

Bruk av sky i offentlig sektor

Contents

Introduksjon	3
Målbilde	4
Hva er sky?	5
Hva er et datasenter	5
Fra datasenter til skytjenester	5
Hva er hybrid?	5
Fysisk og logisk sikring av datasentre	5
Ansvarsmodellen for offentlig sky	5
Azure i Norge	6
Sky og bærekraft	6
Hvordan gjennomføre et skyprosjekt?	7
Strategi og forankring	7
Organisasjon	7
Mal for skydrevet organisasjon	7
Planlegging	7
Klargjøring (Ready)	9
Migrering (Migrate)	9
Innovasjon (Innovate)	9
Sikkerhet (Secure)	9
Forvaltning (Manage)	9
Styresett og kontroll (Govern)	9
Antimønstre for skyadopsjon	10
Risikovurdering for bruk av sky	12
Nyttige definisjoner og terminologi	13
Landingssoner	13
Tilgjengelighet (SLA)	13
Referansearkitektur og hybrid	14
Identitetsløsning for kommunal sektor	14
Feide-innlogging	15
Principle of Least Privilege	15
Skill tilgangsnivå på brukerkontoer	15
Klassifiseringmatrise for applikasjoner	16
Plan for tjenesteporteføljen	16
On-premises	16
Nettverk	16
Sikring av nettverk	17
Sikkerhet i skyen	17
Verktøy	19
Conditional Access	21
Nettverk	22
Private endepunkter	22
Fysisk sikring av datasenter	23
Tekniske komponenter for sikring og compliance	23
Azure Datasenter sikring	23
Kryptering i Azure	23

Azure HSM	23
Konfidensiell Databehandling	23
Customer Lockbox	23
Azure Policy	23
Azure ARC	23
Azure Dedicated Hosts	23
Utvalgte sikkerhetselementer	24
Krisesituasjoner	24
Særskilte norske lover, krav og anbefalinger(som man bør ta stilling til)	24
NSM - Råd og anbefalinger for IKT sikkerhet	24
Eksempel: NSM grunnprinsipper for IKT-sikkerhet 2.0 policy initiative	24
CSA Cloud Controls Matrix (CCM)	26
Automatisering og xOps	27
xOps	27
Infrastruktur som kode / Infrastructure as code (IaC)	27
Valg av verktøy	28
Prinsipper for bruk av infrastruktur som kode	28
Konfigurasjonshåndtering	28
Implementasjon	29
Tilpasning for kommunal sektor	29
Forhåndskrav:	30
Azure landingssone aksellerator	30
Etablering av hybrid oppsett	40
Compliance - Policy initiative for NSM sine grunnprinsipper	40
Vedlegg og støttedokumentasjon	41
Azure i Norge	41
Rapporter, audit, innsyn	41
Schrems-II	41
GDPR	41
Linker	41
Verktøy	41
Dokumentversjon og endringslogg	42

Introduksjon

I en verden som stadig blir mer digitalisert er lagring og prosessering av data i offentlig sky et mer agilt, tidsbesparende, sikkert, miljøvennlig og kostnadseffektivt enn andre alternativer.

Det er et klart behov for offentlig sektor å digitalisere seg raskere. Utfordringer, bekymringer, tvetydighet og mangel på kunnskap rundt lovgivning og tekniske løsninger har ført til at digitalisering i offentlig sektor gått noe saktere enn andre sektorer. Samtidig ser vi at aktører som “knekker koden” på digitalisering kan ta ledende posisjoner, og Norge er et land som kan skryte av sterke fagmiljøer og innovative løsninger som plasserer oss som en av de ledende nasjonene innenfor digitalisering, digital innovasjon og digital transformasjon. Den desentraliserte organiseringen vi har i Norge legger til rette for innovasjon, men kan samtidig skape noen utfordringer for aktørene med mindre ressurser og kompetanse.

Bruk av offentlig sky krever en interdisiplinær tilnærming over både det juridiske og det tekniske domenet. Juridiske tiltak kan ikke løse alle tekniske utfordringer, og tekniske tiltak kan ikke løse alle juridiske utfordringer - men vår påstand er at man kan nå en tilstrekkelig grad av risikoreduksjon gjennom forståelse og avveininger på tvers av domeneene.

Derfor ønsker vi å legge til rette for et åpent samarbeide i å utvikle malverk som skal fasilitere for bruk av skytjenester i offentlig sektor. Vi gjør dette i en “open-source ånd”, og inviterer alle interesserte parter i å bidra. Microsoft og noen utvalgte partnere og domeneeksperter har tatt på seg å lede an i dette arbeidet, men vi er til slutt avhengig av en åpen og konstruktiv debatt og bidrag fra langt flere enn kjerneteamet for å kunne lage løsninger som vil bli allment akseptert.

I første omgang har vi definert skopet til dette prosjektet som kommunal sektor i Norge. Målgruppen for dette dokumentet er både beslutningstagere og operasjonelle IKT-ressurser som skal legge til rette for og gjennomføre prosjekter i sky.

Målet for dette prosjektet er å kunne gi en solid forståelse av hva skyteknologi er, og hvordan man benytter konkrete tjenester, produkter, og teknologier for å sikre en stabil og sikker drift av applikasjoner i skyen.

Helt konkret er målet å levere både referansearkitekturer og verktøy for raskt å kunne bygge såkalte “landingssoner” for ulike risiko og/eller klassifiseringsdomener for bruk av IaaS og PaaS tjenester.¹

Det er viktig å påpeke at hver organisasjon må gjøre sin egen risikovurdering og er selv ansvarlig for juridiske betraktninger og ibruktakelse.

Dette prosjektet kan også ha verdi for andre aktører i både offentlig og privat næringsliv, og vi har som mål å kunne utvide skopet til andre aktører etter hvert som prosjektet modnes.

¹Vi tar ikke med SaaS-tjenester i dette prosjektet, da ansvarsforholdet er annerledes og dermed er det behov for en noe annerledes diskusjon, samt at det allerede er ganske god forståelse av hva dette betyr og hvordan det må håndteres i markedet.

Målbilde

Vi ønsker å tegne et målbilde for hva skyteknologi kan hjelpe kommunal sektor med.

Nedenfor finner du en liste over felles utfordringer vi hører for offentlig sektor - og senere i dokumentet betraktninger på hvordan sky kan hjelpe å kontre noen av disse utfordringene.

- Teknisk gjeld
- Mangel på ressurser (Personell)
- Mangel på kompetanse
- IT Support
- Utdaterte systemer (Og da usikre eller lite fleksible systemer)
- Sikkerhet & Forensic
- Mangel på alternativer
- Tradisjonell sonemodell/IT infrastruktur vs moderne sky-miljø
- Mangel på standardisering (duplikater av fellestjenester, mangel på tjenestekataloger++)
- Lite deling av tjenester (og vanskelig deling på tvers)
- GDPR & Data Governance
- Kommunesammenslåing / Kommunesplitting
- Kost
- Tilknytting til Helsenett (Tannlege/Kommunal helsetjenester mm)

Vi tror at ved å standardisere, dokumentere og bygge en helhetlig arkitektur vil kommunal sektor kunne dra stor nytte av hverandre og kompetansen ute i markedet - samt bidra til å dele og forenkle applikasjon og forvaltningbildet der ute.

Bidra gjerne med innspill til applikasjoner, konkretisering av problemstillinger mm. som kan tas inn i arkitektur og diskuteres.

Hva er sky?

Hva er et datasenter

I informasjonsteknologiens spede barndom var det en gjengs oppfattning at verden kun ville trenge et begrenset antall datamaskiner. Vi kan kalle dette “stormaskinens tidsalder”, og de fleste som benyttet en datamaskin jobbet gjennom en terminal som gav tilgang til data og regnekraft som befant seg i en sentral datamaskin. Disse stormaskinene befant seg typisk i datarommet til en organisasjon eller bedrift - en fysisk sikret lokasjon hvor kun autorisert personell hadde tilgang.

Etterhvert som avhengigheten til datasystemer økte, ble det satt større og større krav til fysisk sikring og redundans for slike datarom, og det ble etterhvert både vanskelig, upraktisk og ulønnsomt å etterleve disse kravene for hver enkelt organisasjon og bedrift. Samtidig fikk vi ny og raskere nettverksteknologi som gjorde det mulig å flytte både stormaskiner, servere og data lengre unna brukerne. Dette la grunnlaget for en ny industri: datasenterindustrien.

Idag er datasenterindustrien en sentral komponent i vår digitale infrastruktur. Dedikerte datasenterleverandører leverer redundante tilkoblinger til nettverk- og elektrisitetsnett, nød-aggregater som holder datasenteret igang selv gjennom lange perioder med strømbrydd, og strenge tiltak for fysisk sikring for å hindre uautorisert tilgang.

I dag vil de aller fleste organisasjoner velge å benytte en profesjonell datasenterleverandør fremfor å bygge sitt eget datarom.

Fra datasenter til skytjenester

Hva er så sky, og hvordan skiller skyleverandører seg fra datasenterleverandører?

Idag bærer stort sett alle rundt på både mere regnekraft og lagringsplass enn vi trenger. (Faktisk har en moderne smarttelefon mer regnekraft enn hele land hadde tilgang til for bare tiår siden. TODO: Kilde) På samme måte har de fleste datarom mer regnekraft og lagringsplass enn organisasjonen som eier det trenger. Vi overdimensjonerer systemene våre for å kunne ta unna for perioder med intens bruk - tenk 8-timers arbeidsdag for de fleste organisasjoner og bedrifter, black-friday og julehandel for varehandelen, og frist for innlevering av skattemeldingen for alle norske borgere. Dette fører til at vi har mange enklitsiloer av overdimensjonerte systemer - dette er både dyrt og har store miljøimplikasjoner. Datasenterindustrien er i ferd med å bli en av verdens mest energikrevende bransjer. (TODO: Kilde)

Med skyteknologi så endres måten man kan kjøpe regnekraft og lagringsplass seg dramatisk. Organisasjoner kan nå kjøpe bare det de har behov for, når de har behov for det. En bedrift i varehandelen kan skalere opp før black-friday, og ned igjen etterpå. De kan til og med designe systemet sitt slik at det autoskalerer med bruk. Finn.no har for eksempel XX% av besøkene sine innenfor lunsj-perioden på hverdagene (TODO: Kilde). Resten av tiden trenger de bare en brøkdel av regnekraften - som så kan frigis av skyleverandøren og selges til andre kunder, for eksempel forskningsorganisasjoner som kjører store jobber som ikke er tidskritiske - og derfor kan kjøpe kapasitet rimeligere, siden deres jobber kan aktivieres når det er mindre behov i markedet. Store skyleverandører vil også flytte om på workloads for kunder, slik at servere, racks, eller til og med hele datasentre kan skrus av for å spare energi i perioder med lav etterspørsel.

En annen forskjell på en datasenterleverandør og en skyleverandør er tjenestespekteret. Mens en datasenterleverandør er som en avansert utleier av fysisk plass, er en skyleverandør også en programvare- og driftsleverandør av hundrevis av avanserte tjenester som gjør det mulig å bygge digitale systemer raskere og bedre.

Hva er hybrid?

...

Fysisk og logisk sikring av datasentre

slik som perimetersikring kombinert med videoovervåking og døgkcontinuerlig bemanning.

Ansvarsmodellen for offentlig sky

Før vi diskuterer felles utfordringer, løsninger og arkitektur er det viktig å forstå hvordan ansvarsmodellen ser ut i sky og hvordan valg av ulike tjenester/komponenter spiller inn på ansvarsområde man har og hva man må sikre.

De fleste kunder som har sky tjenester idag har en god kombinasjon av IaaS/PaaS og SaaS tjenester.

Dette kan forenkle driftsmodellen betraktelig slik overnevnte modell viser - i motsetning til at man kjører alt i eget datasenter (on-prem) hvor man er ansvarlig ansvarlig for alt fra fysisk sikring av bygninger, infrastruktur og hele veien oppover i ‘stacken’.

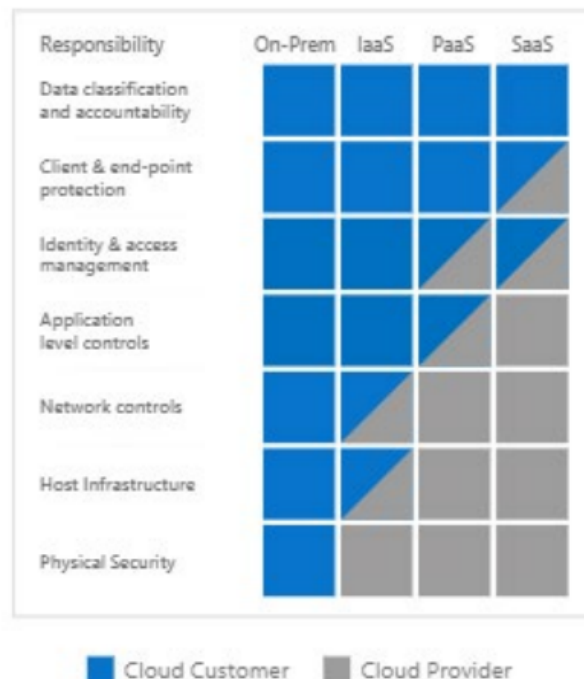
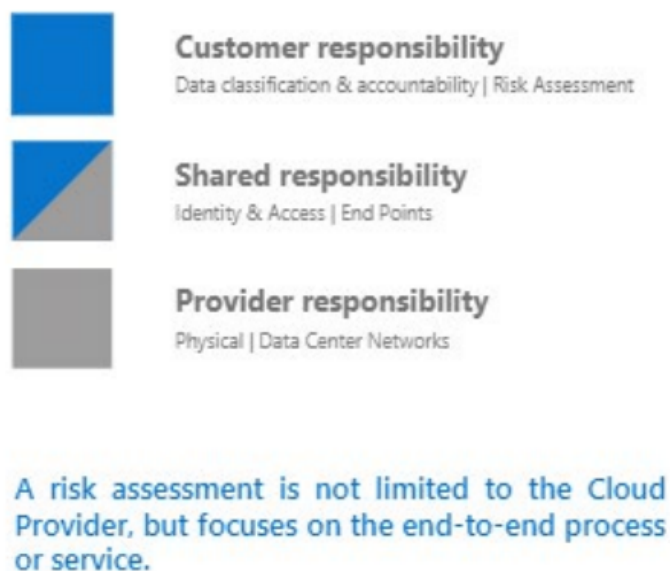


Figure 1: Ansvarsmodell

Azure i Norge

Azure tjenester leveres i Norge fra “Norway East” og “Norway West” regionene. Norway East har 3 soner; datasenter med separat strøm, kjøling og nettverk. Norway West er en sk satellitt-regione som brukes før disaster recovery. Alle Azure regioner bygges med strikte krav på fysisk sikkerhet, tilgang og redundans.

Sky og bærekraft

Hvordan gjennomføre et skyprosjekt?

Skyadopsjon kan fort gå feil dersom man ikke har god forankring, gjør god planlegging og forventningsstyring samt legger ned et godt stykke arbeid i organisasjonstransformasjon.

Microsoft Cloud Adoption framework inneholder ca 1500 sider med god dokumentasjon på hvordan man skal gå frem for å tilvenne seg sky.

Vi prøver å forenkle noen av de viktigste prinsippene for å starte skyadopsjon her.

