# Styrk din IT-sikkerhed i praksis

MB Solutions

# Hvem er jeg?

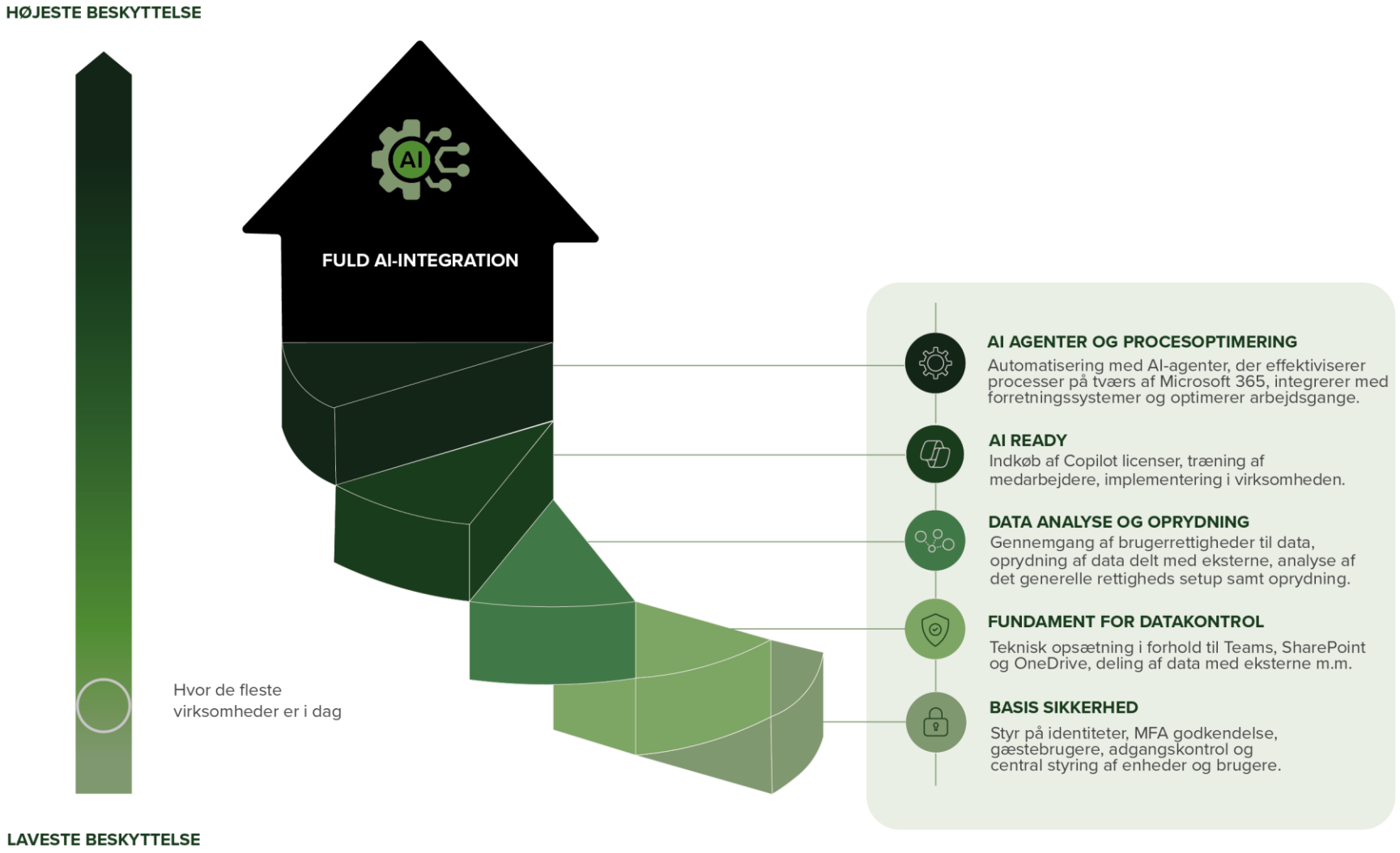
**Jacob Dahlgaard**
**Security Team Lead**

- 8 År i MB-Solutions
- Ansvarlig for MB-Solutions IT-sikkerhedsaktiviteter
- Arbejder med løbende udvikling og drift af IT-sikkerhed hos danske virksomheder
- Fokus på at få sikkerhed til at fungere i praksis – ikke kun på papiret

# Dagsorden

- Forebyggelse & beredskab
- MBS' tilgang til IT-sikkerhed
- Struktur med IT-sikkerhedsårshjul
- Fra anbefaling til implementering
- Prioritering – størst effekt først
- De 5 klassiske sikkerhedshuller
- Det aktuelle trusselsbillede (Arctic Wolf)

# AI & IT Sikkerhed




**AI AGENTER OG PROCESOPTIMERING**
Automatisering med AI-agenter, der effektiviserer processer på tværs af Microsoft 365, integrerer med forretningssystemer og optimerer arbejdsgange.

