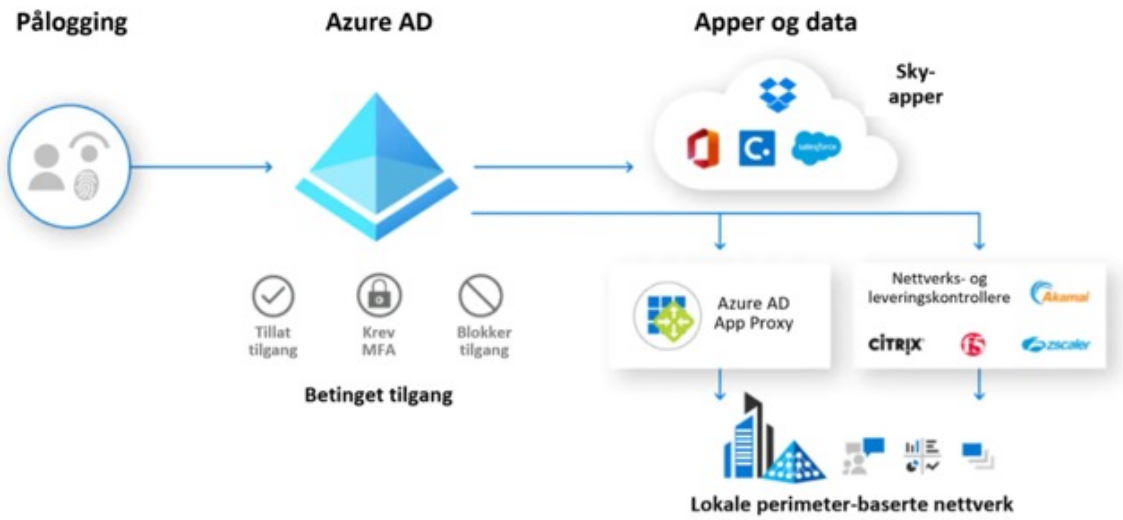
02

Sikkerhet og trusselbeskyttelse

Business Premium leverer flere sikkerhetsfunksjoner enn Microsoft 365 E3 til en betydelig lavere pris. Du får et solid forsvar mot cybertrusler og et robust og motstandsdyktig miljø. Det er en totalpakke som inneholder det meste mindre virksomheter trenger av generelle digitale verktøy. Det gjør Business Premium til Evelons kjerneprodukt for SMB-segmentet. Vårt bidrag er å tilføre omfattende erfaring og kompetanse som kan hjelpe deg med å håndtere sikkerheten.

Beskytt identiteter og ekstern tilgang

Ansatte jobber på tvers av organisasjoner og utenfor huset. Stadig flere er sjelden eller aldri innom bedriftsnettverket. Lokale applikasjoner fases ut og erstattes med skytjenester. Angriperne bryter seg i mindre grad inn i virksomheten, men logger på med rappet legitimasjon. Dette gjør tradisjonell nettverksbeskyttelse av bedriftsressurser mindre effektivt og krever andre sikkerhetstiltak. Den nye sikkerhetsperimeteren eller kontrollplanet er identiteten, det eneste konstante med ansatte som befinner seg hvor som helst og jobber på nær sagt hva som helst.



Miljøet behøver ikke omfatte mer enn en liten organisasjon som bare bruker skyappene som følger med Microsoft 365 Business Premium. Det kan være utvidet med tjenester i Azure eller tredjeparts skytjenester. Det kan være hybrid, kombinert med et lokalt perimeterbasert nettverk. Modellen for å beskytte virksomheten er identitetsdreven, sentrert rundt tilgangen til bedriftsressurser.

Betinget tilgang

Mekanismen har likhetstrekk med en dørvakt på et utested. Han kontroller om du er gammel nok, ikke er overstadig beruset eller utagerende, og at klærne svarer til kodeksen for etablissementet. Om t-skjorten er fillete, vil dørvakten si: «Sorry, kompis. Kom deg hjem og få på deg finstasen.»

For en bruker kan det bety at hun befinner seg på et ikke-godkjent nettverk, for en enhet at den ikke er i samsvar med virksomhetens retningslinjer. Sånn sikrer du at bare godkjente brukere på tiltrodde enheter med klarert programvare kommer inn i virksomheten. Alle andre stenges ute allerede ved inngangsdøren.