Strategi og forankring

En god forankring for skyadopsjon begynner med en skystrategi som er forankret både hos toppledelsen og ansatte. Dersom man ikke har etablert en god skystrategi, så risikerer man at prosjektet mislykkes tidlig og blir blokkert eller nedprioritert.

En god skystrategi bør som et minimum inneholde følgende 4 punkter:

- Motivasjon for sky [Hvorfor skal vi til sky?]
- Forventninger og resultater [Hva kan vi forvente? Hva ønsker vi å oppnå]
- Finansielle betraktninger [Hva vil det koste, hva vil vi tjene, hva vil vi spare?]
- Tekniske vurderinger [Er det mulig? Hvordan kan det utføres teknisk? Hva må til?]

Det finnes en rekke fordeler med sky - men det er viktig å være forent og ha et felles mål på hvorfor man skal til sky og forventingsstyre alle ledd i organisasjonen.

Utvikling av skystrategi ligger beskrevet i mer detalj [her](#) (Engelsk)

Organisasjon

Det er viktig at ikke punktet rundt organisering og organisasjon tas for gitt.. Skytransformasjon er noe nytt, setter nye premisser og krever nye funksjoner og roller innad i en organisasjon.

En velykket skyadopsjon bør etablere et minimum sett av nye teams for å understøtte en rekke funksjoner som er påkrevd for sky.

Disse teamene kan gjerne være virtuelle i starten - men bør utvikles og inngå mer formelt jo mer organisasjonen modnes. De som jobber i slike team må dediseres til å jobbe utelukkende med sky og ikke sitte med flere gamle roller. Erfaring tilsier at driftsoppgaver blir prioritert og fjerner fokus ifra sky.

Mal for skydrevet organisasjon

Som et minimum - bør det etableres arbeidsgrupper for å definere strategi, styring og kontroll (styresett) og et eller flere arbeidsgrupper for adopsjon.

I bildet over ser du eksempler på roller og funksjoner som kan inngå i disse teamene.

Etterhvert som organisasjonen modner seg så vil man konvergere mot en veletablert skyorganisasjon og flere kryssfunksjonelle teams med ulike skyroller bør inngå i et [CCoE](#) (Cloud Center of Excellence). Dette referes ofte til på norsk som et Kompetansesenter sky, og må etableres i organisasjonen så tidlig som mulig, med korrekt forankring. En skyevangelist bør lede et Kompetansesenter sky, og motivere organisasjonen for skyreisen.

Etterhver som skytjenester ibruktages må skyen også driftes. Dette utføres ikke av Kompetansesenter Sky, men av et Driftsenter Sky. I oppstartfasen vil disse to teamene jobbe tett sammen, kanskje som ett team til og med, og etterhvert vil roller og ressurser fordeles mellom disse.

For mer informasjon om hvordan man kan organisere seg og ulike typer funksjoner i en skyorganisasjon - se [her](#).

NB: Organisasjoner befinner seg på ulike stadier i en modenhetsprosess. Ofte vil mangel på styring og kontroll blokkere adopsjon. Vet du hvor dere er i forhold til organisasjon, modenhet og strategi? Har dere dugnadshelter som lager styresett? Har dere automatisert styresett og utrulling av funksjonalitet?

På [denne](#) siden ligger en rekke spørreskjemaer du kan benytte for å finne ut hvor dere ligger an i forhold til skyadopsjon.

Planlegging

En god planlegging bør omfatte minimum

- Hva har vi av IT-systemer og tjenester som skal supporteres, hvordan ser landskapet ut, hva skal til sky, hva bør vi erstatte, hva kan skrives om mm.
- Hvem inngår i ulike arbeidsgrupper for å jobbe med sky og hvordan setter vi det sammen

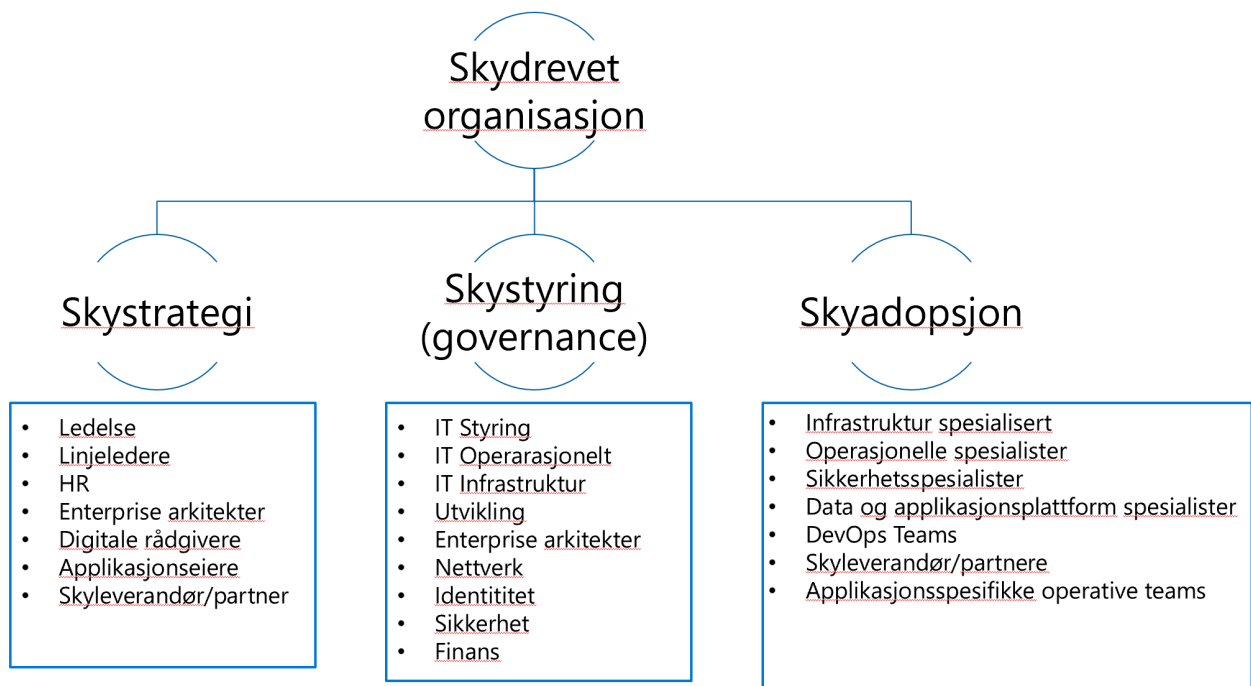


Figure 2: Organization MVP

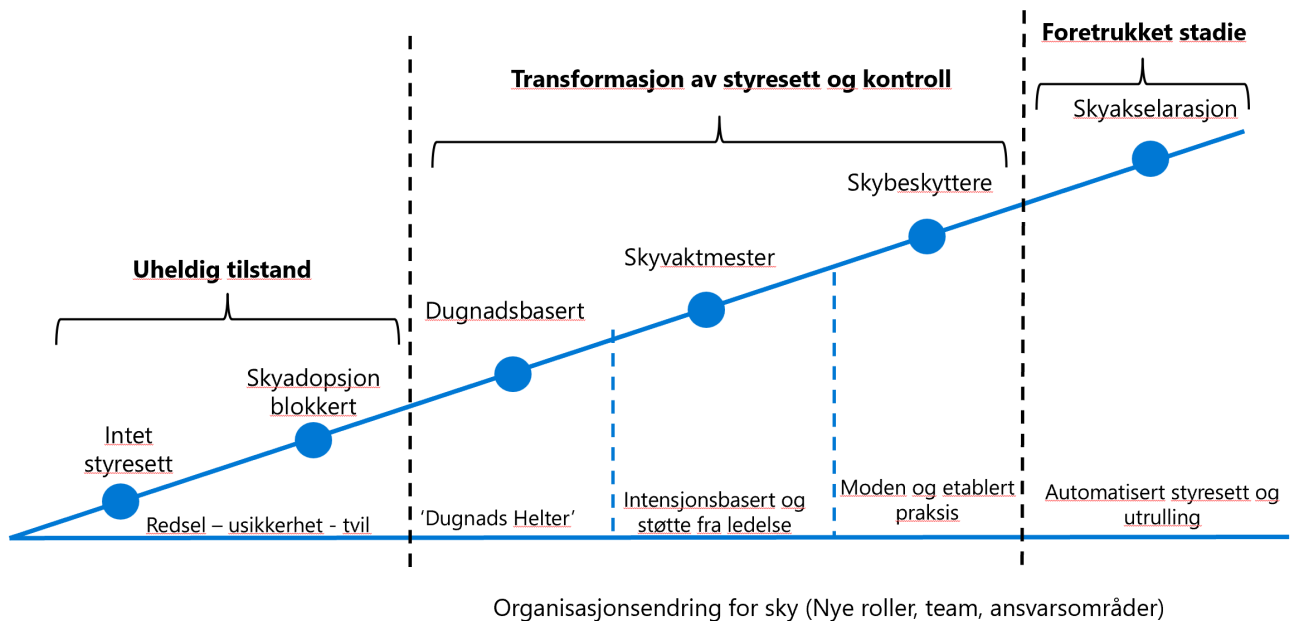


Figure 3: Modenhet

- Kompetanseplan og kompetansebehov.
- Adopsjonsplan med tidsplanlegging og prosjektstyring.

Velg et prosjektverktøy som kan benyttes for å følge utviklingen av skyprosjektet og for å tilordne oppgaver og ansvar.

[Her](#) ligger en rekke utfyllende dokumentasjon og erfaringer rundt å legge gode planer.

Klargjøring (Ready)

Før man kan begynne implementering og adopsjon, så designer man landingssoner som kan benyttes for de ulike applikasjonene man skal tilby på sin plattform.

Klargjøringsfasen kan deles inn i 4 faser:

- Operativ modell - finn den rette modellen man ønsker å ha på operasjonell modell i sky
- Design områder - En rekke områder man bør tenke igjennom og designe for. Viktig å skjønne og tegne hvordan man ser for seg avtaleforhold, AAD tenants, brukerhåndtering mm. for sin kommune (eller flere kommuner).
- Azure landingssoner - forstå ulike landingssoner og valg for å aksellere utrulling av landingssoner og applikasjoner.
- Reisen til en referansearkitektur - valider hvor du er i forhold til implementering og hvilke valg du har for å flytte/migrere eller modernisere applikasjoner mot skyreisen.

Migrering (Migrate)

Inneholder en rekke god dokumentasjon på hvordan du kan migrere eksisterende applikasjoner til sky, ulike scenarioer på flytting til sky og best practices når det gjelder flytting/migrering.

Husk: Migrering er ikke kun en teknisk jobb - husk at organisasjon, brukere og ansatte også vil påvirkes av skyreisen og kreve endringspraksis.

Innovasjon (Innovate)

Hvordan kan sky hjelpe bedriften å innovere? Disse sidene under 'CAF' omhandler nettopp hvordan du kan begynne å ta i bruk sky for innovasjon, lage prototyper og teste ut mot 'publikum' og måle effekt.

[Innovasjon starter med å løse et problem og definere 'business' verdi. Hva kan vi hjelpe innbyggere med? Hva oppnår vi med å løse følgende problem? Får vi nye muligheter? Hvilken motivasjon kan vi ha for å løse problemet?](#)

Husk: Sky åpner for en rekke nye muligheter som tidligere var meget kostbart eller ikke mulig og man kan raskt komme i gang med å lage publikumstjenester, tilgjengeliggjøre data til innbyggere, eller samle inn data.

[Les mer om Digital Inventions her](#)

Sikkerhet (Secure)

Sikkerhet i en hver organisasjon må være en hovedprioritet. Dette inkluderer også forankring av forretning/organisasjon og må ikke kun sees på som en 'teknisk' jobb.

[Sikkerhet i CAF omtales i meget god detalj her](#)

Forvaltning (Manage)

Styresett og kontroll (Govern)

Antimønstre for skyadopsjon

Det er identifisert en rekke ‘antimønstre’ (Anti-patterns) som man bør ta en ekstra titt på for å sikre at man går til sky på riktig grunnlag.

Fase	Antimønster	Referanse
Strategi	Manglende skystrategi	[legg til referanse]
Strategi	Manglende forankring	[legg til referanse]
Strategi	Utilstrekkelig motivasjon	Adopt the cloud without establishing goals
Strategi	Feil motivasjon	Fail to communicate motivations
Planlegging	Feil skydriftsmodell	Choose the wrong cloud operating model
Planlegging	Feil tjenestemodell	Choose the wrong service model
Planlegging	Erstatte fremfor å modernisere	Replace architecture
Klargjøring	Benytte forhåndsvisningstjenester i produksjon	Assume released services are ready for production
Klargjøring	Upresise antakelser rundt robusthet og høytilgjengelighet	Assume increased resiliency and availability
Klargjøring	IT som en skyleverandør	Become a cloud provider
Adopsjon	Utilstrekkelig sikring	Migrate, modernize, or innovate without guardrails
Adopsjon	Utilstrekkelig kartlegging	Migrate, modernize, or innovate without an assessment
Adopsjon	Påtvunget arkitektur	Dictate an architecture
Adopsjon	Ett abonnement	Use a single subscription
Administrasjon	Neglisjere gevinst for bedriften	Focus on tooling, not business outcomes
Styresett	Feiljusterte forventinger rundt delte ansvarsområder	Misunderstand shared responsibilities
Styresett	Upresise ut-av-boksen antakelser rundt sikkerhet	Assume out-of-the-box solutions provide security
Styresett	Egendefinerte rammeverk for samsvar og styresett	Use a custom compliance or governance framework
Organisering	IT som kostsenter	Treat IT as a cost center
Organisering	Utvikling av plattform uten godkjenning fra forretningen	Antipattern: Invest in new technology without involving the business

Fase	Antimønster	Referanse
Organisering	Tjenesteutsette kjerneområder i forretningen	Antipattern: Outsource core business functions
Organisering	Tekniske beslutningstakere fremfor skyarkitekter	Antipattern: Hire technical decision makers instead of developing cloud engineers

Har man utilstrekkelig med forankring i organisasjonen eller syntes det er vanskelig å jobbe med adopsjon - så kan både skyleverandør og partnere hjelpe deg med å kjøre ulike workshops.

På Azure Marketplace og find CAF partner kan du finne liste over partnere som tilbyr workshops.

Er du usikker på om du har en adopsjonsplan? Undersøk om din organisasjon har en adopsjonsplan og se hvordan det påvirker deg.

Er du usikker på hvilke partnere som tilbyr workshops i skyadopsjon så sjekk [Azure Marketplace her](#).

Risikovurdering for bruk av sky

- Menneskelig feil
- Mangel på kompetanse
- Brudd på fiberkabler (Datasenter eller hel region)
- Strømbrydd (Datasenter)
- Tjeneste(r) går ned (oppgradering, patching)
- Leverandør går konkurs
- Ikke tilgjengelig kapasitet
- Internett går ned
- Myndigheter ber om innsyn
- Hacker(e) får tilgang (Storage, compute)
- Korrupt ansatt (internt)
- Korrupt ansatt (vendor/tredjepart)
- Korrupt ansatt (tjenesteleverandør (datasenter eller skyleverandør))
- Myndigheter klarer å få digital tilgang til datasentere
- Fysisk tilgang til utstyr
- Schrems-II
- GDPR
- FISA 702

Mitigering av risiko

Nyttige definisjoner og terminologi

Landingssoner

Landingssoner i Azure består av abonnement (Subscriptions) konfigurert på en skalerbar måte og som samtidig ivaretar sikkerhet og tilhørende tjenester som nettverk og identitet.

