DEVICE & IDENTITY *Management*

# DEVICE & IDENTITY MANAGEMENT

## FRIGØR MEDARBEJDERE OG HOLD DATA SIKRE PÅ **TVÆRS AF ENHEDER**

Moderne it-brugere forventer at kunne arbejde alle steder fra og via flere typer enheder. Samtidig forventer dataejerne *(i sidste ende virksomhedens ledelse)* at adgang til data sikres behørigt. Microsoft stiller, som en del af den hybride arbejdsplads, cloudbaserede teknologier til rådighed, der kan understøtte begge behov.

At udnytte den teknologi kræver specialviden, som typisk ikke er værdiskabende at etablere og opretholde internt i virksomheden. Device & Identity Management *(DIM)* er en service, der giver adgang til knowhow, best practices og værktøjer, som gør teknologien til en brugbar løsning, der er praktisk anvendelig i virksomheden.

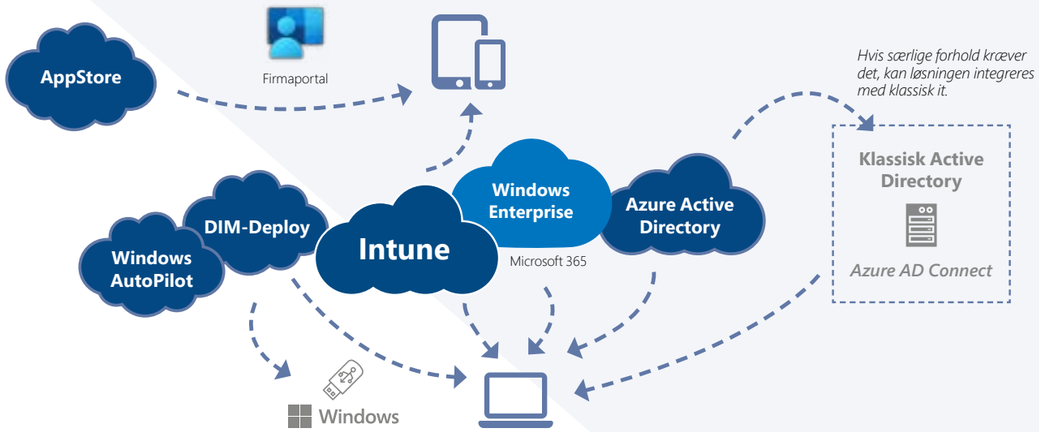
Med DIM opnås kontrol med virksomhedens enheder *(pc, mac, smartphones og tablets)*. Enheder kan automatisk installeres med nyeste Windows, Office, antivirus software samt øvrige forretningssystemer, og kan løbende holdes opdateret. De kan desuden nemt nulstilles og gøres klar til brug igen. Smartphones og tablets kan automatisk få installeret udvalgte apps og der kan etableres politikker, der fx kræver beskyttelse med pinkode.

Værktøjer til styring af betinget adgang og multifaktorgodkendelse samt medarbejderes mulighed for selv at nulstille deres adgangskode kan også være omfattet.

## EN PRAKTISK BRUGBAR LØSNING

**– der følger best practice**

Med Device & Identity Management samles moderne teknologier og værktøjer til en praktisk brugbar løsning, der kan styre både pc'ere, mac's, smartphones og tablets – og vi opdaterer løsningen løbende, så den følger best practice.





## KONTROL OVER ENHEDER

**- er afgørende for sikker adgang til data i skyen**

Med Microsoft 365 følger mange muligheder fx automatisk udrulning og vedligehold af enheder, selvbetjent nulstilling af adgangskode og styring af mobile enheder.

Det vil sige at alle enheder, der kan få adgang til virksomhedens vigtige data, kan komme under kontrol.

## EN ADGANGSKODE ER IKKE NOK

**– uanset hvor kompleks den er**

Det er overraskende let for it-kriminelle at lokke adgangskoder ud af dine medarbejdere. Mailadresser findes nemt fx på hjemmesiden og phishing-mails laves professionelt og meget troværdige. Dine brugeres adfærd på usikre wi-fi netværk udgør også et nemt mål, fordi gemte koder kan aflures *(medmindre du har aktiveret Credential Guard)*. Alt i alt kan en adgangskode, ikke længere betragtes som sikker nok, i sig selv.

## BESKYT VED HOVEDDØREN

**Giv kun betinget adgang til data**

Med reglerne for betinget adgang kan du sikre at flere betingelser skal være opfyldt *(foruden kendskab til korrekt brugernavn og adgangskode)* for at få adgang til virksomhedens vigtige data. Det er nødvendigt for at kunne løfte sikkerheden til et passende niveau.


**Risikobaseret betinget adgang**

Det er muligt at lade en automatiseret risikovurdering indgå i forløbet.
Ved hjælp af kunstig intelligens vurderes forhold som fx:

| | |
|---|---|
| Lækkede adgangskoder | Login fra anonyme ip-adresser |
| Login fra måske inficerede enheder | Informationer fra Windows Defender ATP* |
| Umulig eller atypisk rejseaktivitet | Login fra ip-adresser med mistænkelig aktivitet |

**forudsætter Azure Active Directory Premium P2, der fx er med i Microsoft 365 E5 eller E3 med E5 security udvidelsen.*

## DET FÅR DU MED **DEVICE & IDENTITY MANAGEMENT**

**DIM** - *Basic*

- **WINDOWS & APPLICATION DEPLOY MANAGEMENT**
  *Automatik til installation af Windows 10/11 og apps på pc/mac og smartphone/tablet samt automatik til opdatering af Windows 10/11 og antivirus*
- **POLICY MANAGEMENT**
  *Konfiguration af sikkerhedspolitikker m.m.*
- **DISK ENCRYPTION MANAGEMENT**
  *Konfiguration af diskkryptering (BitLocker)*
- **BEST PRACTICE MANAGEMENT**
  *Løbende best practice tilpasning af løsningerne*

**DIM** - *Pro*

- **CONDITIONAL ACCESS MANAGEMENT**
  *Konfiguration af betinget adgang og multifaktorgodkendelse samt udvidet identitetsbeskyttelse*
- **SELF-SERVICE PASSWORD RESET MANAGEMENT**
  *Opsætning af selvbetjent nulstilling af adgangskode (og hjælp til selvhjælp)*
- **ASSET MANAGEMENT**
  *Adgang til Asset Management rapporter via Power BI*
- **CONFIGURATION BACKUP MANAGEMENT**
  *Backup af Intune opsætning (forudsætter GTM Pro)*

### Andre har suppleret med:

Sikker håndtering af dine enheder og identiteter er blot en del af en større sammenhæng. Derfor er Device & Identity Management-løsningen også en del af den større samlede løsning, Modern Management Suite. Desuden ser vi ofte danske virksomheder kombinere løsningen med:

*Aktuelt for mig*

**Heimdal Security**
***- Proaktiv beskyttelse mod trusler som antivirus ikke fanger***
Automatiseret patching af sikkerhedskritiske tredje-parts software samt monitorering og blokering af ondsindet datakommunikation i realtid.

**Cloudprint - Styring af lokale printere via cloud**
Print som du plejer, men slip for manuel vedligeholdelse, installation og løbende opdatering af printerdrivere på alle dine enheder samt fejlprint, der aldrig bliver hentet. Du vil kunne printe som du altid har kunnet, men ved at udnytte teknologien i løsningen opnår du højere sikkerhed og mere fleksibilitet.