Betinget tilgang er hjørnesteinen i Microsofts sikkerhetsmodell og implementering av Zero Trust:

- Bruker og stedsbasert. Hold følsomme data beskyttet ved å begrense brukertilgang basert på geolokasjon eller IP-adresse med stedsbaserte policyer for betinget tilgang.
- Enhetsbasert. Sørg for at bare registrerte og klarerte enheter får tilgang til bedriftsdata med enhetsbasert betinget tilgang.
- Applikasjonsbasert. Arbeidet behøver ikke stoppe opp når bruker ikke er på bedriftsnettverket. Sikre tilgang til bedriftsskyen og lokale apper og opprettholde kontroll med betinget tilgang.
- Risiko-basert. Beskytt dine data mot ondsinnete hackere med risikobaserte policyer som kan brukes på alle apper og alle brukere, enten lokalt eller i skyen (krever Azure AD Premium P2).

Sikkerhetsstandarder

Nye Microsoft 365-organisasjoner er satt opp med Sikkerhetsstandarder, som gir en god idé om hva Microsoft anser for å være beste praksis. De sørger for enhetlig registrering av MFA og krever at administratorer alltid skal benytte MFA, brukere bare ved faresignaler. Det gjelder for tilgangen til alle skyapper. Eldre protokoller blokkeres. Men standardene tillater ingen tilpasninger og er ikke kompatible med betinget tilgang eller identitetsbeskyttelsen i Azure AD. Blokkering av SMTP kan skape problemer for multifunksjonsskrivere og skannere. Som annen faktor støttes bare Authenticator.

Betinget tilgang med MFA

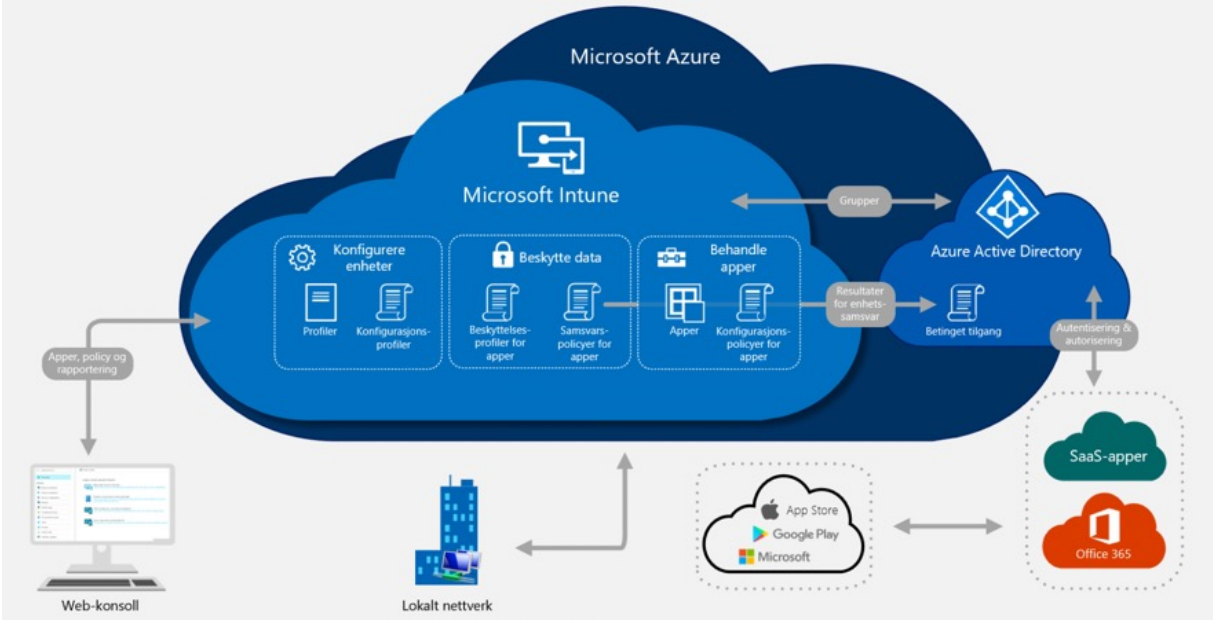
I Business Premium deaktiverer du Sikkerhetsstandarder og gjenskaper reglene de implementerer med Betinget tilgang. Nå kan du legge til unntak og plusse på med andre retningslinjer. Du vil typisk kreve at enhetene brukere logger på fra, er registrert i Intune og er i samsvar. Du blokkerer for påloggінger fra fiendtligsinnete land. Som en forlengelse av MFA setter du opp passordløs pålogging med Hello for Business eller Authenticator. Så kan du skrittvis forfine regelsettene med tilgangen til kritiske systemer.