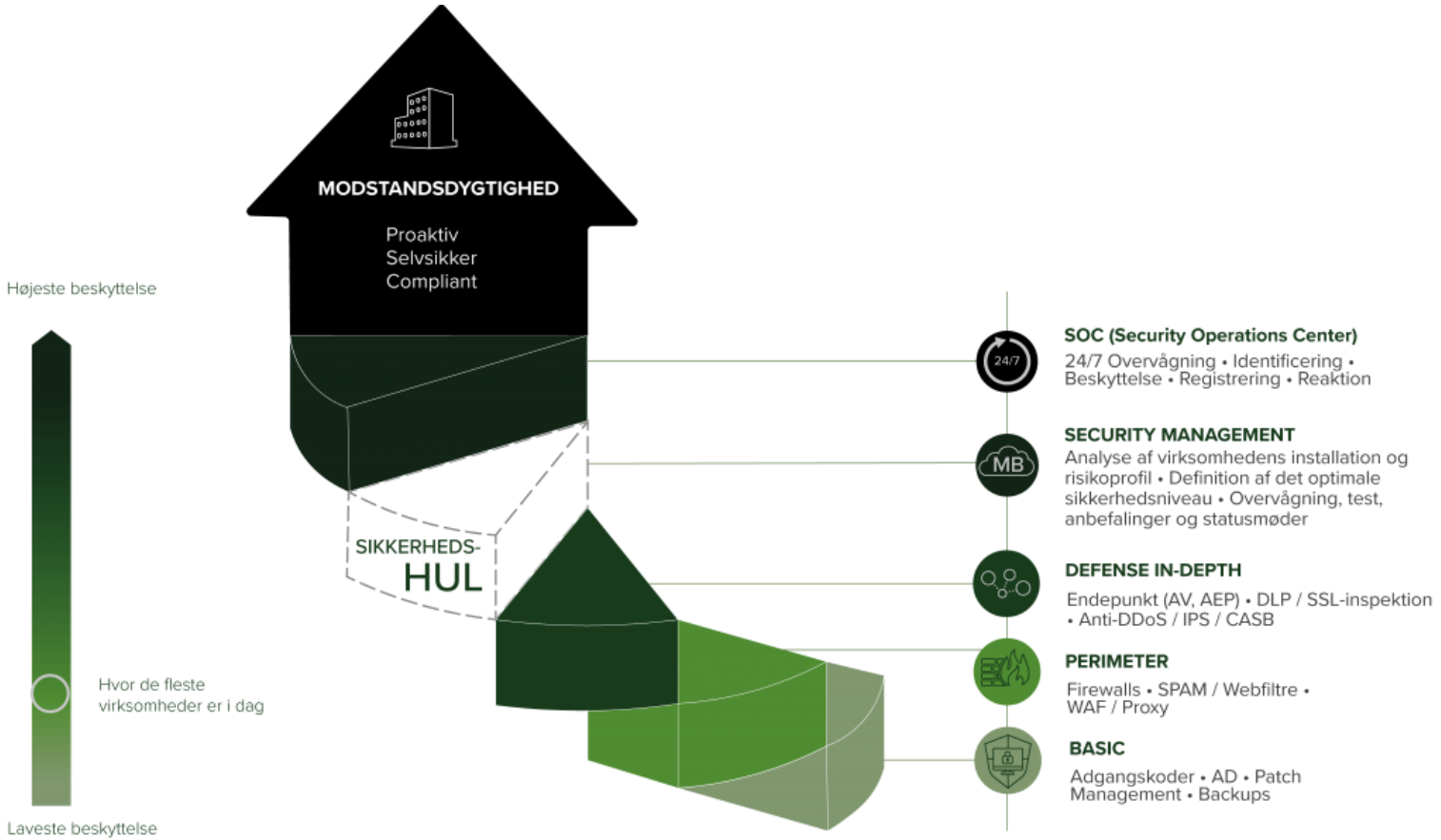
**AI READY**
Indkøb af Copilot licenser, træning af medarbejdere, implementering i virksomheden.