Landingssoner muliggjør migrering, modernisering og innovasjon i stor-skala i Azure - samtidig som man kan rapportere på compliance (eller etablerte styringsregler man har satt for sin organisasjon).

Landingssonene som etableres tar høyde for alle plattformressurser som er nødvendig for å understøtte en bedrifts applikasjons-portefølje og differensierer ikke mellom infrastruktur som tjeneste (IaaS) og plattform som en tjeneste (PaaS).

Generelt kan vi se på oppbyggingen av en landingssone slik:

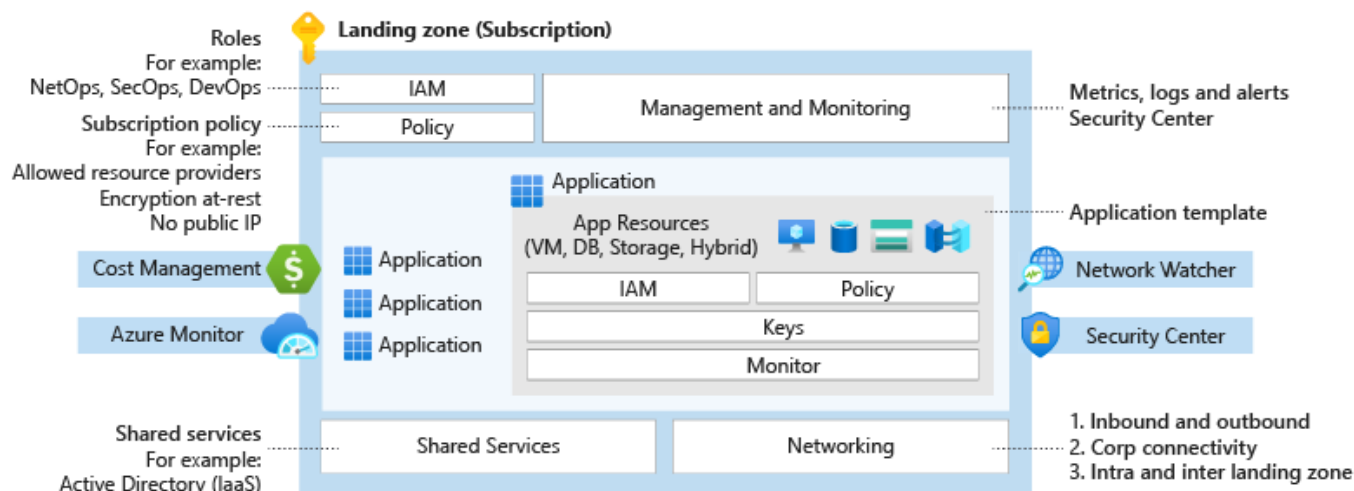


Figure 4: Landingssone

En målarkitektur for offentlig sektor må ta høyde for både on-prem (/edge) og allmenn sky samt styringsett som understøtter dette holistisk.

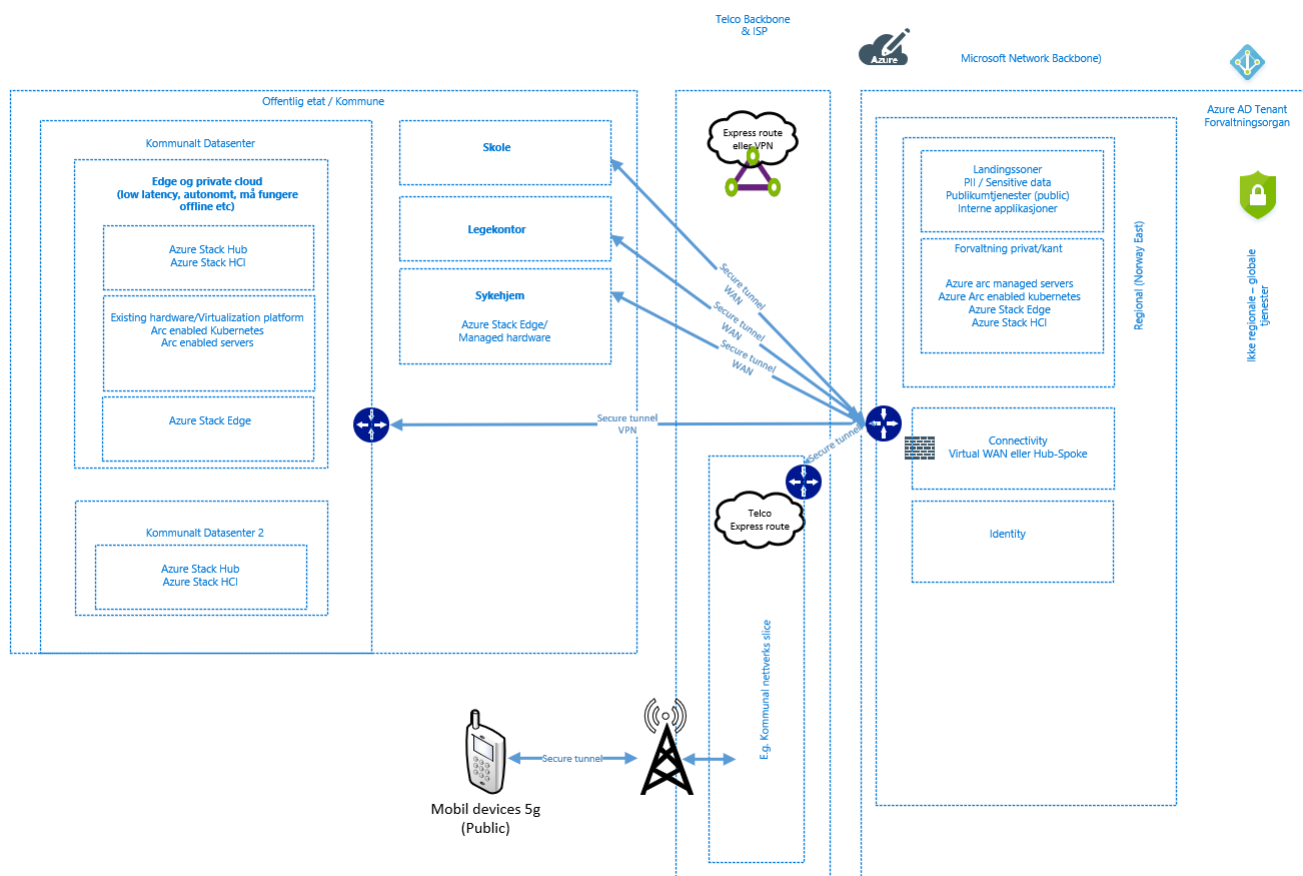
Tilgjengelighet (SLA)

- Høy tilgjengelighet (E.g - Konsumenttjeneste) 99.99 eller 99.95% oppetid. Noe nedetid (minutter) per år akseptabelt. Redundante server(e) og lagringskopier - men ikke på tvers av datasentere.
- Meget høy tilgjengelighet (e.g. pasientsystem) 99.99% eller høyere. Redundante servere og kopier av data på tvers av datasentere (med mer enn 10 km avstand).
- Unntakssituasjon (Disaster scenario) En hel region går ned og blir utilgjengelig.
- Fullstendig suverenitet/autonomitet (autonomy/soveriginity) Skyleverandør går konkurs, Norge mister all kommunikasjon med omverden, systemer som må fungere uavhengig av skyleverandør.

Referansearkitektur og hybrid

Rent overordnet kan man se på en helhetlig arkitektur hvor vi skiller på hva som lovmessig må ligge i egne datasentre/edge (lovmessig reguleringer og krav eller samfunnskritikalitet) og hvordan vi klassifiserer ulike applikasjoner som plasseres i sky, edge eller on-premises.

En Hybrid arkitektur bør understøtte applikasjoner som deployes ‘hvorsomhelst’ - fra helt på kanten (edge - eksempelvis på et sykehus eller på en kiosk/terminal til egne datasentre og helt opp til offentlig sky). Applikasjonkrav- (lover, latens og kritikalitet) og modenhet (utviklet med moderne teknologi) bør avgjøre hvor applikasjoner deployes. For å få til dette kreves ett hybrid skyoppsett - hvor onprem og skyen er koblet sammen.



*** Overordnet bilde ***

Identitetsløsning for kommunal sektor

Azure Active Directory (Azure AD) benyttes som identitetsløsning:

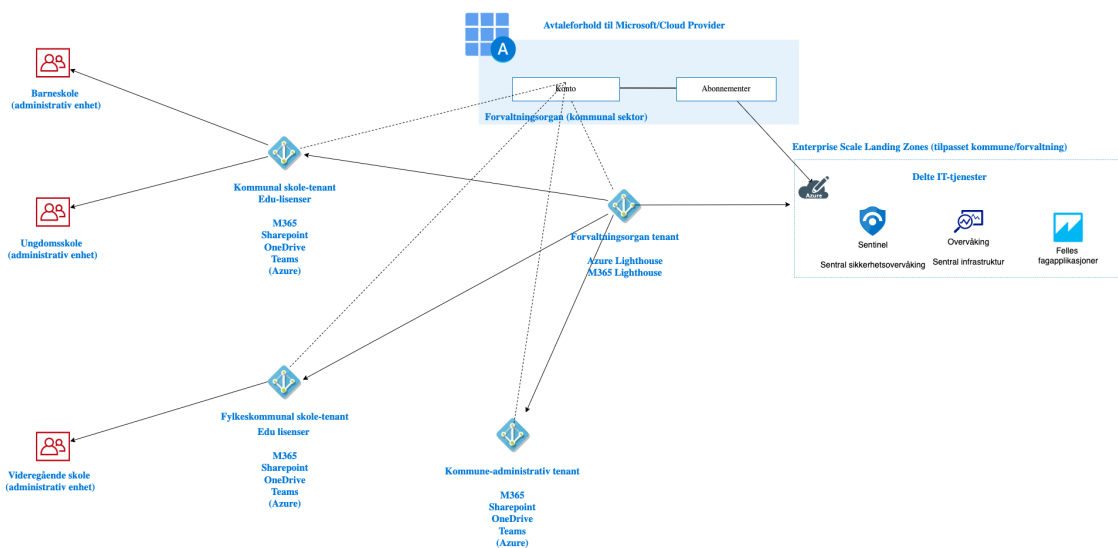


Figure 5: Referanse arkitektur kommunal sektor

Denne arkitekturen er tiltenkt et scenario hvor et felles forvaltningsorgan drifter og tilrettelegger sky-løsninger og IT-infrastruktur for flere kommuner og en fylkeskommune.

Det er etablert et sett med leietakere (tenants) i denne referanse-arkitekturen:

- Forvaltningsorgan
 - Benyttes primært for sentral administrasjon av andre tenants via delegerte tilganger og Azure Lighthouse
- Kommunal skole
 - Rabattert lisensiering for Microsoft 365-tjenester (Edu-lisenser)
 - [Administrative enheter](#) Azure AD benyttes for delegert administrasjon per skole
- Kommunal administrasjon
 - Synkronisert mot lokale katalogtjenester via [Azure AD Cloud Sync](#)
- Fylkeskommunal skole
 - Rabattert lisensiering for Microsoft 365 tjenester (Edu-lisenser)

Skole og administrasjon er adskilt grunnet behov for et galvanisk skille mellom disse miljøene. Administrativ tenant vil også inneholde brukere, grupper og andre typer objekter som brukes for tilgang til sensitive tjenester innen helse med mer - og har strengere behov for drift, forvaltning og sikkerhet enn utdannings-miljøer som omfattes av andre regelverk.

Kommunal- og fylkeskommunal skole er separert i dedikerte tenants i den initielle arkitekturen, men teknisk sett kunne disse vært slått sammen i en tenant. Hovedårsaken til et skille er at fylkeskommuner og kommuner er selvstendige offentlige myndighetsorgan som tradisjonelt har separate IT-organisasjoner, så her trengs innspill fra disse organisasjonene ift mulig endringer.

Feide-innlogging

[Feide](#) er den nasjonale løsningen for sikker innlogging og datadeling i utdanning og forskning. Våren 2022 fikk Feide støtte for innlogging med Azure AD-autentisering, noe som gjør det mulig for elever og lærere å logge på tjenester som støtter Feide med sin Microsoft-konto.

Principle of Least Privilege

I [prinsippet om least privilege](#) skal en brukerkonto eller en prosess kun ha tilgang til det som kreves for å kunne utføre oppgaven, og gjerne kun i den perioden oppgaven utføres hvis mulig. Og kontoen bør ellers ha så lite rettigheter som mulig.

Dette prinsippet henger også tett sammen med det neste avsnittet om å skille tilgangsnivå på brukere.

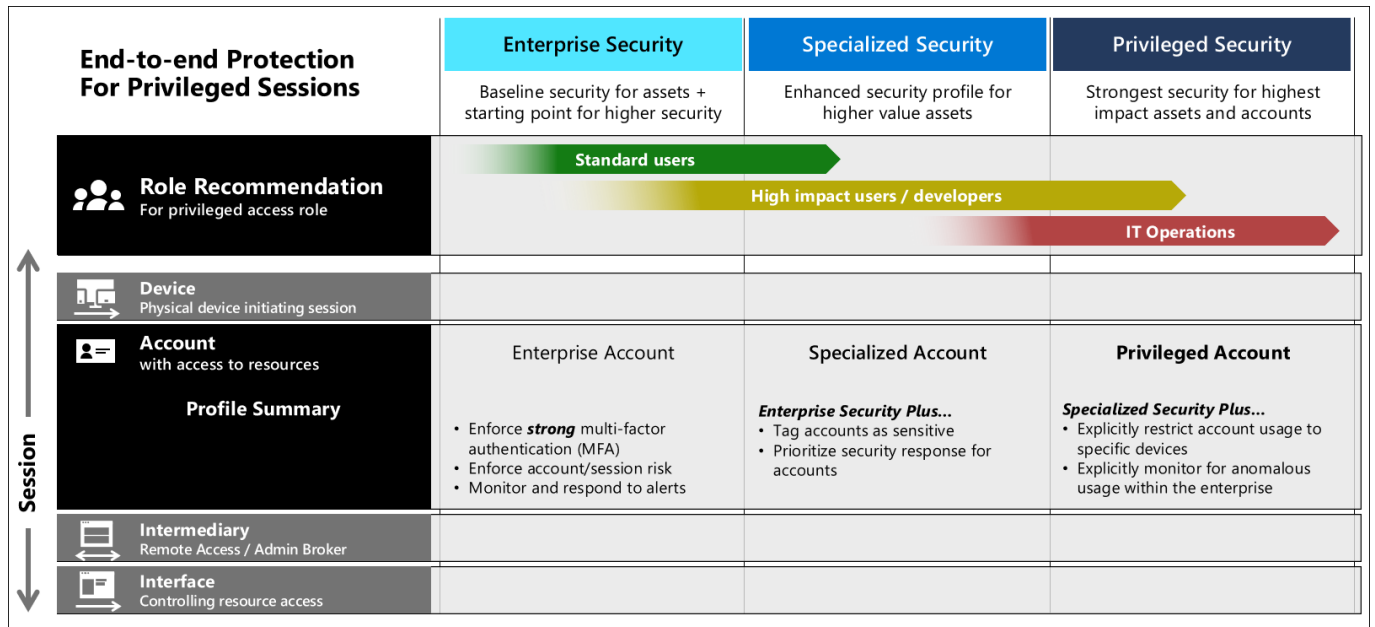
Skill tilgangsnivå på brukerkontoer

For brukere med høye tilgangsnivåer skal brukerkontoene som er gitt rettighetene skilles ut i egne brukere, og ikke gis til brukerens vanlige brukerkonto som brukes til å logge på PC-en og lese e-post med.