Passord og passordløst

Azure AD klarer seg ikke uten passord ennå. Med passordløst slipper du oppgi det, annet enn i spesielle tilfeller. Azure AD Password Protection lar deg oppdage og blokkere kjente svake passord og deres varianter. Det kan ytterligere sperre for passord som er spesifikke for virksomheten din. Her kan du konfigurere smart utstenging etter et gitt antall mislykkede påloggingsforsøk og hvor lenge du må vente før du kan prøve på nytt. Du bør rulle ut tjenesten Selvbetjent tilbakestilling av passord. Det sparer IT for mye arbeid og gjør det lettere for brukere.

Sikre og behandle enheter

Til forskjell fra Windows Active Directory (AD) har Azure AD ingen innebygde funksjoner for å forvalte datamaskiner. Til gjengjeld kommer Microsoft 365 Business Premium med Microsoft Intune, selskapets markedsledende plattform for mobil enhets- og applikasjonsbehandling. Den lar deg administrere maskiner med Windows, macOS og Linux, samt mobilenheter med Android og iOS/iPadOS – uansett hvor de befinner seg, så sant de er koblet opp mot Internett.



Samtidig har Intune utviklet seg til en stadig voksende produktfamilie for alt innen skyadministrasjon av endepunkter. Microsoft er i full gang med å videreutvikle infrastrukturen som driver Intune, ved å bruke datavitenskap og kunstig intelligens (KI). Sånn kan de levere styrket endepunktsbeskyttelse og -samsvar og utnytte datadrevne muligheter, som intelligent automatisering og utbedring. Intune sentraliserer og forenkler verktøy, styrker sikkerheten og reduserer de totale eierkostnadene.

Du konfigurerer enheter ved hjelp av **konfigurasjonsprofiler**, ikke ulikt gruppepolicyer. Du sikrer data med **beskyttelsespolicyer** for apper og **samsvarspolicyer** for enheter. Intune lar deg rulle ut apper, holde dem oppdatert og tilpasse dem med **konfigurasjonspolicyer**. Du administrerer Intune i portalen for Endepunktbehandling. Det er full støtte for hybride miljøer med lokalt Windows AD.

Med Intune kan du distribuere apper fra Apple App Store, Google Play og Microsoft Store. Azure AD godkjenner og autoriserer brukere når de benytter applikasjoner fra tredjeparter og i Microsoft 365. Med det følger alle sikkerhetsmekanismer i identitetstjenesten, som engangspålogging, MFA og ulike former for identitetsbeskyttelse. Kombinert med Intune blir enheten til en identitet i tillegg til bruker. Du behøver ikke nærme deg enheter fysisk. Det gjør det til et ideelt verktøy for å forvalte maskiner som sjelden eller aldri er innom virksomheten. Intune gir detaljerte opplysninger om maskinvare og installerte programmer. Du kan sette opp varsler og ta ut rapporter, blant annet om enhetene er i samsvar med retningslinjene dine.

Intune lar deg distribuere sertifikater, VPN-profiler og Wi-Fi-konfigurasjoner. Med Premium-løsningen som skal være klar i mars 2023, vil du blant annet få fjernhjelp med støtte for lyd, så det blir lett for IT-teknikere og brukere å samarbeide om å fikse feil på enheter. En annen funksjon er administrasjon av endepunktprivilegier, som gir sluttbrukere lokale administratorrettigheter ved behov. Det er annonsert endepunktsanalyse og app-patching med mer.

Forsvar deg mot cybertrusler

Microsoft 365 Defender er sikkerhetssentret i Business Premium. Det svarer på trusler og administrerer sikkerhet på tvers av identiteter og enheter, applikasjoner og data. Hendelser samler opp varsler fra de ulike Defender-produktene og ordner dem til meningsfulle ende-til-ende-angrepshistorier. Sånn inngår alle varsler ovenfor i én og samme hendelse, noe som reduserer arbeidskøen og forbedrer hastigheten på undersøkelsen. Defender for Office 365 og Defender for Business er integrert i en koordinert pakke som sørger for utvidet oppdagelse og respons (XDR). Det gir forbedret datadekning, kombinert med behandling av hendelser, automatisk undersøkelse og utbedring.