**DATA ANALYSE OG OPRYDNING**
Gennemgang af brugerrettigheder til data, oprydning af data delt med eksterne, analyse af det generelle rettigheds setup samt oprydning.

**FUNDAMENT FOR DATAKONTROL**
Teknisk opsætning i forhold til Teams, SharePoint og OneDrive, deling af data med eksterne m.m.

**BASIS SIKKERHED**
Styr på identiteter, MFA godkendelse, gæstebrugere, adgangskontrol og central styring af enheder og brugere.

# Forebyggelse




- Awareness træning
- Tilpasning af teknisk opsætning
- Patch & sårbarhedsstyring
- Overblik over enheder og identiteter
- IT beredskabsplan

# Beredskab

## Arctic Wolf

### SOC

+1000 Security Engineers across SOC and Incident response teams. Infused with AI capabilities to deliver outcome in the modern IT era.

- **Aurora Platform**
- **Security Teams**
- **Concierge Partner Model**
- **Arctic Wolf Labs**

## SOC as a Service

### Managed Detection and Response

24/7/365 Detection and Response.

### Incident Response

Eradication & Remediation

Forensics analysis & reporting

Negotiation with threat actors.

Recover & Restore Operations

## MB Solutions

### NEXT Generation Cloud Provider

Local pressens, tailored services and innovative solutions to meet the specific needs of each client.

- **Vulnerability assessment**
- **Compliance**
- **Managed IT Services**

# Hvordan MBS arbejder med IT-sikkerhed

1

**Vi starter med en grundig onboarding og analyse**

- Fakta før anbefalinger
- Overblik over miljøet
- Fælles udgangspunkt

2

**Sikkerhed tilpasses virksomhedens risikoprofil**

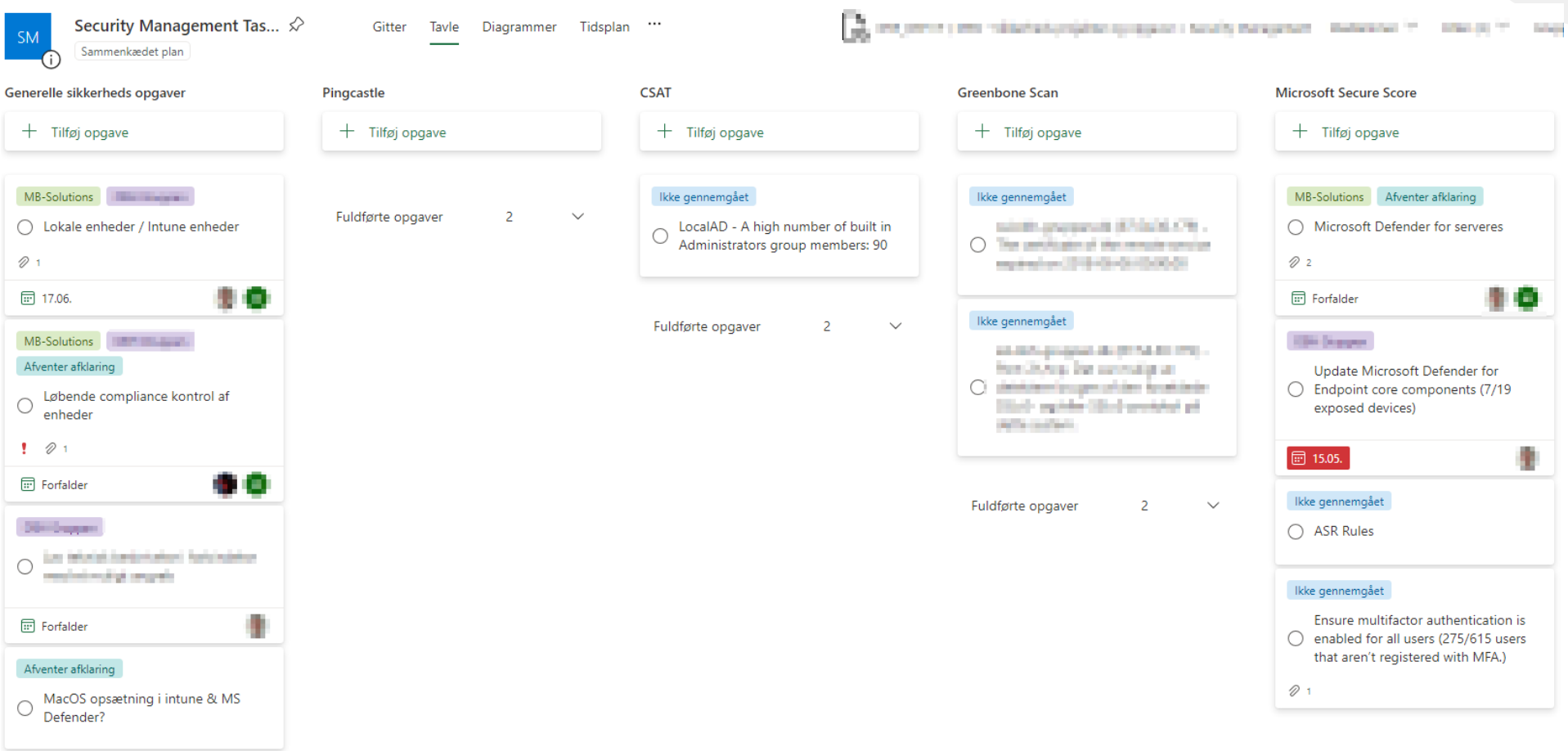
- Ikke one-size-fits-all
- Realistisk og relevant sikkerhedsniveau