Eksempel på høye tilgangsnivåer: * Azure AD-roller, som Global administrator, User administrator, Security administrator, osv. * Tilgang til produksjonsmiljø for en tjeneste som kjører i en Azure subscription.

De samme prinsippene gjelder ikke kun for sky, men også on-premises-miljøer.

Illustrasjonen fra Microsoft viser tre ulike sikkerhetsnivåer for å skille brukerkontoer avhengig av rettighetene deres.



For mer informasjon, se Microsofts dokumentasjon på temaet: <https://docs.microsoft.com/en-us/security/compass/privileged-access-accounts>.

Klassifiseringmatrise for applikasjoner

Her er et forsøk på hvordan vi kan tenke rundt klassifisering/skille av applikasjoner:

- Publikumstjeneste/Applikasjon (Internett eksponert)
- Intern applikasjon (interne ansatte)
- Ikke PII/sensitivt
- PII/Sensitivt
- Begrenset (Sikkerhetsloven)
- Konfidensielt (Sikkerhetsloven)
- Ikke samfunnsskritisk (tåler noe nedetid)

Samfunnsskritiske tjenester som må kjøre og være tilgjengelig er delt på tvers av lokasjoner/uavhengig av lokasjon.

Sluttbrukere eller systemer - bruker internet (VPN eller MPLS) eller telefoni for å nå tjenester.

- Samfunnsskritiske - lokale tjenester (edge & hybrid) Samfunnsskritiske tjenester må fungere i nødssituasjon hvor deler faller ut og tåler lite/eller ingen nedetid eller er svært sensitive til latens.

Sluttbrukere/systemer befinner seg lokalt (e.g. et sykehus/ambulanse) mm.

Plan for tjenesteporteføljen

I forbindelse med etablering av en sky-strategi bør tjenesteporteføljen evalueres. Prinsipper for hvordan tjenesteporteføljen skal håndteres må etableres. Det anbefales å sanere tjenester der det lar seg gjøre, og standardisere og modernisere tjenestene man sitter igjen med. Jo mer moderne teknologi tjenestene støtter (som PaaS/Serverless) jo bedre og billigere kan de kjøre i sky samt moderne onprem miljø. Tjenester består ofte av flere komponenter. Hvis mulig anbefales det å flytte alle komponentene til en tjeneste til skyen. Ofte lar dog dette seg ikke gjøre ved første forsøk, og da ender man opp med en hybrid tjeneste som man kan jobbe med å utvikle og migrere til sky. Følgende flyt-diagram viser hvordan en slike evaluering kan gjøres:

PaaS onprem kan være en god løsning for tjenester som må stå i lokale datasentre grunnet regulativer, latens, etc.

On-premises

Dette er servere (virtualisert eller bare-metal) du har i dine egne datasentre hvor du kan drifte deler av applikasjon-sporteføljen i et hybrid miljø.

Nettverk

I et hybrid scenario (hybrid sky) som dette whitepaperet fokuserer på opprettes en tilkobling mellom Azure og det lokale nettverket. Dette for strekking av lokale tjenester (som integrasjoner) til sky, samt å kunne nå sky-tjenester

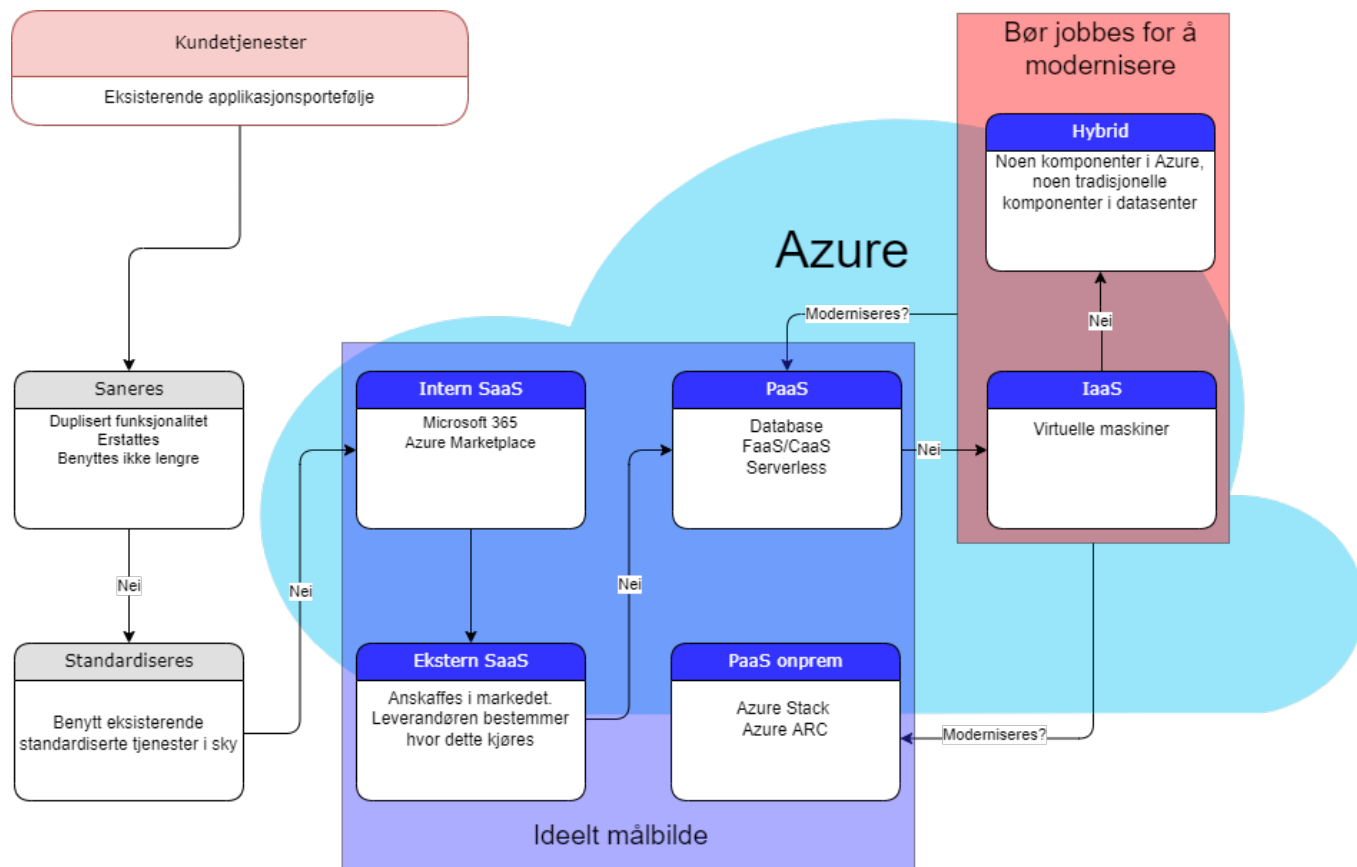


Figure 6: Tjenestemigrering flowchart

ifra lokalt nettverk. Denne utvekslingen av data gjøres på en sikker måte via en kryptert privat forbindelse slik som Site-to-Site VPN eller Azure ExpressRoute Direct.

Det er viktig å kjenne til at ExpressRoute er en privat kobling til Azure men den er ikke kryptert hvis man ikke bruker ExpressRoute Direct, som har mulighet for MACSec. Når man bygger koblinger fra datasenter eller kontor med ExpressRoute må man vurdere om alle protokoller som benyttes er krypterte eller om man må bruke VPN over Expressroute. De fleste moderne protokoller er allerede kryptert, men i ett moderniserings-prosjekt er det mulig att man må legge til kryptering (grunnet legacy trafikk).

Dersom det er et behov for mange klienter og/eller kontor som skal nå Azure over VPN/Express Route - så anbefales det å benytte Azure Virtual WAN. Dette forenkler ruting mellom nettverk både internt i Azure og hybride forbindelser mot lokale nettverk. Alternativet er en tradisjonell hub/spoke topologi hvor man manuelt håndterer ruting, noe som fort kan bli komplekst i store miljøer.

Sikring av nettverk

I Azure finnes det mange aspekter av nettverkssikkerhet. På mange måter kan man designe en nettverkstopolgi som ligner et tradisjonelt datasenter med mikrosegmentering mm.

Ser man på kommunal sektor har en tradisjonell sone-inndeling vært benyttet i stor grad, hvor grunnkonseptet er en administrativ sone (ofte kalt "åpent nett") plassert bak en "ytte brannmur" mot internett hvor vanlige klienter er plassert. I tillegg har man en sikker sone som er plassert bak en "indre brannmur". Det er som regel kun servere som kjører fagsystemer med sensitive data (typisk innen helsesektoren) og terminalservere som er plassert i den sikre sonen - hvor brukere aksesserer applikasjonene via publisert skrivebord (typisk Remote Desktop eller Citrix).

Videre har det vært vanlig med helt separat infrastruktur for skole/utdanning, med eksempelvis dedikerte nettverk med tilhørende dedikert instans av Active Directory - som er synkronisert ut til en egen Azure AD tenant.

Før man går i nærmere detaljer på hvordan dette anbefales i et sky-miljø bør man se på den helhetlige tilnærmingen til sikkerhet og identitet i skyen.

Sikkerhet i skyen

Når det kommer til hvem som er ansvarlig for sikkerhet i et skymiljø er dette generelt sett et felles ansvar mellom kunde og leverandør, men det er ulike grenser for ulike tjenestemodeller:



Figure 7: Ansvarsmodeller

For Software as a Service (SaaS)-tjenester slik som Office 365 hvor Microsoft drifter all underliggende infrastruktur har kunden «kun» ansvar for tilgangsstyring og data lagret inne i tjenestene. Infrastruktur rundt tjenestene slik som servere, nettverksinfrastruktur, høytligjengelig med mer håndteres av Microsoft.

Når det kommer til Azure er det flere tjeneste-modeller inne i bildet: - **Infrastructure as a Service (IaaS)** – Lagring, nettverk og virtuelle maskiner – hvor kunden selv har ansvaret for elementer som vedlikehold av operativsystem (pathing), eksponering av tjenester mot internett med mer. - **Platform as a Service (PaaS)** – Eksempelvis Azure SQL og lagringskontoer, hvor underliggende infrastruktur driftes og vedlikeholdes av Microsoft. Kunden konsumerer data-laget.

Microsoft har over flere år tilstrebet og anbefalt en «nulltillits-modell» (Zero Trust), hvor grunnprinsippene er:

- **Bekreft eksplisitt** – Valider alltid identitet, enheters helse og uregelmessige bruksmønstre
- **Benytt lavest privilegerte tilgang** – For å sikre både data og produktivitet, begrense brukertilganger ved hjelp av «Just In Time access» (JIT), «Just Enough Access» (JEA) og risikobaserte adaptive tilgangspolicyer
- **Anta sikkerhetsbrudd** – Minimer spredningsradiusen ved innbrudd ved å segmentere tilgang etter nettverk, brukere, enheter og applikasjoner. Krypter alle sesjoner ende-til-ende. Benytt analyseverktøy for å oppdage trusler, få innsikt etter eventuelle innbrudd og for å forbedre forsvar og sikkerheten.

Dette er en stor endring fra tradisjonelle tilnærminger:

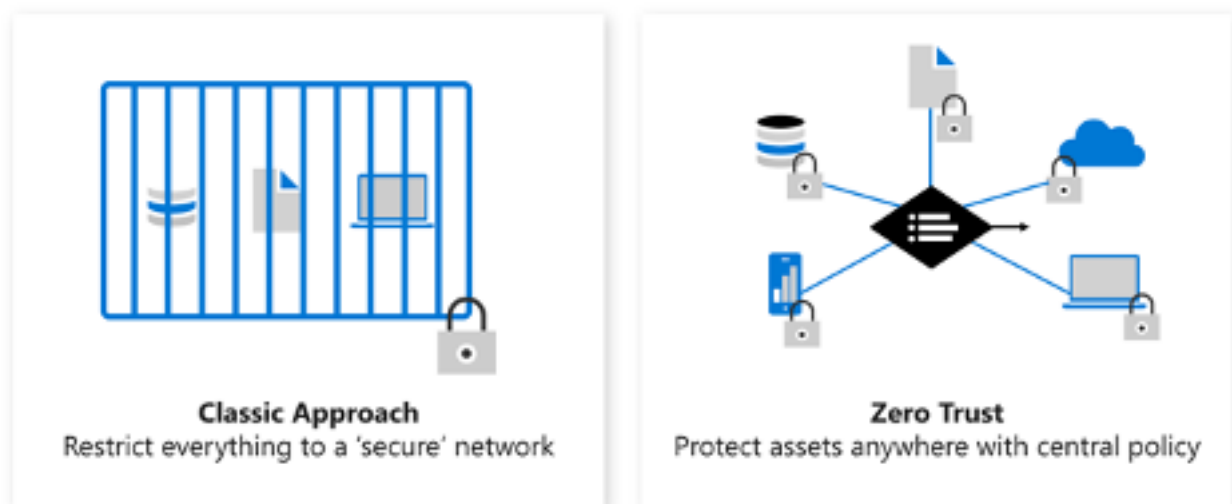


Figure 8: Tradisjonelle tilnærminger

Der hvor man tidligere satt fysisk på en arbeidsstasjon i det lokale nettverket benyttes det nå i stor grad mobile enheter (laptop, nettbrett, mobiler, med mer) og hjemme/hytttekontor.

Identitet har derfor blitt en ny viktig faktor for sikring, hvor bruk av multifaktor-autentisering og policy-basert styring har blitt essensielle virkemidler. Som en konsekvens av endrede bruksmønstre ser vi at identitet har blitt en

sterkere sikkerhets-mekanisme enn nettverk når det gjelder tilgang til produktivitetsløsninger som e-post og andre samhandlingsløsninger:

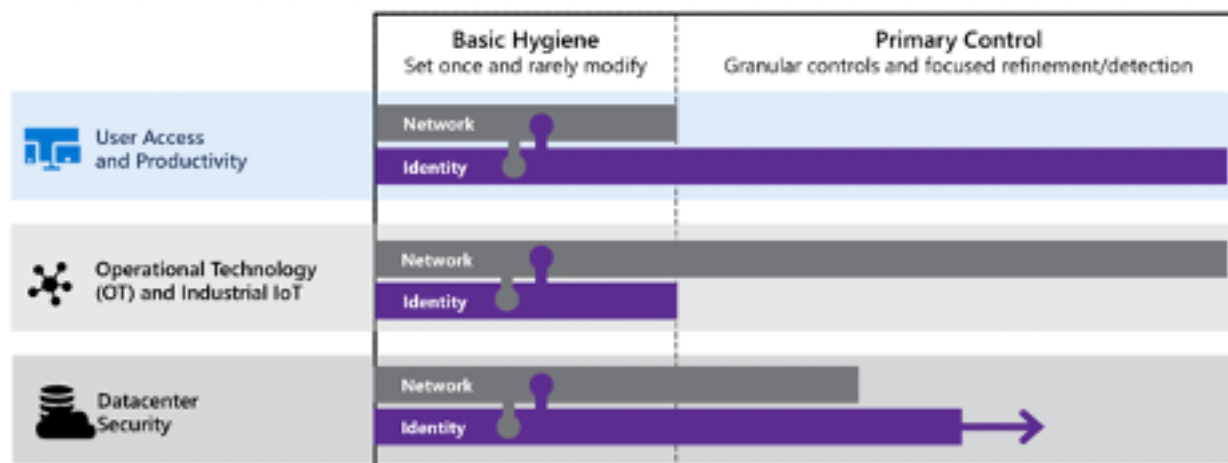


Figure 9: Tilgangsmekanismer

Når det kommer til infrastruktur har vi fremdeles behov for kontroll på nettverksnivået, men ved å følge Zero Trust prinsippene bør disse være mer segmenterte enn tidligere. Mikrosegmentering hvor det opprettes dedikerte nettverkssoner for hver enkelt applikasjon/løsning er derfor en anbefalt tilnærming.