Automatiserte angrepsavbrudd isolerer automatisk infiserte enheter og blokkerer kompromitterte brukere under et pågående angrep. Gjentatte angrep hindres med en ny metode for **prioriterte sikkerhetsanbefalinger** basert på trusseletterretning og beste praksis. Det følger med **kontekstsensitive brukanvisninger** som holder deg i hånden og gir veiledning når du må løse sikkerhetshendelser.

Defender for Business

Defender for Business leverer endepunktsbeskyttelse i verdensklasse, langt mer enn tradisjonell virus- og trusselbeskyttelse. Det er en omfattende plattform som forebygger og beskytter mot angrep på alle dine enheter, med støtte for Windows, macOS, Android og iOS/iPadOS. Du får verktøyene du trenger for å oppdage, etterforske og utbedre sikkerhetsbrudd på endepunkter. Defender for Business opererer proaktivt, i sanntid og reaktivt.

Den består av fem komponenter:

- **Trussel- og sårbarhetsadministrasjon** hjelper deg med å oppdage og utbedre sårbarheter i programvare og feilkonfigurasjoner.
- **Angrepsflatereduksjon** gjør deg motstandsdyktig overfor typiske tekniker som benyttes ved cyberangrep.
- **Neste generasjons beskyttelse** sørger for avansert virus- og trusselbeskyttelse basert på virusdefinisjoner, samt lokal og skybasert analyse og maskinlæring.
- **Endepunktdeteksjon og respons** lar deg identifisere vedvarende trusler og fjerne dem.
- **Automatisert undersøkelse og utbedring** jobber 24/7 med å bekjempe angrep ved hjelp av kunstig intelligens, noe som reduserer varslingsvolumet.

Onboarding og administrasjon av enheter er forenklet. **APIer og integrasjon** automatiser arbeidsflyter og innlemmer data i eksisterende sikkerhetsplattformer og rapporteringsverktøy.

Visste du at?

Angripere bryter seg ikke inn i virksomheten lenger – de logger på med stjålen legitimasjon

Defender for Office 365

E-post er fortsatt den mest utbredte metoden for å innlede angrep og trenge inn i en virksomhet. Alle innkommende og utgående meldinger filtreres gjennom flere lag i Exchange Online Protection (EOP). Det skjermer organisasjonen mot skadelig programvare, søppelpost og phishing. Defender for Office 365 utvider beskyttelsen til å dekke mer avanserte former for nettfiske og angrep med ukjent skadevare (nulldagstrusler). Dessuten beskytter den også lagringsområder i SharePoint, Teams og OneDrive.

Defender for Office 365 omdirigerer vedlegg som ikke er fanget opp av antivirusfiltret og åpner dem i et detonasjonskammer, en container som kjører i Azure. Der undersøkes de ved hjelp av maskinlærings- og analyseteknikker for å oppdage om de inneholder kode med ondsinnete hensikter. Hvis ingen mistenkelig aktivitet blir oppdaget, frigis meldingen. Microsoft opererer med en stadig oppdatert liste over skadelige koblinger, men undersøker dem i tillegg i sanntid idet du klikker på dem. Angripere sender ofte først uskyldige lenker som passerer gjennom e-postkontrollen, for så å endre dem.

Beskytt følsomme data

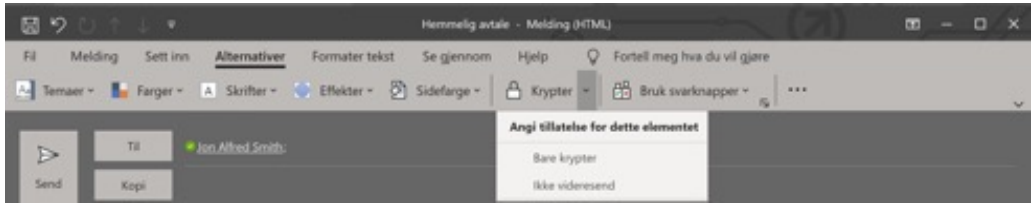
Microsoft Purview Informasjonsbeskyttelse lar deg manuelt klassifisere, merke og beskytte dokumenter og e-post. Du benytter følsomhetsetiketter for å legge til topp- og bunntekster eller vannmerker.
For sensitiv informasjon vil du ofte kryptere og angi detaljerte rettigheter til innholdet. Da fungerer merkelappene som en overbygning for Azure Rights Management (Azure RMS), en teknologi for å beskytte og styre rettigheter til følsomme data. Den har fellestrekk med digital rettighetsadministrasjon (DRA), som har som mål å begrense bruksmulighetene til opphavsrettsbeskyttet informasjon. Når du leier en film på nettet, får du lesetilgang i en begrenset tidsperiode.