3

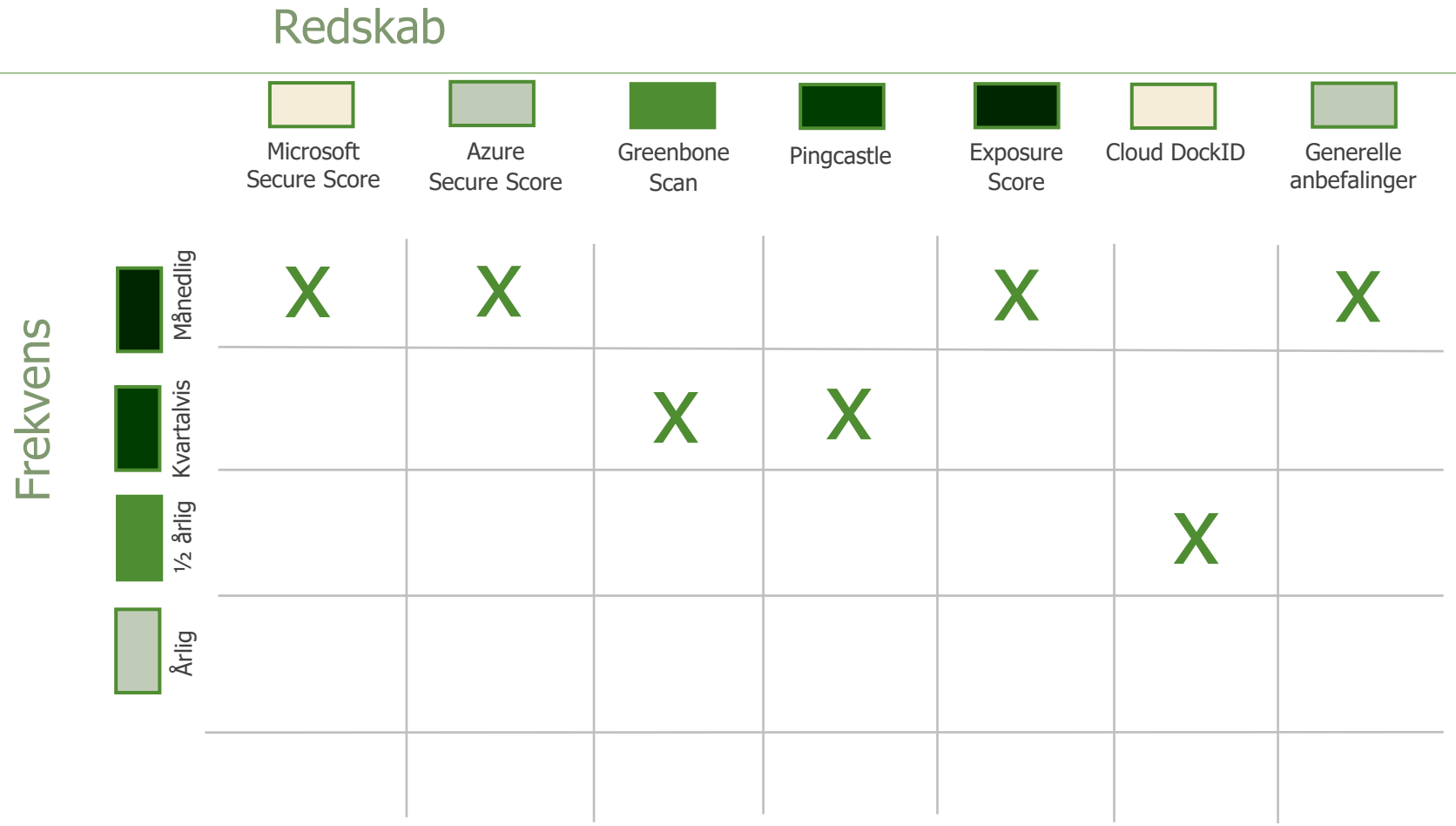
**Anbefalinger bliver omsat til konkrete handlinger**