En god del virksomheter har i prinsippet også en slik tilnærming for lokal infrastruktur i dag, hvor dedikerte nettverkssegmenter er opprettet for IoT-enheter og ulike andre formål, slik som dedikerte subnet for fagapplikasjoner med ulike krav til sikkerhet.

Det anbefales at samme tilnærming videreføres i Azure, og at det etableres en sentral tilgangskontroll via en brannmur og/eller nettverkssikkerhetsgrupper (NSG - Network Security Groups). NSGer – som forenklet kan ses på som aksesslister tildelt til virtuelle nettverkskort - skalerer til et visst punkt, hvor det typisk blir nødvendig med en sentral styringsmekanisme for enklere administrasjon og oversikt.

Azure Firewall er en PaaS-tjeneste for nettopp dette formålet, som på generell basis anbefales fremfor 3. parts appliance-løsninger for lavere TCO (Total Cost of Ownership).

Verktøy

For å understøtte Zero Trust-prinsippene har Microsoft en hel del verktøy og tjenester som er relevante i kontekst av sikkerhet i Azure:

- **Defender for Cloud Apps** – En såkalt "Cloud Access Security Broker" som primært fokuserer på SaaS-tjenester for å få en total oversikt over tjenester i bruk (avdekke eventuelle «Shadow IT»-tjenester). I tillegg til tett integrasjon med Microsoft 365 finnes connectorer mot en hel del 3. parts skytjenester. Unormal aktivitet på tvers av skytjenester er et scenario som kan oppdages og varsles på med denne tjenesten.

- **Azure AD Identity Protection** – Basert på en hel del signaler slik som lokasjon, IP-adresser og andre elementer vil denne tjenesten kunne avdekke potensielle farer og klassifisere risiko ved brukerpålogginger (Lav, Middels, Høy risiko) i Azure AD. Eksempel på et scenario er atypisk reise, hvor en bruker logger på fra 2 forskjellige land eller verdensdeler med kort mellomrom. Da vil denne tjenesten kunne konfigureres til å varsle og hvis ønskelig blokkere brukerkontoen, slik at man har automatisk blokkering for scenarier hvor en brukerkonto kan ha blitt kompromittert.

- **Defender for Identity** – En skytjeneste som samler informasjon og signaler fra on-prem Active Directory i form av sensorer/agenter på domenekontrollere. Tjenesten kan avdekke scenarier som «lateral movement», hvor en kompromittert konto benyttes for å logge seg på videre inn til andre servere eller klienter.

- **Defender for Cloud** – En skytjeneste som kontinuerlig scanner tjenester i et Azure-abonnement for å gi et innblikk i sikkerhetskonnfigurasjon og tilby anbefalinger for å øke sikkerheten. Det er flere under-tjenester som kan aktiveres som en del av denne tjenesten

- Microsoft Defender for Servers
- Microsoft Defender for Storage
- Microsoft Defender for SQL
- Microsoft Defender for Containers
- Microsoft Defender for App Service
- Microsoft Defender for Key Vault

- Microsoft Defender for Resource Manager
- Microsoft Defender for DNS
- Microsoft Defender for open-source relational databases
- Microsoft Defender for Azure Cosmos DB (Preview per Mars 2022)

Hver av disse undertjenestene har egne pris-modeller, eksempelvis Microsoft Defender for Servers har en sum per måned per server som modell – mens Defender for Resource Manager er priset basert på antall forespørsler som går gjennom Azure Resource Manager (API-tjenester hvor alle Azure management-operasjoner går gjennom).

Defender for Servers kan også benyttes på maskiner utenfor Azure, slik som servere i eget datasenter eller andre skyplattformer. Tjenesten inkluderer lisens for Defender for Endpoint, og gir følgende ekstra funksjonalitet:

- Verktøy for scanning av sårbarheter i operativsystemet – her kan man velge mellom Microsofts egen «threat and vulnerability»-løsning og en sårbarhets-scanner fra Qualys (en av de ledende leverandørene av sanntids identifisering av sårbarheter) som er lisensiert som en del av tjenesten.
- Docker nedlåsning – Containere som kjører inne i virtuelle maskiner scannes og sammenlignes opp mot CIS (Center for Internet Security) sine Docker Benchmarks.
- Fil-løs angrepsdetektering – Angrep hvor payloads ikke lagres på disk, men kun kjøres i minne og typisk persisteres inne i kompromitterte prosesser oppdages og alarmeres på.
- Auditd alarmer (for Linux) – auditd er et subsystem på kernel-nivå som er ansvarlig for å overvåke kall til kernel. Defender for Servers detekterer unormal aktivitet slik som tvilsomme prosesser og innlasting av ukjent kernel-moduler.

• **Defender for IoT** – tjeneste som ikke går under Defender for Cloud, men som også er en viktig komponent rundt skysikkerhet. Produktet ble lansert i Januar 2021 som et resultat av et oppkjøp («CyberX»), og er myntet på enheter som i motsetning til laptop og telefoner ikke støtter installasjon av agenter eller annen management-software. De går dermed på mange måter under radaren når det kommer til overvåking og synlighet overfor sikkerhetsansvarlige. Uten en slik synlighet er det veldig utfordrende å oppdage om enheter er kompromitterte. En rekke enheter for industrielle kontrollsystemer tilknyttet områder som elektrisitet, vann, transport, datasentre, smarte bygninger, farmasi, olje og gass samt andre kritiske løsninger går inn i denne kategorien enheter. Defender for IoT er agentløs, og har innebygd kjennskap til en stor mengde industrielle protokoller og benytter seg av utstrakt bruk av Machine Learning og automatiserte deteksjoner på samme måte som flere av Microsofts andre skysikkerhetsløsninger. For å benytte denne løsningen kan en fysisk eller virtuell appliance settes opp for mottak av kopi av nettverkstrafikk fra switcher (vha SPAN port eller TAP), slik at tjenesten ikke påvirker IoT-enhetene som overvåkes på noe vis. I videoen under ifra Microsoft Ignite, spilt inn kort tid etter oppkjøpet av CyberX, vises integrasjon med Microsoft Sentinel og hvordan alarmer for eksempelvis uautorisert PLS-programmering fanges opp.

• **Microsoft Sentinel** – En SIEM (security information and event manager) plattform basert på stor grad av innebygd AI (Artificial Intelligence) for analysering av store datamengder.



Figure 10: Sentinel

Selv om dette er en skytjeneste kan den også samle inn data fra hvor som helst, som for eksempel logger fra on-prem nettverksutstyr kan streames ut via syslog.

Det er over tid bygget opp et stort community rundt Sentinel, og man kan finne en rekke spørringer og såkalte playbooks både fra Microsoft og andre på steder som GitHub. Playbooks gjør det mulig å blant annet foreta automatiske handlinger basert på hendelser som oppstår, for eksempel å blokkere en bruker, sende varsel til en Teams-kanal eller å opprette en sak i et brukerstøttesystem slik som ServiceNow eller andre.

Det finnes også en hel del connectorer mot for eksempel Azure AD, aktivitetslogger i Azure, Defender for Cloud, Defender for Identity, Checkpoint, Cisco, AWS, Google med mange flere for innsamling av data. Sentinel vil dermed kunne være et sentralt nav for deteksjon og håndtering fra mange (potensielt alle) kilder som benyttes i en organisasjon.

- **Azure Arc for Servers** – Dette er en tjeneste som gjør det mulig å prosjektere servere som kjører utenfor Azure inn som objekter i Azure. Dette muliggjør bruk av tagging slik at man har ett sted å samle metadata om servere. En annen funksjon som er kjernen i det denne tjenesten muliggjør er installasjon av [VM extensions](#), slik som Azure Monitor Agent og Defender for Servers. Andre eksempler som kan trekkes frem er Azure Automation Hybrid Runbook worker extension, som gjør det mulig å kjøre PowerShell og Python runbooks på on-prem servere. En annen er Azure Key Vault Certificate sync, som gjør det mulig å synkronisere et sertifikat fra et sentralt Key Vault ut mot flere servere.

Conditional Access

Betinget tilgang (conditional access) er en funksjon i Azure Active Directory som gjør det mulig å definere policyer som forenklet sagt er et sett med «if then»-klausuler.

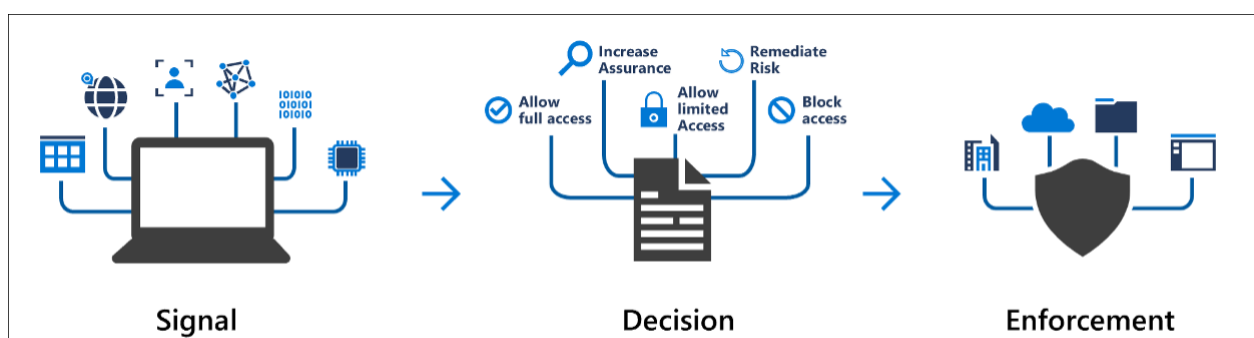


Figure 11: Betinget tilgang

En rekke signaler samles og evalueres. Policyer kan defineres å gjelde all autentisering mot alle applikasjoner i Azure AD, eller granuleres per applikasjon. Mange har allerede definert slike policyer for tilganger til Microsoft 365.

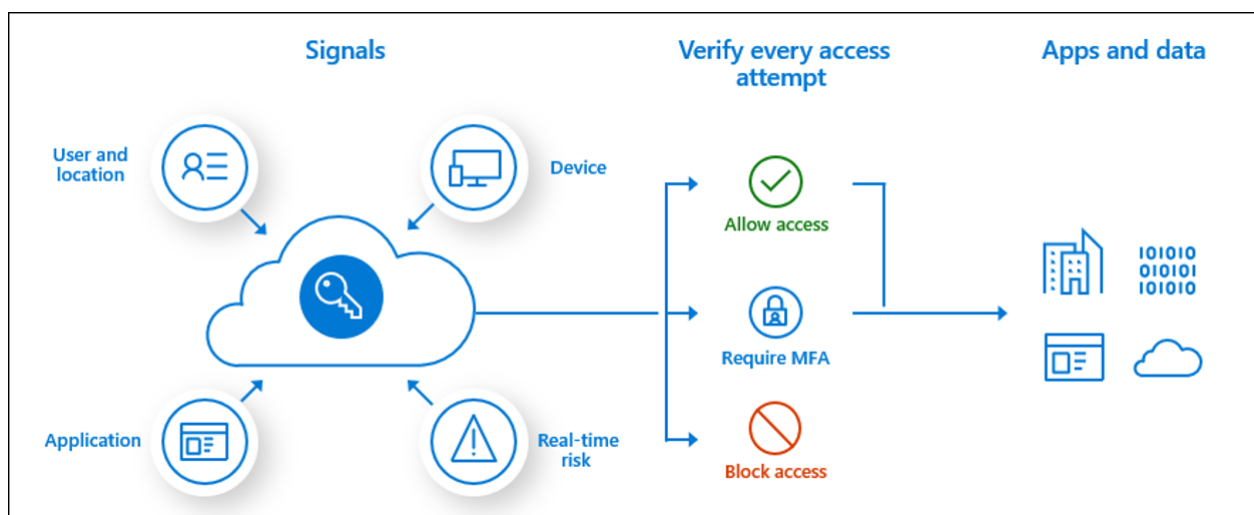


Figure 12: Betinget tilgang

Signaler som ofte brukes:

- Gruppemedlemskap – for å begrense en policy eller tilgang til en bestemt gruppe brukere
- IP lokasjonsinformasjon – IP-ranger som anses som trygge slik som bedriftens offisielle IP-adresse ut mot internett samt geografisk tilhørighet til offisielle adresser brukere logger på fra
- Enheter – type operativsystem og informasjon om enheten er en del av Azure AD og/eller Active Directory
- Applikasjon – spesifikke applikasjoner kan trigge dedikerte policyer
- Sanntids risikoanalyse

- Integrasjon med Azure AD Identity Protection for scenarier som atypiske reiser (pålogging fra 2 land med kort tids mellomrom)
- Microsoft Defender for Cloud Apps
 - Muliggjør ytterligere innsikt i brukeres pålogginger og aktiviteter

Basert på signaler kan ulike avgjørelser defineres:

- Blokkere tilgang (den mest restriktive avgjørelsen)
- Tillate tilgang
 - Betingelser hvor en eller flere av følgende påkreves
 - * Multifaktor autentisering
 - * Enhet må være markert som trygg (oppdaterte antivirus/malware-definisjoner som et eksempel)
 - * Enhet må være hybrid Azure AD joined
 - * Klient-applikasjonen som aksesseres må være forhåndsgodkjent

Ønsker man å begrense tilgang til administrasjonsverktøyene i Azure er det mulig å lage en policy som vil legge restriksjoner på tilgang via:

- Azure portal
- Azure Resource Manager provider
- Classic Service Management APIs
- Azure PowerShell
- Visual Studio Subscriptions administrator portal
- Azure DevOps
- Azure Data Factory portal

Selv om en standard bruker ikke har noen tilganger i Azure vil man kunne logge på portal.azure.com, men ikke se noen abonnementer eller ressurser. Dette vil blokkeres for vanlige brukere ved innføring av en slik policy.

Nettverk

Private endepunkter

Et privat endepunkt i Azure er et virtuelt nettverkskort med en privat IP adresse fra et virtuelt nettverk man selv har opprettet, og som dermed kan tilgjengelig gjøres fra interne on-prem nettverk via ExpressRoute eller VPN. Dette nettverkskortet kobles til Azure Private Link for å bringe PaaS-tjenester inn i det interne nettverket.