Azure RMS opererer på samme vis. Du kan på en finmasket måte bestemme hva andre kan gjøre med et dokument eller en e-post. Du angir hvem som skal ha tilgang, og hva slags: lese, endre eller full kontroll. Du kan la tilgangen til dokumenter utløpe på en bestemt dato. Du kan tillate eller nekte personer å skrive ut eller kopiere innhold. Du kan kreve at bruker er tilkoblet når dokumentet åpnes, og du kan tilbakekalle rettighetene. Du kan bruke følsomhetsetikette på data som er opprettet i Word, Excel, PowerPoint og Outlook på alle plattformer. Outlook støtter ikke vannmerker.

Visste du at?
Multifaktor-autentisering (MFA) beskytter mot 99,9 % av identitetsangrep

Office 365-meldingskryptering

E-post mellom Microsoft 365-organisasjoner overføres alltid over krypterte linjer. Exchange Online Protection (EOP) forsøker å sette opp en sikker forbindelse til e-postsystemer utenfor Microsoft-skyen. Overfor partnere kan den tvinges frem med tvungen TLS. En annen mulighet er å benytte Office 365-meldingskryptering, som sørger for trygg ende-til-ende-kommunikasjon.



Outlook og Exchange samarbeider med Azure RMS og bruker to RMS-maler for å kryptere meldinger. Under fanen Alternativer kan du klikke på Tillatelse og velge opsjonen Bare krypter, som innebærer: Krypter melding og vedlegg. Gi mottaker retten til å dekryptere e-posten og gjøre med den hva hun vil. Her kunne vi også valgt Ikke videresend, noe som koder e-postmeldingen, men pålegger restriksjoner. Meldingene kan leses og besvares av alle autoriserte mottakere, uavhengig av e-postsystem.

Administrasjon av brukere

Du benytter Azure Active Directory (AD) for identitets- og tilgangsstyring, det skybaserte motstykket til Windows AD. Til tross for navnelikheten er katalogtjenesten veldig forskjellig. Azure AD er basert på åpne standarder og har innebygde sikkerhetsmekanismer som sørger for minst like trygg tilgang til apper og data over et åpent, fiendtlig Internett som på bedriftsnettverket.