- Ikke kun rapporter
- Prioriterede opgaver
- Aftalt plan & implementering

# Opgave håndtering

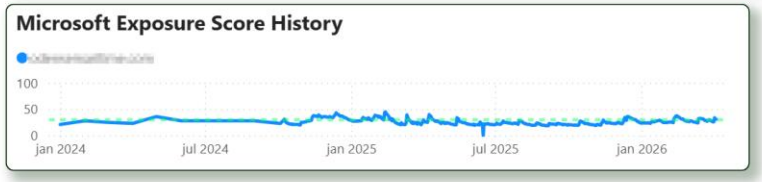


# IT-sikkerhedsårshjul

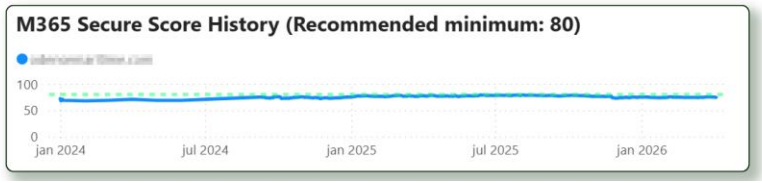


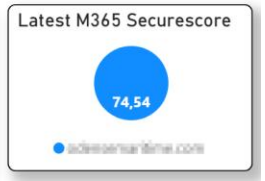
# Alt data på ét sted

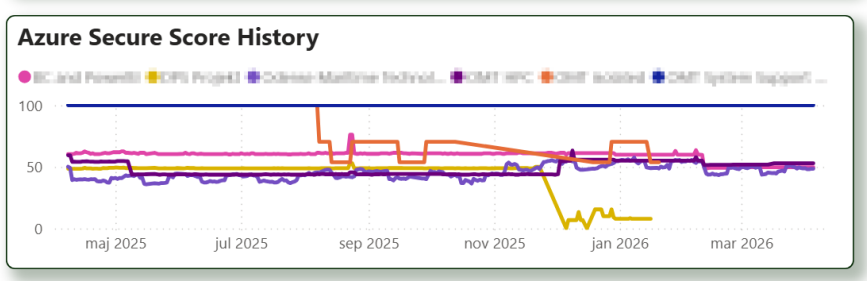


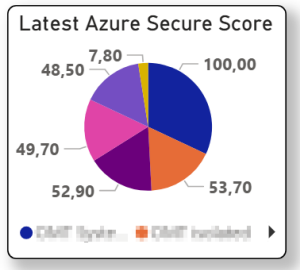


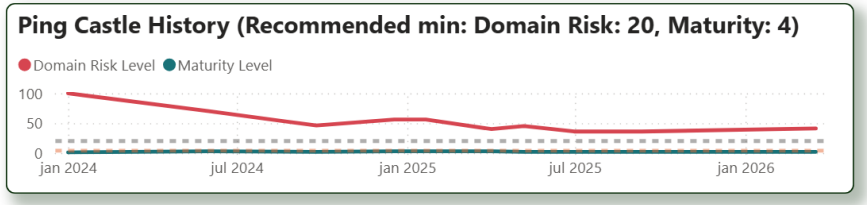