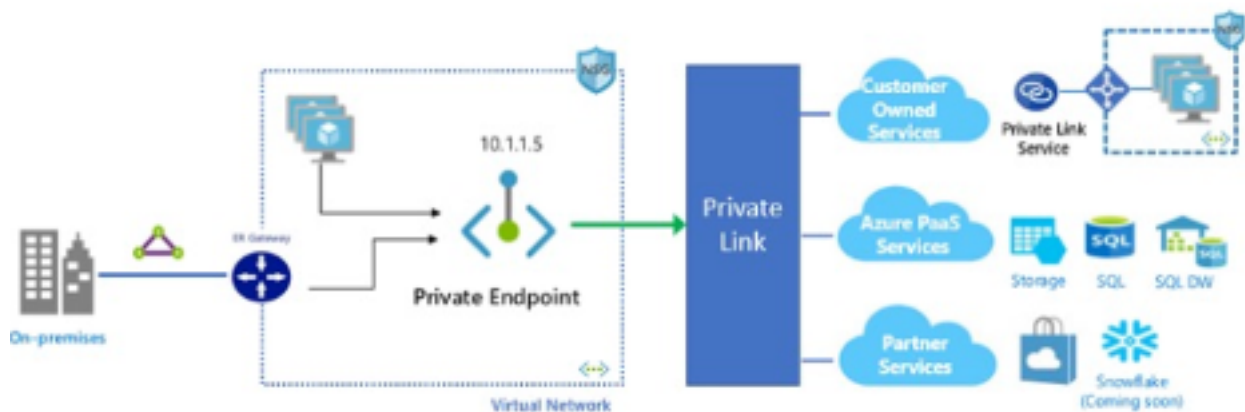


Figure 13: Privat endepunkt

Med dette oppnås en høyere grad av sikkerhet, siden ekstern tilgang for tjenester kan deaktiveres.

Selv om tjenester står eksponert direkte mot internett via offisielle IP-adresser betyr det ikke nødvendigvis at de er usikre. For eksempel et Key Vault kan likevel være sikret på identitetslaget i form av multifaktor-autentisering, på samme måte som en SaaS-tjenesten slik som Exchange Online. En fordel med å bruke private endepunkter er bedre beskyttelse mot data-lekkasjer grunnet feil konfigurasjon av tilganger. Eksempelvis vil en mappe i en lagringskonto være åpent tilgjengelig via internett dersom rettighetene på mappen ved en feil er satt til anonym tilgang. En annen fordel er at PaaS-tjenester som er konfigurert med private endepunkter kan aksesseres via ExpressRoute, og dermed unngå å måtte traversere internett. Det vil gi lavere latens, siden trafikken går via den private kommunikasjonslinjen fra ExpressRoute til ISP-en.

Fysisk sikring av datasenter

Artikkelen [Azure security fundamentals documentation](#) inneholder en hel mengde informasjon om sikkerhet i sky - blant annet [denne artikkelen](#) som beskriver fasiliteter og fysisk sikkerhet på Microsofts datasentre.

Microsoft har også en [virtuell datasenter omvisning](#) som kan anbefales for å få et visuelt inntrykk av den fysiske sikkerheten.

På [Microsoft Service Trust Portal](#) er ytterligere dokumentasjon rundt valideringer utført av 3. parter opp mot industri-standarder tilgjengelig.

Tekniske komponenter for sikring og compliance

Azure Datasenter sikring

Kryptering i Azure

Moderne nettverksprotokoll er krypterte og standardinstillingene på Azure Platform tjenester er att di er kryptert med TLS.

All data som lagres i Azure er også kryptert, standardinstillingene bruker krypteringsnøkler som Microsoft genererer og håndterer for kunden slik at alt er transparent. Hvis ønskelig kan man bruke kundeadministrerte krypteringsnøkler ("Customer Managed Keys"). Da må kunden håndtere disse selv og hvis man mister disse er dataene utilgjengelige.

Azure HSM

Nøkkelhåndtering og hemmelighetshåndtering i Azure har flere nivåer av sikkerhet slik at hver kunde får sine behov trygget.

- Azure Key Vault Standard: Programvarebasert sikker nøkkelhåndtering.
- Azure Key Vault Premium: Har samme funksjonalitet som Standard men alle nøkler og hemmeligheter lagres på en maskinvarebasert sikkerhetsmodul (Hardware Security Module, HSM). FIPS 140-2.
- Azure Key Vault Managed HSM: Key Vault med dedikert maskinvarebasert sikkerhetsmodul. FIPS 140-3.
- Azure Dedicated HSM: Gir full tilgang til en maskinvarebasert Thales sikkerhetsmodul som er hostet i Azure Datasenter. Kan brukes som og kobles til On-Premise Thales HSMer. FIPS-140-3.

Konfidensiell Databehandling

Den seneste forbedringen i datasikkerhet er "Confidential Compute", Konfidensiell Databehandling. I korthet handler det om å kryptere all data også mens den behandles. Kombinert med kryptering på nettverk og lagring kan kunden forsikre seg om att ikke engang Microsoft kan lese dataen mens den behandles.

Konfidensiell databehandling kan ikke anses som en magisk løsning til datasikkerhet men den kan være en viktig byggestein ved håndtering av sensitiv data. KD/CC fjerner behov å stole på de som har fysisk tilgang til serverene eller administrativ tilgang til virtualiseringslaget (Hypervisor). Rent juridisk vil Confidential Compute trolig ikke løse utfordringer rundt GDPR og Schrems-II.

Customer Lockbox

Azure Support trenger oftest ikke tilgang til kundedata ved feilsøking. Hvis support trenger tilgang til kundedata må en leder godkjenne en forespørsel internt som gir tidsbegrenset tilgang til kundedata. Denne prosessen har blitt utvidet å gi mulighet for kunden å godkjenne/avslå forespørselen.

<https://docs.microsoft.com/en-us/azure/security/fundamentals/customer-lockbox-overview>

Azure Policy

Endringer i kundens Azure infrastruktur bestilles programmatisk via ett API som kalles "Azure Resource Manager". Til dette APIet kan kunden legge til egne regler eller aktivere eksisterende eksempelregler fra Microsoft. Disse retningslinjer kan advare, stoppe eller automatisk endre på bestillingen. Med bruk av Azure Policy kan man oppfylle interne og eksterne standarder på datasikkerhet, logging m.m.

Azure ARC

Azure Dedicated Hosts

Azure har streng separasjon mellom virtuelle maskiner på samme fysiske server men det er situasjoner der man ønsker enda mer separering. I slike tilfeller kan man ta i bruk dedikerte servere. Da betaler kunden for en hel server med f.eks. 100 prosessorkjerner og 768 GB RAM og velger selv størrelsen på de virtuelle maskiner som kjører på serveren.

Utvalgte sikkerhetselementer

- Security baseline
- Security baseline (Azure Stack Edge)
- [Security baseline \(Azure Stack HCI\)](#)
- Azure Active Directory : Conditional access
- Azure Active Directory : Privileged identity management (PIM)
- Microsoft Defender for Cloud
- Azure DDOS Protection

Krisesituasjoner

I en særskilt krisesituasjon bør vi stille oss følgende spørsmål:

- Hvor lang tid tar det før ditt eget utstyr begynner å feile (on-premises utstyr)?
- Hvilke 'skjulte' avhengigheter har dine systemer? (eks. DNS/CA mm)
- Hvordan skal sluttbrukere nå applikasjoner som er eksponert på internett?

Særskilte norske lover, krav og anbefalinger(som man bør ta stilling til)

- [Arkivloven](#): “Arkivloven inneholder ingen bestemmelser som direkte regulerer lagring av arkiv i skytjenester, og er i utgangspunktet ikke til hinder for bruk av slike løsninger. Det følger likevel av arkivloven § 9 b at arkivmateriale ikke kan «først ut or landet, dersom dette ikke representerer ein naudsynt del av den forvaltningsmessige eller rettslege bruken av dokumenta.” Når det er lagt til grunn at den fysiske lagringsplassen avgjør hvor data er å finne, følger det naturlig av denne bestemmelsen at overføring av arkivmateriale til servere i utlandet bryter med forbudet mot å føre arkiv ut av landet.”

NSM - Råd og anbefalinger for IKT sikkerhet

NSM har en rekke råd og anbefalinger for IKT sikkerhet. [Grunnprinsipper for IKT-sikkerhet 2.0](#) er et supplement til eksisterende nasjonale og internasjonale regelverk, standarder og rammeverk innen IKT-sikkerhet og er inspirert av mange av disse.

Tekniske tiltak fra grunnprinsipper for IKT-sikkerhet kan knyttes mot Azure Policies for en automatisert overvåkning og rapportering av compliance på tvers av hele virksomhetens digitale eiendom. Azure har over 700 eksisterende innebygde policies for IaaS, PaaS og hybrid i tillegg til muligheten for å lage egne tilpassede policies. En samling av Azure policies som er gruppert etter et felles formål kalles en Policy Initiative. Tilsvarende samlinger av Azure policies finnes og vedlikeholdes av Microsoft for anerkjente internasjonale regelverk som: [ISO 27001:2013](#) og [CIS 1.3.0](#).

Under vises et skjermbilde fra Azure Policy sin compliance oversikt hvor utvalgte NSM prinsipper er knyttet inn. Merk at dette kan gi en oversikt på tvers av tjenester og infrastruktur, med Azure Arc kan man også evaluere policy tilstand mot hybrid og multisky.

Compliance i Azure Policy viser tilstanden for de spesifikke policy definisjonene man har knyttet opp og det vil sjeldent være et en-til-en forhold mellom en kontroll i et rammeverk og en policy. Et rammeverk eller en standard vil også inneholde prosess og organisatoriske tiltak som ikke kan knyttes opp mot en teknisk policy. Derfor vil compliance mot f.eks NSM grunnprinsipper, ISO 27001:2013 eller CIS 1.3.0 i Azure Policy kun gi en delvis oversikt over det totale bildet.

Under vises et eksempel på sikkerhetstiltak fra ulike kategorier i NSM grunnprinsipper som er knyttet mot relevante Azure Policies. Et sikkerhetstiltak kan ha flere Azure Policies for en bredere dekning og eksempelet viser muligheten for kombinasjon på tvers av IaaS, PaaS i Azure og hybrid/multisky.

Eksempel: NSM grunnprinsipper for IKT-sikkerhet 2.0 policy initiative

Sikkerhetstiltak	Grunnprinsipp	Kategori	Azure Policy referanse	Kommentar
2.3.1 Installer sikkerhetsoppdateringer så fort som mulig.	2.3 Ivareta en sikker konfigurasjon	2. Beskytte og opprettholde	System updates should be installed on your machines	IaaS i Azure

Sikkerhetstiltak	Grunnprinsipp	Kategori	Azure Policy referanse	Kommentar
2.5.1 Styr dataflyt mellom nettverks-soner.	2.5 Kontroller dataflyt	2. Beskytte og opprettholde	All network ports should be restricted on network security groups associated to your virtual machine	Azure nettverk
2.5.1 Styr dataflyt mellom nettverks-soner.	2.5 Kontroller dataflyt	2. Beskytte og opprettholde	Storage accounts should restrict network access	Azure nettverk
2.6.7 Bruk MFA for å autentisere brukere.	2.6 Ha kontroll på identiteter og tilganger	2. Beskytte og opprettholde	MFA should be enabled on accounts with write permissions on your subscription	Azure AD
2.7.2 Aktiver kryptering i de tjenestene som tilbyr slik funksjonalitet.	2.7 Beskytt data i ro og i transitt	2. Beskytte og opprettholde	Secure transfer to storage accounts should be enabled	PaaS i Azure
2.7.3 Krypter lagringsmedier som holder konfidensiell data.	2.7 Beskytt data i ro og i transitt	2. Beskytte og opprettholde	Transparent Data Encryption on SQL databases should be enabled	PaaS i Azure
2.7.4 Benytt kryptering når konfidensiell informasjon overføres.	2.7 Beskytt data i ro og i transitt	2. Beskytte og opprettholde	Web Application should only be accessible over HTTPS	PaaS i Azure
3.1.1 Gjennomfør jevnlig sårbarhetskartlegging.	3.1 Oppdag og fjern kjente sårbarheter og trusler	3. Oppdage	A vulnerability assessment solution should be enabled on your virtual machines	IaaS i Azure eller hybrid-og multisky med Azure Arc
3.1.3 Benytt automatisert og sentralisert verktøy for å håndtere kjente trusler (som skadevare).	3.1 Oppdag og fjern kjente sårbarheter og trusler	3. Oppdage	Monitor missing Endpoint Protection in Azure Security Center	IaaS i Azure eller hybrid-og multisky med Azure Arc

Mer detaljerte eksempler vil være å finne under [Implementasjon](#)

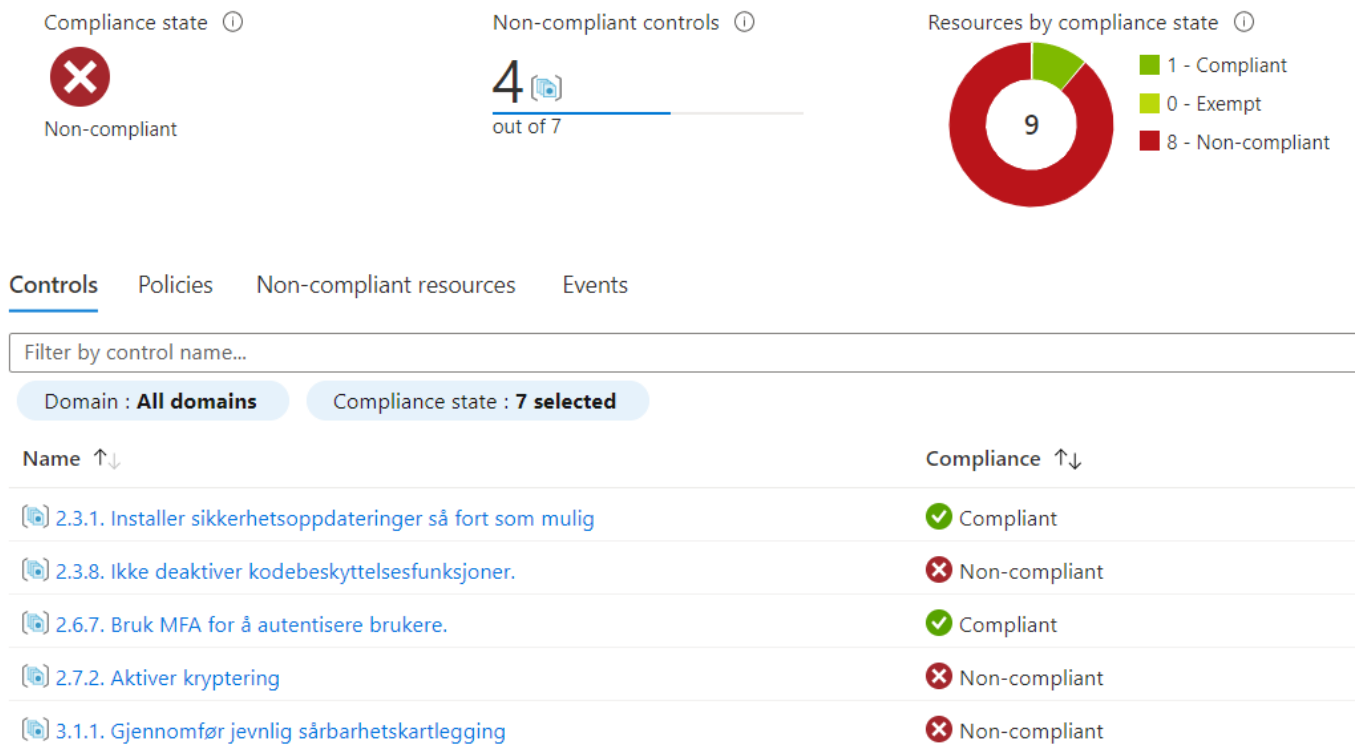


Figure 14: Policy initiative

CSA Cloud Controls Matrix (CCM)

Cloud Security alliance og (<https://cloudsecurityalliance.org/research/cloud-controls-matrix/>)[CCM mapping] er vanlig brukt for benchmarking mot ulike sertifiseringer og i kravspesifikasjoner rettet mot skyleverandør.