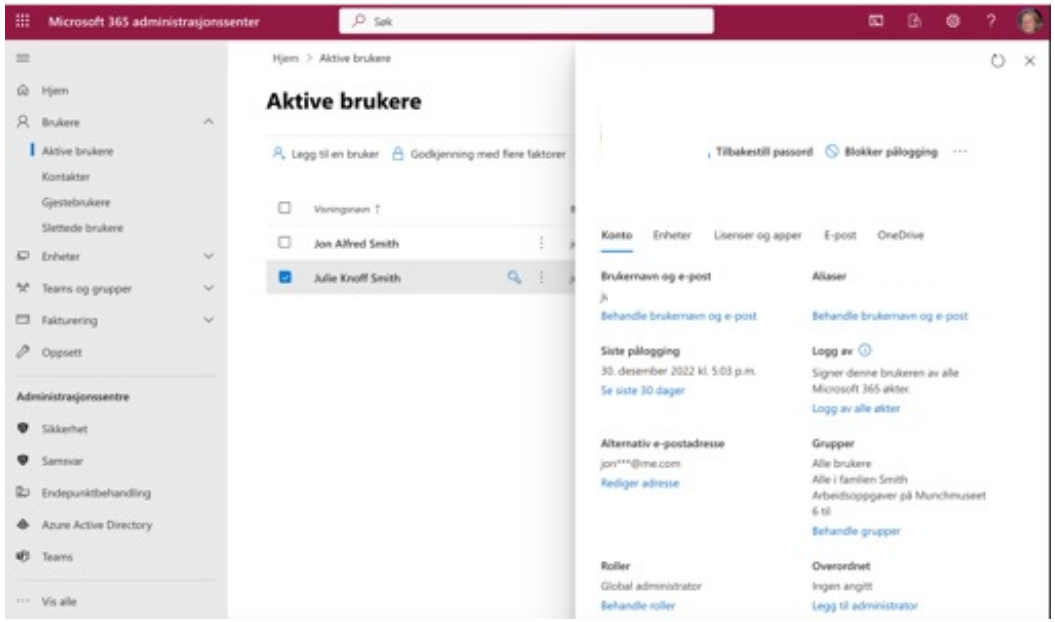
3 typer brukere

I Microsoft 365 finnes det tre typer brukerkontoer. Det kan være rene skybrukere som er opprettet direkte i Azure AD. Brukere kan være synkronisert til skyen fra lokalt Windows AD og er hybride. Det kan dreie seg om gjester med eksterne kontoer – B2B står for Business-to-Business, bedrift-til-bedrift.

Håndtere skytjenester

For organisasjoner uten lokal infrastruktur må du opprette og administrere brukerne i Azure AD. Det gjøres også ofte av virksomheter når de vurderer og utforsker skyen, eller når de har hastverk med å komme i gang med Teams. Administrasjonssentret for Microsoft 365 er oversiktlig organisert. I den grå navigasjonsruten til venstre ser du alternativer for å forvalte brukere, enheter, teams og grupper. Der finner du også menypunkter for fakturering og oppsettet for organisasjonen din. Under er det pekere til portaler for Sikkerhet og Samsvar pluss andre administrasjonssentre.

Antakelig vil du tilbringe mye tid med aktive brukere. Navnet vises øverst på kortet. Du kan tilbakestille passord, blokkere pålogging og slette bruker. Du kan behandle brukernavn og primær e-postadresse. Du får en oversikt over påloggingsaktiviteten for de 30 siste dagene. Du kan angi en alternativ adresse for å tilbakestille passordet om en bruker har glemt det og blir låst ute av kontoen. Du kan tildele roller. Normalt skal sluttbrukere ikke ha administratortilgang. Til det oppretter du egne kontoer med akkurat nok rettigheter (prinsippet om minste privilegium). Du kan ta det enda et skritt videre ved bare å tillate administrativ tilgang fra spesielt herdede maskiner. Men her er det primært et testmiljø.

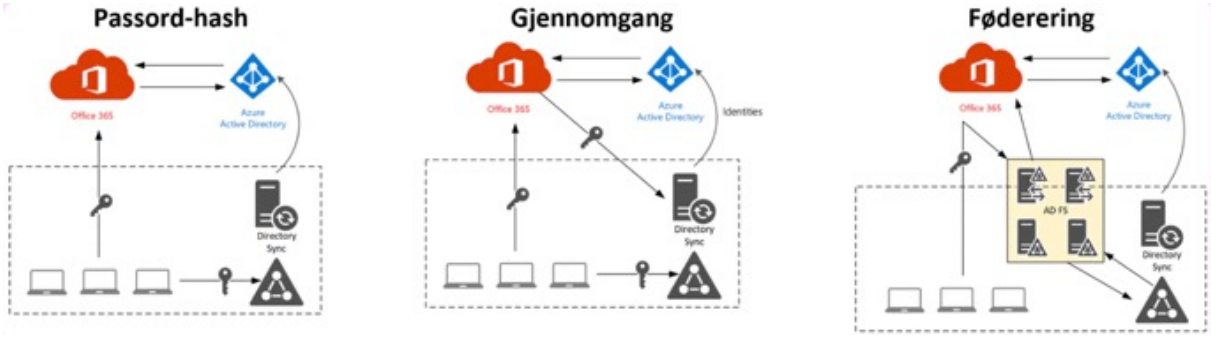


Et alias er en annen adresse andre kan benytte for å sende e-post. Du kan logge av brukere fra alle Microsoft 365-sesjoner. Du kan administrere medlemskap i grupper og legge til en overordnet som bruker rapporterer til. Blar du lengre ned, finner du kontaktinformasjon som kan redigeres. Du kan invitere bruker til å laste ned Microsoft 365 Apps på enhetene hun bruker, eller tilbakekalle dem. Her kan du også aktivere godkjenning med flere faktorer på den gamle måten, som ikke er anbefalt.