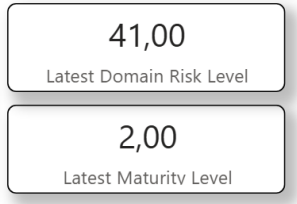


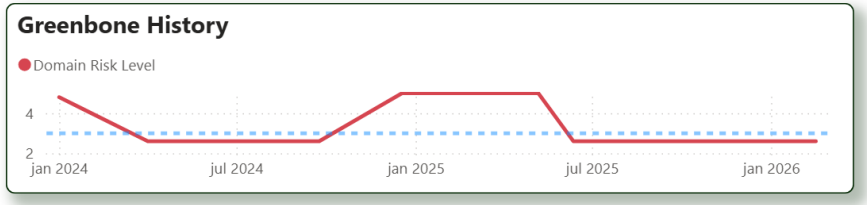



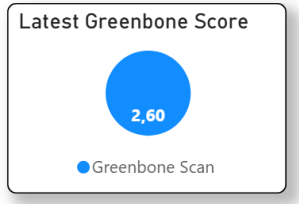



# Prioritering i IT-sikkerhed – hvad giver mest værdi først?

## Microsoft Secure Score

Overview | **Recommended actions** | History | Metrics & trends

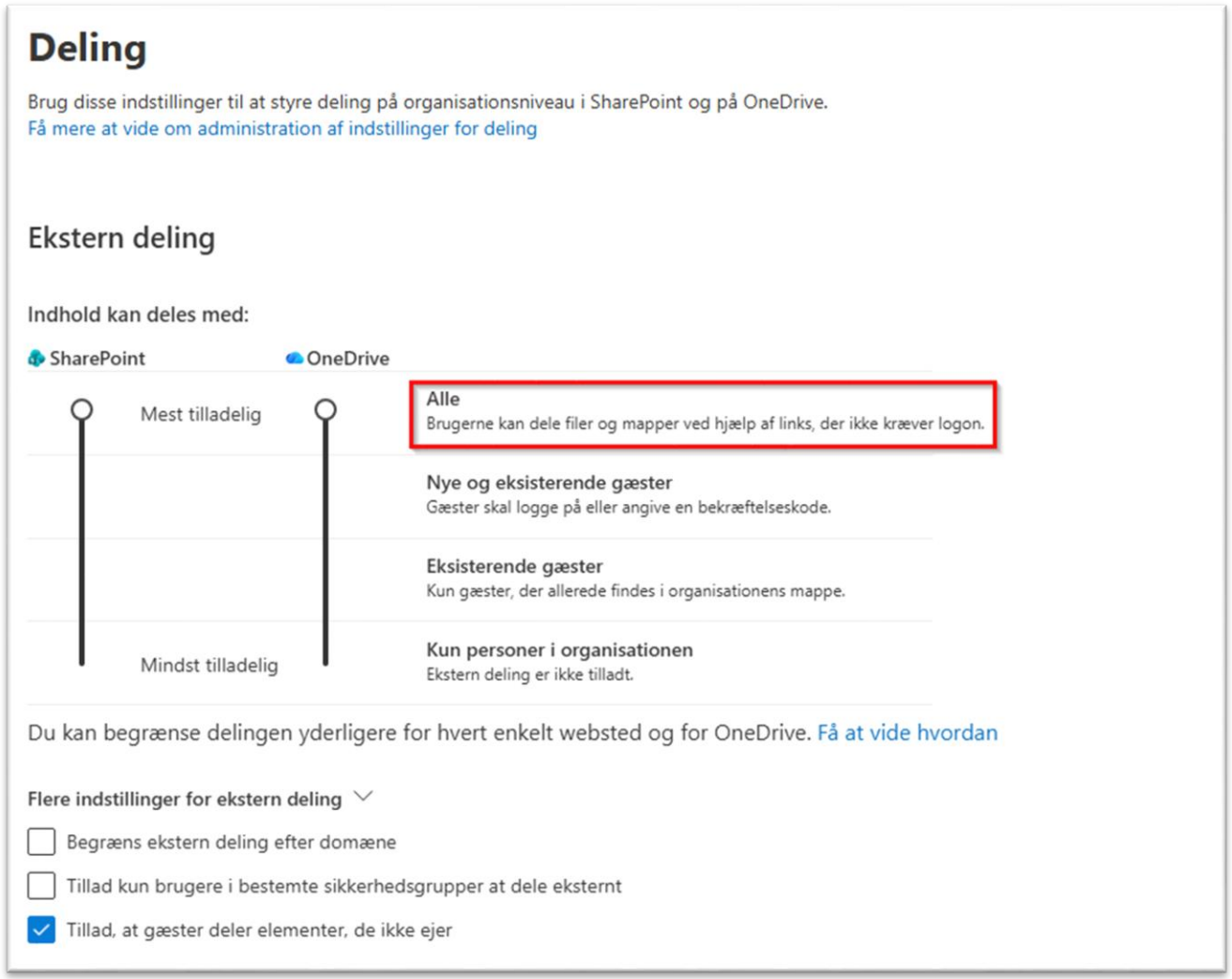
Actions you can take to improve your Microsoft Secure Score. Score updates may take up to 24 hours.