Microsoft har en omfattende mapping på hvordan dere skyløsning mappes mot CCM kontrollere.

Se full rapport her mot ulike kontroller fra f.eks CIS/NIST/PCI/ISO mm: <https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/>

Automatisering og xOps

Mulighetene for automatisering i allmenn sky bidrar til å øke potensialet til DevSecOps og en xOps-tilnærming.

Uten automasjonsprosesser vil mange etablerings- og vedlikeholdsoppgaver måtte gjøres manuelt. Dette bidrar til at oppgavene tar lengere tid, og kan medføre at miljøene blir får flere feil enn det ville fått med automatiske prosesser.

Automatisering i seg selv ikke er målet, da feil bruk av automatisering kan skape like mange problemer som det løser. Derimot skal det påpekes at automatisering er en styrkemultiplikator som kan bidra til at oppgaver kan gjøres raskere og feilfritt.

De viktigste områdene der automasjon bidrar inkluderer

Konsistens: Skala- og stordriftsfordeler krever at systemer og løsninger etableres på en konsistent og enhetlig måte. Gjennom bruk av automasjon sikrer organisasjonen seg for at standarder følges og at like systemer forblir like, også over tid.

Felles metodeverk og plattform: Gjennom bruk av automasjon ser man at oppgaver som utføres andre steder i IT-miljøet eller organisasjonen kan gjenbruke de samme prinsippene som tas i bruk i allmenn sky. Dermed oppnår man etter hvert å gjennomføre samme metoder på tvers av plattformer og miljø, noe som er med til å forbedre organisasjonens verdi og leveransekraft.

Raskere utførelse og feilretting: Når man benytter automasjon og kodebasert infrastruktur vil tiden man får igjen fra manuelle prosesser kunne benyttes til mer produktive aktiviteter. Samtidig blir feilsøking enklere gitt at man har en baseline å forholde seg til, hva har gått feil underveis.

xOps

Det er ikke bare tradisjonelle driftsprosesser (Operations – derav Ops) som er aktuelle for sky, men man ser at det er flere navn på moderne driftsformer som for eksempel AgileOps og DevOps/DevSecOps. I bunn og grunn betyr det en tettere knytning mellom utviklere, de som jobber med infrastrukturen og de som følger opp infrastrukturen og applikasjonene i etterkant. For å få opp hastigheten og kontrollen av dette kommer punktene under som en nødvendighet for å lykkes med xOps

Det viktigste med disse er at de er mer agile enn tradisjonelle driftsformer, og noen av metodene for å få opp takten samtidig som man øker tilgjengelighet og reduserer TTR (time to resolve) inkluderer:

- Høy grad av automatisering.
- Definere infrastruktur med script eller kode.
- Feiltolerant arkitektur.
- Resistente applikasjoner som tåler feil.

Dette er ikke noe nytt, men denne type metodikker gjør seg stadig mer aktuelle ved bruk av sky samtidig som hele skyplattformen er mulig å programmere mot; både som administrator og utvikler.

Med høy grad av automatisering kreves standarder, prinsipper og ikke minst forståelse som gjenspeiler seg i organisasjonens kultur. Det handler om hvordan en IT- eller utviklingsavdeling benytter de tilgjengelige verktøyene på best mulig måte, satt i et system som fungerer på tvers av roller og miljø i organisasjonen.

En annen grunn til at det er viktig å drive denne kulturendringen er å kunne senke listen for å få gjort endringer og publisert ny kode eller nye løsninger.

Infrastruktur som kode / Infrastructure as code (IaC)

Det er ofte lett å opprette nye ressurser i en allmenn skytjeneste gjennom selvbetjeningsportaler. Det opprettes da gjerne manuelt, og manuelle prosesser kan lede til feil over tid. I tillegg vil manuelle prosesser ofte være dårligere dokumentert slik at når man skal gjenskape en løsning så vil den ikke bli gjenskap helt likt.

Infrastruktur som kode (IaC), sørger for å opprette/provisjonere ressurser ved bruk av kode.

IaC, i kombinasjon med et system for versjonskontroll (typisk Git), gir oss fordeler som:

- Informasjon om hvem, hva og hvorfor en endring ble gjort.
- Det kan settes arbeidsflyter som f.eks. at en endring skal godkjennes av andre.
- Understøtter DevSecOps.
- Gjenbruke kode på tvers av miljøer (som dev, test, qa og prod) – og dermed få et helt likt miljø på tvers.
- Man kan enkelt opprette midlertidige miljøer for test, for så å rive det ned, noe som utnytter de økonomiske mulighetene som ligger i bruk av allmenn sky.
- Enklere etablere miljøet på nytt ved et disaster recovery-scenario.
- Ved et konfigurasjonsendring som ikke fungerte som tiltenkt kan du rulle tilbake til en tidligere versjon av koden.

- Vi har full oversikt over endringer, og vi ser hva som er gjort av hvem når.
- Vi ser ofte at man får et ryddigere miljø, der navnestandarder følges i større grad og valg gjort i infrastrukturen er i større grad gjennomtenkte.

Valg av verktøy

Det finnes flere løsninger/språk for infrastruktur som kode. Noen av de mest populære er:

- Terraform (cloud agnostic)
- Pulumi (cloud agnostic)
- Bicep (kun for Azure)

Prinsipper for bruk av infrastruktur som kode

For at infrastruktur som kode (IaC) skal fungere optimalt i organisasjonen bør noen prinsipper følges:

- *Lagre koden i et system for versjonshåndtering* (Version Control System – VCS). Dette er kilden og dokumentasjonen over infrastrukturen. Endringer i infrastrukturen er drevet av endringer gjort i versjonshåndteringen. På denne måten får vi:
 - Vi ser hvem som har gjort hva, og aller helst med en kommentar om hvorfor.
 - En kollega kan gå gjennom endringen og godkjenne før endringen rulles ut.
 - Det er ofte lett å endre systemet tilbake.
 - Det er lett for alle i teamet å se hvilke endringer som gjøres.
 - Når en endring er gjennomført kan det automatisk trigge andre hendelser. For eksempel en trigger som kjører en automatisk test av at systemet fungerer som planlagt.
- *Bygg alt med kode*. Ikke ta snarveier ved å lage noe manuelt. Man vil da miste fordelene med å få en fullstendig oversikt ved å se på koden.
 - Lås gjerne ned muligheten for å endre konfigurasjon og etablere nye ressurser ved å la brukerne kun ha lesetilgang til miljøet. Prosessen for infrastruktur som kode bør kjøre som en service-konto i en eller annen form.
- *Dokumenter minimumet*. For å hindre at dokumentasjonen blir utdatert, dokumenter bare det aller nødvendigste av infrastrukturen andre steder. Koden er alltid den oppdaterte dokumentasjonen.
- *Benytt organisasjonens prefererte verktøy for infrastruktur som kode*. Ved at alle benytter det samme kan enklere dele kunnskap, arbeidsmetodikk og jobbe på tvers av teams. Bli også enig om et sett med standarder for navngiving og struktur.
- Gjør små endringer, istedenfor store bolker med endringer. Noen fordeler:
 - Lettere å teste
 - Lettere å rulle tilbake endringen
 - Lettere å feilsøke
 - Et lite problem kan forsinke en stor utrulling. Når man tar det i mindre bolker, kan fortsatt andre endringer gjennomføres.
 - Det er mer motiverende å gjøre unna små endringer, fremfor store endringer som kan føles uoverkommelig.

Konfigurasjonshåndtering

Konfigurasjonshåndtering, eller Configuration management, håndterer konfigurasjonsstyring på OS- og applikasjonsnivå. Dette sørger for førstegangsoppsett av OS og applikasjon og senere konfigurasjonsendringer.

Eksempel på slike verktøy:

- Chef
- Puppet
- Ansible
- Microsoft DSC (PowerShell Desired State Configuration)

Disse verktøyene integrerer godt med løsninger for infrastruktur som kode og det bør være et mål at tjenester som har behov for VM-er i sky benytter en form for automatisering av konfigurasjonen.

Implementasjon

Når det kommer til praktisk implementasjon er det flere metoder å gjøre dette på, selv om man benytter seg av et eksisterende rammeverk som Cloud Adoption Framework Enterprise-scale (Hub-Spoke eller virtual WAN). En oversikt over mulige implementasjonsvalg er tilgjengelig [her](#).

I den initielle referanse implementasjonen for kommunal sektor ser man for seg Enterprise Scale implementasjonen benyttes som et fundament. Denne setter opp en rekke basis funksjonalitet for skyplattformen og inkluderer en rekke regler (policies) som man kan velge å ta i bruk og som forhåndskonfigureres basert på valg man gjør ved første gangsoppsett.

NB: Det er viktig å nevne at dette kun er en mal, og man må ha en styring/forvaltningsgruppe som jobber med kravene og plattformen med fullstendig målbilde for sin kommune. Regelsett bør også forvaltes sentralt på sikt.

Referanseimplementasjonen tilgjengeliggjør en rekke regler - men setter relativt liten føring på hvilke regler (policies) som er aktive og dette bør videreutvikles når plattform modnes og over tid. Det er fullt mulig å starte enkelt og utvide og tilpasse underveis. Nettverkdesign bør tenkes godt igjennom før man begynner noen fullskala utrulling og integrering, siden det er vanskeligere å endre på i etterkant enn styreregler.

For å også konkretisere norske forhold er det også laget eksempel på hvordan slike regler kan lages/utvikles og deploys på toppen - for å imøtekomme norske forhold og anbefalinger (som eks. NSM sine grunnprinsipper).

Tilpasning for kommunal sektor

Vurder følgende tilpasninger for kommunal sektor:

- Separat Azure AD tenant for forvaltning (“forvaltningsenhet/forvaltningsorgan”)
- Begrens tilgang til forvaltningsenhet/forvaltningsorgan (PIM og conditional access for brukere)
- Etabler styring og forvaltningsgruppe for skyplattform for å understøtte behov i kommune (cloud center of excellence)
 - Husk: Skyplattformen er levende og skal forvaltes, dokumenteres og videreutvikles og tilbys til andre enheter.
 - Levende dokumentasjon av plattform (wiki eller lignende)
 - Vurder DevOps-implementering for plattform (Infrastruktur og policies as code).
- Benytt og deploy Enterprise Scale i Azure AD Tenant til forvaltningsenhet som utgangspunkt.
- Opprett delte Azure tjenester, Active Directory, nettverk i Azure Subscription(s) tilknyttet forvaltningsenhet som kan benyttes av andre kommunale enheter
- Separat Azure AD tenant - for hver kommunal enhet (e.g. Skole/Barnehage/mm) som krever det (e.g. av innsyn), har eksisterende SaaS tjenester (e.g M365/Teams/mm), egne administrative grenser, lisensavtaler med partnere/Microsoft direkte mm.
- For kommunale enheter som har behov for egne Azure tjenester, har eksisterende lisensieringsavtaler eller Azure tjenester, vurder hvordan disse integreres med sentralt forvaltningsorgan.
 - Må fakturering skje direkte mellom leverandør og kommunal enhet (eller kan dette flyttes til forvaltningsenhet - sammen med tjenester?)
 - Skal tjenestene integreres med sentrale tjenester fra forvaltningsorgan (eks. Vnet peering / IAM)
 - Skal tjenestene inn under sentral forvaltning? Forvaltes gjennom Azure Lighthouse fra Azure AD til forvaltningsenhet
- Etablere IAM og B2B for forvaltning av kommunale enheter med separate Azure AD Tenants (hvor det er behov for høyere tilgangsnivå, eks. Global Admin/Lisens administratorer mm.). Implementer PIM for disse rollene.
- Etablere B2B trust mellom tenants innad i kommune hvor informasjon skal deles
- Tilknytting av tjenester mellom forvaltningsenhet og fylkeskommune

Eksempel på avtaleforhold, tenants og forvaltningsenhet/organ i kommunal sektor - merk avtaleforhold til Microsoft/Cloud provider kan være flere og bør kartlegges/gås opp.

Noen prinsipper lagt til grunn: - Enheter innad i en kommune må kunne dele tjenester - Enkel oppkobling av utstyr til delte tjenester (nettverk - Site-to-site, Point-to-site) - Sentral forvaltning og enkelt kunne legge opp nye tjenester til ansatte og innbyggere - Mulighet for å slå sammen eller splitte opp kommuner. - Skoler/Barnehager/andre kommunale enheter - har allerede eksisterende Azure AD tenants / eller må være splittet ut i separat tenant (av lisensiering/lovmessige eller sikkerhetsmessige grunner) - Standardisering og modernisering av plattform - Mulighet for å samarbeide og dele tjenester med kommuner/fylkeskommune og raskere komme opp med nye tjenestetilbud til innbyggere på tvers.

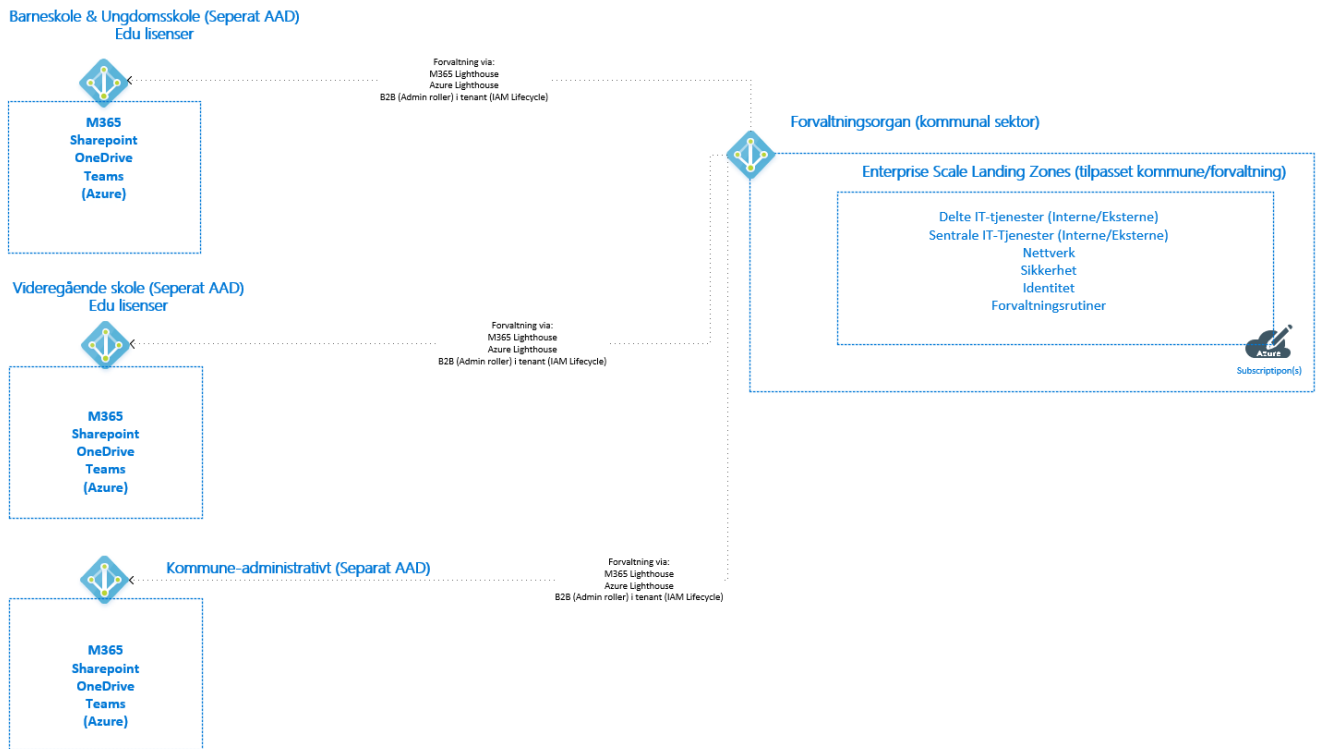


Figure 15: Referanse-arkitektur-kommunal

Forhåndskrav:

- 1 Azure AD tenant (forvaltningsenhet)
- 1 Azure AD tenant eller fler (for kommune/enheter innad i kommune)
- 1 eller flere Azure abonnementer
 - Ett enkelt kan benyttes, men anbefales kun for test & proof-of-concepts. Se [Use a single subscription](#) for mer info. For produksjons-opplett anbefales minimum 4: Connectivity, Identity, Management og Landing Zone.
- Rettigheter
 - Global Administrator i Azure AD
 - Owner på Root Management Group (/)

Azure landingssone aksellerator



Trykk på knappen over og autentiser deg mot Azure-miljøet du ønsker å provisjonere ressurser til.