Enheter viser hvilke datamaskiner og mobilenheter som er registrert for bruker i Intune. Du får informasjon om samsvarstilstand, modell, operativsystem, siste innsjekking og registret dato. Herfra kan du velge å fjerne firmadata. **Lisenser og apper** gir muligheten til å administrere dem for hver enkelt ansatt (en annen mulighet er på gruppenivå). Under **E-post** finner du de vanligste funksjonene for å håndtere e-post. Du ser hvor mye av postboksen som er brukt. Du kan sette opp tillatelser (Send som og Send på vegne av) og behandle videresending av e-post og automatiske svar. **OneDrive** lar deg forvalte OneDrive for Business per bruker, med innstillinger for lagringsplass og deling.

Synkronisere hybride identiteter

Eksisterende virksomheter har ofte en infrastruktur med Windows AD og trenger å integrere Microsoft 365 sømløst. Brukere bør ha samme brukernavn og passord lokalt og i skyen og logge på bare én gang for å få tilgang til alle ressurser. Det lar seg gjøre på tre forskjellige måter ved å sette opp synkronisering med Azure AD Connect. Du kan konfigurere dette på en lokal server eller i skyen som del av Azure AD-klargjøringstjenesten. Da administrerer du brukere lokalt i Windows AD.



Microsoft anbefaler at man bruker **Synkronisering med passord-hash.** Den lagrer ikke lokale passord i Microsoft 365 som mange tror. Selskapet har overhodet ikke tilgang til dem. Windows AD benytter en hashfunksjon for å oppbevare passord kryptert i et ikke-reversibelt format. Før det sendes til Microsoft 365, blir det lagt til en salt-verdi (et vilkårlig tall) og hashes ytterligere tusen ganger. Ved kontakt med en domenekontroller får brukere sømløs engangspålogging (single sign-on); uten forbindelse kreves en fornyet pålogging med samme legitimasjon (same sign-on). Begge former forkortes med SSO.

Gjennomgangsautentisering og **Synkronisering med føderering** bør bare benyttes om man har helt spesielle behov, som lokal autentisering, bruk av smartkort og tredjeparts MFA.

Invitere eksterne identiteter

I portalen for Microsoft Entra kan du invitere eksterne brukere. De autentiseres av identitetstjenester utenfor din organisasjon, som Google eller Outlook.com. Brukere i andre Microsoft 365-organisasjoner godkjennes der, dessverre uten at de kan ta med seg lisenser. Dette er forskjellig fra invitasjoner fra Teams, SharePoint og OneDrive for Business som foretas i applikasjonene.

Konklusjon og avslutning

Microsoft 365 er langt mer enn en løsning for å driftsutsette IT-miljøet. Det er et eget økosystem med innebygde opplevelser som fungerer på tvers av plattformer. Det integrerer mennesker, enheter, apper og data. Produktivitetsskyen er en organisme som lever og ånder, med teknologier som er inkluderende og trivselsfremmende. Vi har mindre fokus på applikasjoner enn på oppgavene vi skal utføre. Og skyen er alltid på. Geografisk distribuerte datasentre med speilede tjenester sørger for høy tilgjengelighet. Sikkerhet er ikke noe som er lagt til i ettertid, men er bygget inn fra starten av.

Med Business Premium får du et godt balansert produkt som møter utfordringene en typisk SMB-kunde sliter med: Hvordan kan vi forbedre eksternt arbeid med ansatte som jobber fra flere lokasjoner? Hva kan vi gjøre for å opprettholde et trygt miljø med mange personlige og mobile enheter? Hvilke tiltak kan vi iverksette for å få ned kostnadene med en økning i phishingangrep og løsepengevirus? Business Basic og Standard, som henvender seg til samme SMB-segment, gir ikke nok sikkerhet. Med dagens trusselbilde bør du velge Business Premium. Men det kan også være alt du trenger.