Eksportér | 198 elementer | Søg | Filtre

| Rank | Recommended action | Score i... | Points achi... | Status | Regress... |
|---|---|---|---|---|---|
| 1 | Block Office applications from creating executable content | +0.77% | 0/9 | To address | No |
| 2 | Block process creations originating from PSExec and WMI comı | +0.77% | 0/9 | To address | No |
| 3 | Block all Office applications from creating child processes | +0.77% | 0/9 | To address | No |
| 4 | Block abuse of exploited vulnerable signed drivers | +0.77% | 0/9 | To address | No |
| 5 | Block executable files from running unless they meet a prevalei | +0.77% | 0/9 | To address | No |
| 6 | Block executable content from email client and webmail | +0.77% | 0/9 | To address | No |
| 7 | Block untrusted and unsigned processes that run from USB | +0.77% | 0/9 | To address | No |
| 8 | Block persistence through WMI event subscription | +0.77% | 0/9 | To address | No |

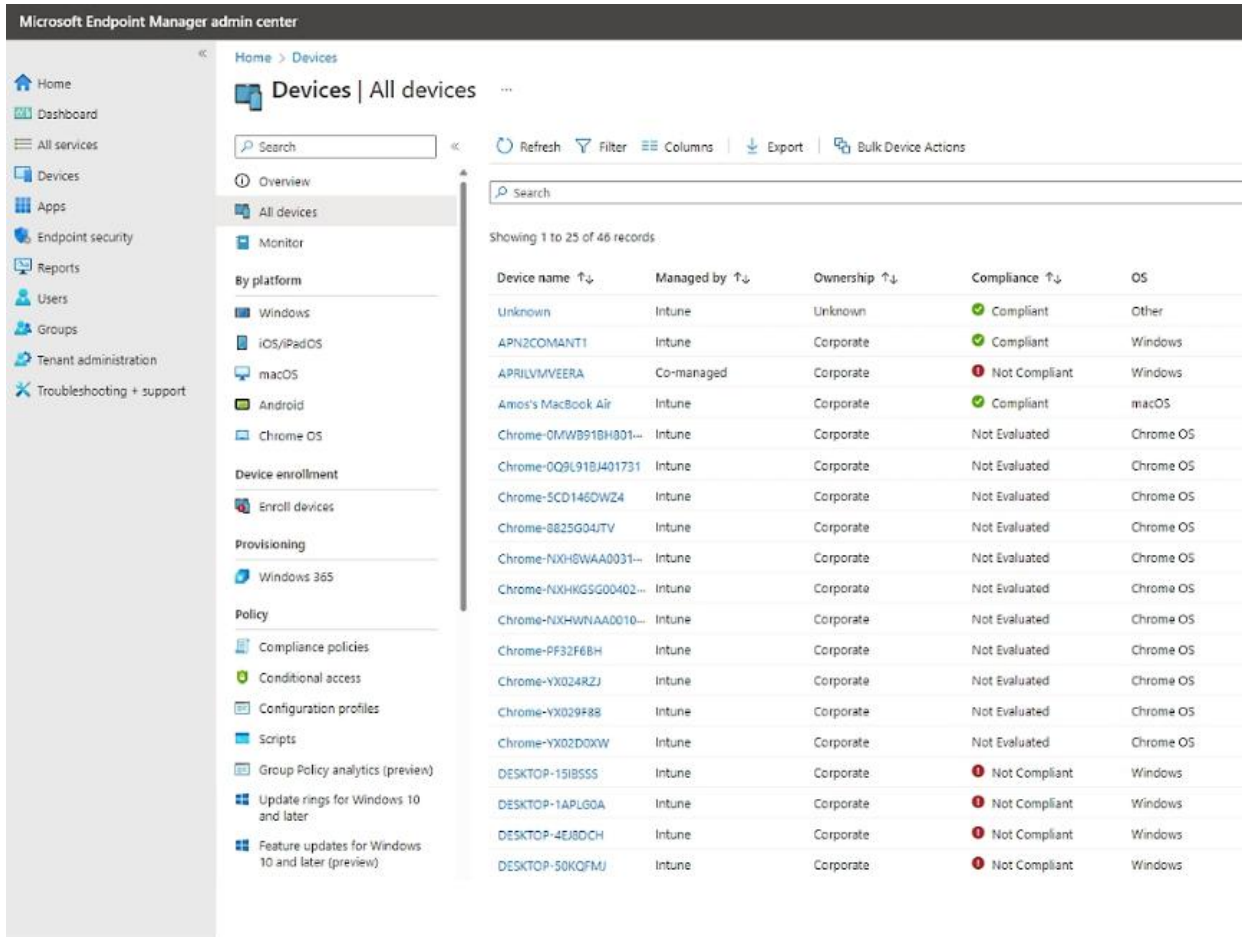
- **IT-sikkerhed prioriteres ud fra et 360-graders perspektiv**
- **Beslutninger baseres på data fra hele IT-miljøet**
- **Tekniske anbefalinger omsættes til en prioriteret handlingsliste**
- **Vi starter med få tiltag, der giver størst effekt**