Velg region for utrulling, typisk “Norway East” for norske kunder:

Gå til fanen “*Azure core setup*” og angi et prefix (maks 10 tegn) som vil benyttes på Azure Policy og andre ressurser som provisjoneres av malverket:

Gå til fanen “*Azure Platform management, security, and governance*”.

Angi om du ønsker å aktivere overvåking:

Angi hvilket abonnement som skal benyttes for felles administrasjons-ressurser (“*Management*”) og hak av for de løsningene du ønsker å aktivere:

Tilsvarende for sikkerhets-løsninger i Microsoft Defender for Cloud:

NB: Dette er tjenester som potensielt kan medføre betydelige kostnader, spesielt om de aktiveres i eksisterende miljø.

Angi en eller flere e-post adresser i feltet “*Microsoft Defender for Cloud Email Contact*”:

Azure landing zone accelerator

Deploy from a custom template

Deployment location **Azure core setup** Platform management, security, and governance Platform DevOps and automation Network topology and connectivity Identity

Template

Customized template [↗](#)
76 resources

Edit template Edit parameters

Project details

Deploying templates at the directory (tenant) scope enables scenarios like applying policies and assigning roles across the Azure Active Directory tenant you are currently logged into. You can change the deployment scope by updating the schema in the deployment template.

Directory *

.onmicrosoft.com

Switching directories will result in the Azure portal being reloaded. Any progress will be lost.

Instance details

Region * ⓘ

Norway East

Figure 16: Landingsone aksellerator

Azure landing zone accelerator

Deploy from a custom template

Deployment location **Azure core setup** Platform management, security, and governance Platform DevOps and automation

Azure Landing Zones ARM deployment requires access at the tenant root (/) scope. Visit this link to ensure you have the appropriate RBAC permission to complete the deployment

Azure Landing Zones will create the management group hierarchy under the Tenant Root Group with the prefix provided at this step.
[Learn more](#)

Management Group prefix * ⓘ

akom

Select dedicated subscriptions or single subscription for platform resources ⓘ

☒ Dedicated (recommended)

☐ Single

Figure 17: Landingsone aksellerator

i To enable platform management, security and governance, you must allocate a management Subscription. Please note, this Subscription will be moved to the platform Management Group, and ARM will deploy a Log Analytics workspace and requisite settings. We recommend using a new Subscription with no existing resources. Note that Azure Policy will be used to govern the configuration for the platform at scale.

Deploy Log Analytics workspace and enable monitoring for your platform and resources **i**

☒ Yes (recommended) ☐ No

Log Analytics Data Retention (days) **i** 30 Days

Figure 18: Landingssone aksellerator

Subscription * **i**

Select which Azure Monitor solutions you will enable for your Log Analytics workspace
[Learn more](#)

Deploy Agent Health solution **i** ☒ Yes (recommended) ☐ No

Deploy Change Tracking solution **i** ☒ Yes (recommended) ☐ No

Deploy Update Management solution **i** ☒ Yes (recommended) ☐ No

Deploy Activity Log solution **i** ☒ Yes (recommended) ☐ No

Deploy VM Insights solution **i** ☒ Yes (recommended) ☐ No

Deploy Service Map solution **i** ☒ Yes (recommended) ☐ No

Figure 19: Landingssone aksellerator

Enable Microsoft Defender for Cloud for AppServices ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Enable Microsoft Defender for Cloud for Storage ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Enable Microsoft Defender for Cloud for Azure SQL Database ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Enable Microsoft Defender for Cloud for SQL servers on machines ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Enable Microsoft Defender for Cloud for Key Vault ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Enable Microsoft Defender for Cloud for Azure Resource Manager ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Enable Microsoft Defender for Cloud for DNS ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Enable Microsoft Defender for Cloud for Containers (Kubernetes and Container Registries) ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Deploy Microsoft Sentinel ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No

Figure 20: Landingssone aksellerator

Select which Microsoft Defender for Cloud solutions you will enable.

[Learn more](#)

Deploy Microsoft Defender for Cloud and enable security monitoring for your platform and resources ⓘ

☒ Yes (recommended)
☐ No

Microsoft Defender for Cloud Email Contact * ⓘ

Enable Microsoft Defender for Cloud for servers ⓘ

☒ Yes (recommended)
☐ No


Enable Microsoft Defender for Cloud for open-source relational databases ⓘ

☒ Yes (recommended)
☐ No

Figure 21: Landingssone aksellerator

Utrulling av kontinuerlig integrasjons- og utrullings pipelines er valgfritt og kommer an på organisasjonens strategi og modenhet rundt infrastruktur som kode:

Deployment location Azure core setup Platform management, security, and governance Platform DevOps and automation

i Azure Landing Zones provides an integrated CI/CD pipeline via AzOps that can be used with either GitHub Actions or Azure DevOps pipelines. 

Deploy integrated CI/CD pipeline? *

☐ Yes (recommended)
☒ No

Figure 22: Landingssone aksellerator

Gå til fanen “*Network topology and connectivity.*” I referanse-utrulling for kommune-sektoren velges “*Virtual WAN (Microsoft managed)*” som nettverkstopologi:

I valgene som blir tilgjengelig etter å ha valgt “*Virtual WAN (Microsoft managed)*” i forrige steg gjøres følgende tilpasninger: - **Subscription:** Velg abonnementet som skal være dedikert for nettverks-ressurser. - **Address space:** Angi CIDR som vil benyttes i hub (brukes primært for sentral routing) - **Region for the first networking hub:** Norway East - **Deploy VPN Gateway:** Yes (alternativt ExpressRoute Gateway dersom dette er satt opp, men for initielle oppsett og test-miljøer er VPN Gateway tilstrekkelig). - **Enable Azure Firewall as a DNS Proxy:** Yes (muliggjør videresendte navneoppslag fra interne DNS servere for private endepunkter i Azure)

i To enable network topology and connectivity, you must allocate a dedicated connectivity Subscription. Please note, this Subscription will be moved to the connectivity Management Group, and ARM will deploy the first hub virtual network for either a hub and spoke or Virtual WAN network topology. Additional networking platform resources such as gateways or Azure Firewall can be deployed. We recommend using a new dedicated Subscription with no existing resources.

- Deploy networking topology ⓘ
- ☐ Hub and spoke with Azure Firewall
 - ☐ Hub and spoke with your own third-party NVA
 - ☒ Virtual WAN (Microsoft managed)
 - ☐ No

Figure 23: Landingssone aksellerator

Subscription * ⓘ	<input type="text" value=""/>
Address space (required for vWAN hub) * ⓘ	<input type="text" value="10.100.0.0/23"/>
Region for the first networking hub * ⓘ	<input type="text" value="Norway East"/>
Enable DDoS Protection Standard ⓘ	<input type="radio"/> Yes (recommended) <input checked="" type="radio"/> No
Deploy VPN Gateway ⓘ	<input checked="" type="radio"/> Yes <input type="radio"/> No
Select the VPN Gateway scale unit ⓘ	<input type="text" value="2 scale units"/>
Deploy ExpressRoute Gateway ⓘ	<input type="radio"/> Yes <input checked="" type="radio"/> No
Deploy Azure Firewall ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> No
Enable Azure Firewall as a DNS proxy ⓘ	<input checked="" type="radio"/> Yes <input type="radio"/> No
Select Azure Firewall tier ⓘ	<input type="text" value="Standard"/>

Gå til fanen “*Identity*” og velg abonnementet som skal være dedikert for identitets-ressurser:

La alle anbefalte innstillinger stå:

Trykk “*Next: Landing Zone configuration*”.

Velg abonnementer som skal være dedikert for hybride og online landingssoner:

La anbefalte innstillinger være aktivert ift hvilke policyer som blir aktivert for de valgte landingssone abonnemementene:


Trykk *Review and create* etterfulgt av *Create* for å starte provisjoneringen.

Azure landing zone accelerator ...

Deploy from a custom template

Assign recommended policies to govern identity and domain controllers ⓘ ☒ Yes (recommended) ☐ No

Identity subscription

 Ensure you select a subscription that is dedicated for Identity. Selecting the same Subscription here for Management or Connectivity will result in a deployment failure. If you want to use a single Subscription for all platform resources, select 'Single' on the 'Azure Core Setup' blade.

Subscription * ⓘ

Figure 24: Landingssone aksellerator

Select which of the the recommended policies you will assign to your identity management group.

[Learn more](#)

Prevent inbound RDP from internet ⓘ ☒ Yes (recommended) ☐ No

Ensure subnets are associated with NSG ⓘ ☒ Yes (recommended) ☐ No

Prevent usage of public IP ⓘ ☒ Yes (recommended) ☐ No

Ensure Azure VMs (Windows & Linux) are enabled for Azure Backup ⓘ ☒ Yes (recommended) ☐ No

Figure 25: Landingssone aksellerator

Select the subscriptions you want to move to corp management group.
[Learn more](#)

Corp landing zone subscriptions (optional)

0 selected

▼

Select the subscriptions you want to move to online management group.
[Learn more](#)

Online landing zone subscriptions (optional)

0 selected

▼

Select which of the the recommended policies you will assign to your landing zones.
[Learn more](#)

Enable DDoS Protection Standard ⓘ

☒ Yes (recommended)
☐ Audit only
☐ No

Prevent usage of Public Endpoints for Azure PaaS services in the corp connected landing zones ⓘ

☒ Yes (recommended)
☐ Audit only
☐ No

Ensure encryption in transit is enabled for PaaS services ⓘ

☒ Yes (recommended)
☐ Audit only
☐ No

Figure 26: Landingssone aksellerator

Ensure Azure VMs (Windows & Linux) and Azure Arc-enabled servers are being monitored ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Ensure Azure VMSS (Windows & Linux) are being monitored ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Enable Kubernetes (AKS) for Azure Policy ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Prevent privileged containers in Kubernetes clusters ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Prevent privileged escalation in Kubernetes clusters ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Ensure HTTPS ingress is enforced in Kubernetes clusters ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No

Figure 27: Landingssone aksellerator

Ensure Azure VMs (Windows & Linux) are enabled for Azure Backup ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Prevent inbound RDP from internet ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Ensure subnets are associated with NSG ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Prevent IP forwarding ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Ensure Azure SQL is enabled with transparent data encryption ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Ensure auditing is enabled on Azure SQL ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No
Ensure secure connections (HTTPS) to storage accounts ⓘ	<input checked="" type="radio"/> Yes (recommended) <input type="radio"/> Audit only <input type="radio"/> No

Figure 28: Landingssone aksellerator

Review + create

< Previous

Next : Review + create >

Figure 29: Landingssone aksellerator

Etablering av hybrid oppsett

Etter provisjonering av ressurser i Azure er det noe steg som må utføres i lokalt miljø for å etablere forbindelse og fullføre det hybride oppsettet:

- Etablere VPN tunnell mellom Azure Virtual WAN og lokalt nettverk. Se dokumentasjon for detaljer.
- Etablere site for nettverk i Azure i Active Directory Sites & Services
- Melde inn domenekontrollere i Azure (plassert i Identity abonnementet) og promotere disse til domenekontrollere
- Konfigurere Azure Firewall regler for kommunikasjon mellom Azure nettverk og lokale nettverk

Compliance - Policy initiative for NSM sine grunnprinsipper

Som et eksempel - viser vi her hvordan man kan gjøre en mapping av NSM sine grunnprinsipper, basert på ISO standarden og Azure policies og deploye dette for å få laget en tilpasset compliance rapport for Norske forhold. Man kan se for seg at det videreutvikles flere policies og kontrollmekanismer basert på community dersom dette er nyttig. Gjennom Azure Arc kan man også gjøre policy og compliance rapportering på eksisterende infrastruktur.

Eksempel på hvordan NSM sine grunnprinsipper kan mappes og deployes er foreløpig dokumentert [her](#). Dokumentasjon og mal vil bli overført til dette dokumentet.

Vedlegg og støttedokumentasjon

Azure i Norge

- [2 datasentere i Norge](#)
- [Datalagring i Azure](#)
- [Availability Zones in Norway](#)
- [Mission Critical workloads in Norway](#)

Rapporter, audit, innsyn

[Klareringssenter](#) inneholder hundrevis av rapporter, innsyn og tredjepart audits for Microsoft sine tjenester i sky. Her kan du finne alt fra linker rundt overholdelse av regler og standarder, personvern, datainnsyn mm.

Alternativt kan du også gå inn her for å finne rapporter direkte: <https://servicetrust.microsoft.com/>

Schrems-II

- [EU Data Boundry](#)
- [EU Data Boundry - FAQ](#)

GDPR

Som kunde opprettholder du eierskap til kundedata – innhold, personlige kundedata og andre data du leverer til lagring og drifting i Azure-tjenestene. Du har også kontroll over eventuelle andre geografiske områder der du bestemmer deg for å rulle ut løsningene eller replikere dataene dine.

Der en tjenestes funksjonalitet krever global datareplikering, er detaljene tilgjengelige [her](#).

Linker

- [Protecting privacy in Microsoft Azure](#)
- [Microsoft EU Data Boundary](#)
- [Trusted Cloud](#)
- [Datalagring i Azure](#)
- Microsoft Azure SOC Rapporter
- Online Services Terms for Microsoft Azure

Verktøy

- Azure Advisor
- Microsoft Defender for Cloud
- Azure Policy
- [Azure Optimization Engine](#)

Dokumentversjon og endringslogg

Versjon	Dato	Endringer
0.5	Oslo, 31 mai 2022	Første utkast