Forsiktige anslag går ut på at rundt 50 prosent av alle SMB-bedrifter er blitt utsatt for nettangrep i de senere år. Det gjør at de fleste SMB-kunder ser på IT-sikkerhet som topprioritet i sin organisasjon. Samtidig klarer mange ikke å håndtere den på egenhånd og føler seg overveldet. Business Premium er del av svaret. Den andre biten er å velge riktig samarbeidspartner som kan bidra med å sette opp og

Sikkerhetskopiering og gjenoppretting

Business Premium har flere mekanismer for å beskytte og berge data, men mangler en dedikert backup-løsning. Det er hendig med papirkurvene i SharePoint og OneDrive, versjonslogger og -historikk og funksjonene Gjenopprett SharePoint og OneDrive. I Outlook (Exchange) har vi mappene Slettede og Gjenopprettbare elementer. Brukere kan på den måten hente frem data og sparer IT for mye arbeid. Men det beskytter ikke mot menneskedrevne løsepengevirus- og utpressingsangrep. Angriperne vil sørge for å ødelegge alle kopier. Det du må ha, er uforanderlige backuper som trusselaktørene ikke har tilgang til. Det får du med det produktet vi anbefaler: Cloud Backup.

Tilleggslisenser

Enkelte ganger trenger du mer enn hva som følger med Microsoft 365 Business Premium. Da kan du bruke produktet som en grunnpakke du utvider med tilleggslisenser, og det blir fortsatt mye rimeligere enn et fullt Microsoft E5-abonnement. Du kan ha behov for utvidet identitetsbeskyttelse i **Azure AD Premium P2**, som oppdager og fjerner bruker- og sesjonsrisikoer i skyen. I hybride miljøer er det helt uunnværlig med **Defender for Identity**, som avdekker kompromitterte kontoer og stadiene i en angrepskjede. Det kan være nødvendig med automatisert oppdagelse og merking av data på tvers av hele ditt digitale miljø, lokalt og i skyen, noe som krever **E5 Information Protection and Governance**.

De grafiske figurene er selvlaget i Visio og fra Microsoft. Teknisk inneholder Microsoft 365 Business Premium blant annet disse lisensene: Azure AD Premium P1, Azure Information Protection (AIP) P1, Exchange Online P1 med e-postarkivering og Defender for Office 365 P1. Defender for Business er en spesialtilpasset versjon av Defender for Endpoint P2.Du kan lese mer om disse teknologiene på Aktuelt og fagblogg: https://www.evelon.no/artikler.

Om Evelon

Evelon er IT-folka som bryr seg – ærlige, kunnskapsrike og innovative. Ved å etterleve våre verdier ønsker vi at du som kunde raskt skal føle deg som en del av Evelon. Med kompromissløs dedikasjon både til kvalitet i alt vi leverer, og til fornøyde kunder beviser vi hvorfor vi er det beste valget for deg. Vi er store nok til å kunne betjene større bedrifter, små nok til å sørge for personlig oppfølging.

Kundetilfredshet

Kundetilfredshet er og har alltid vært en strategisk prioritering for selskapet, og de ansatte gir det lille ekstra for å gjøre kundene fornøyd. Vi legger vekt på en god tilbakemeldingskultur – feirer de grønne, bryr oss om de gule og tar tak i de røde meldingene.

Sertifiseringer

Våre rådgivere har til sammen over 120 sertifiseringer, primært innenfor Microsoft, VMware, ISO/IEC 27001, Veeam, ITIL, Cisco, Fortinet, Sophos og TOGAF. Med så stort utvalg spesialister er det enkelt for oss å finne riktige personer til hvert enkelt prosjekt.

Leverandørstatuser

Vi er minimum gullpartner hos våre viktigste leverandører. Dette bør gi våre kunder en trygghet om at vi besitter riktig kompetanse, at vi har god relasjon og dialog med leverandøren, samt at vi kan vise til mange fornøyde kunder innenfor hvert område.

Oslo
Brynsalleen 4
0667 Oslo
21 41 50 00

Tønsberg
Åshaugveien 68
3170 Sem
91 34 63 66

Brevik
Strømtangvegen 11 A
3950 Brevik
35 03 20 00

Lillehammer
Bryggerigata 1
2609 Lillehammer
21 41 50 00

salg@evelon.no

Nyttige lenker

Microsoft 365 Business Premium

Følsomhetsetiketter i Microsoft 365 Business Premium

Microsoft 365 Business Premium - En innføring

Sikkerhetsmodellen i Microsoft Business Premium

Sikre og behandle enheter i Microsoft 365 Business Premium

Brukeradministrasjon i Microsoft 365 Business Premium

Trusselbeskyttelse i Microsoft 365 Business Premium

Databeskyttelse og samsvar i Microsoft 365 Business Premium