# De klassiske 5 huller (OneDrive/SharePoint deling af data)

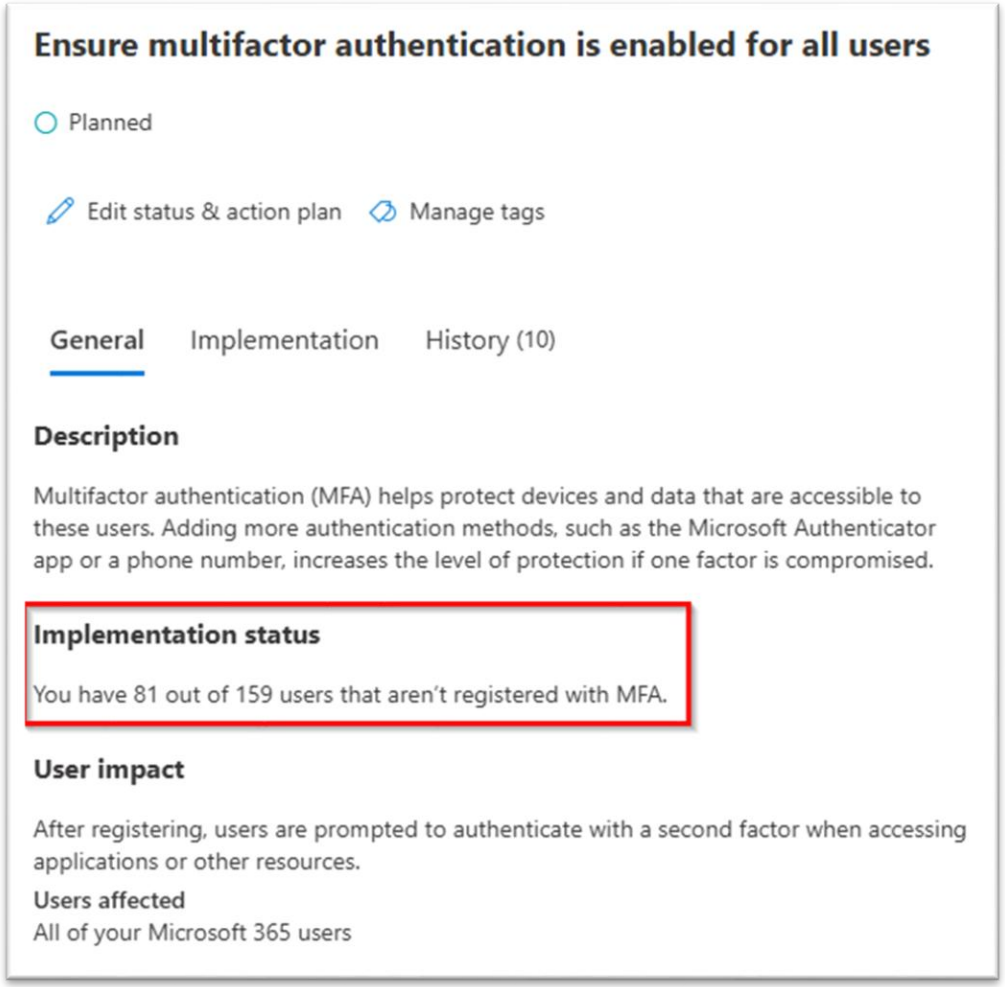



- **Deling kan ske uden krav om login eller MFA**
- **Begrænset sporbarhed**
- **Gæster kan dele videre med andre gæster**
- **Ukontrolleret adgang til kritiske data**

# De klassiske 5 huller (Unmanaged enheder)

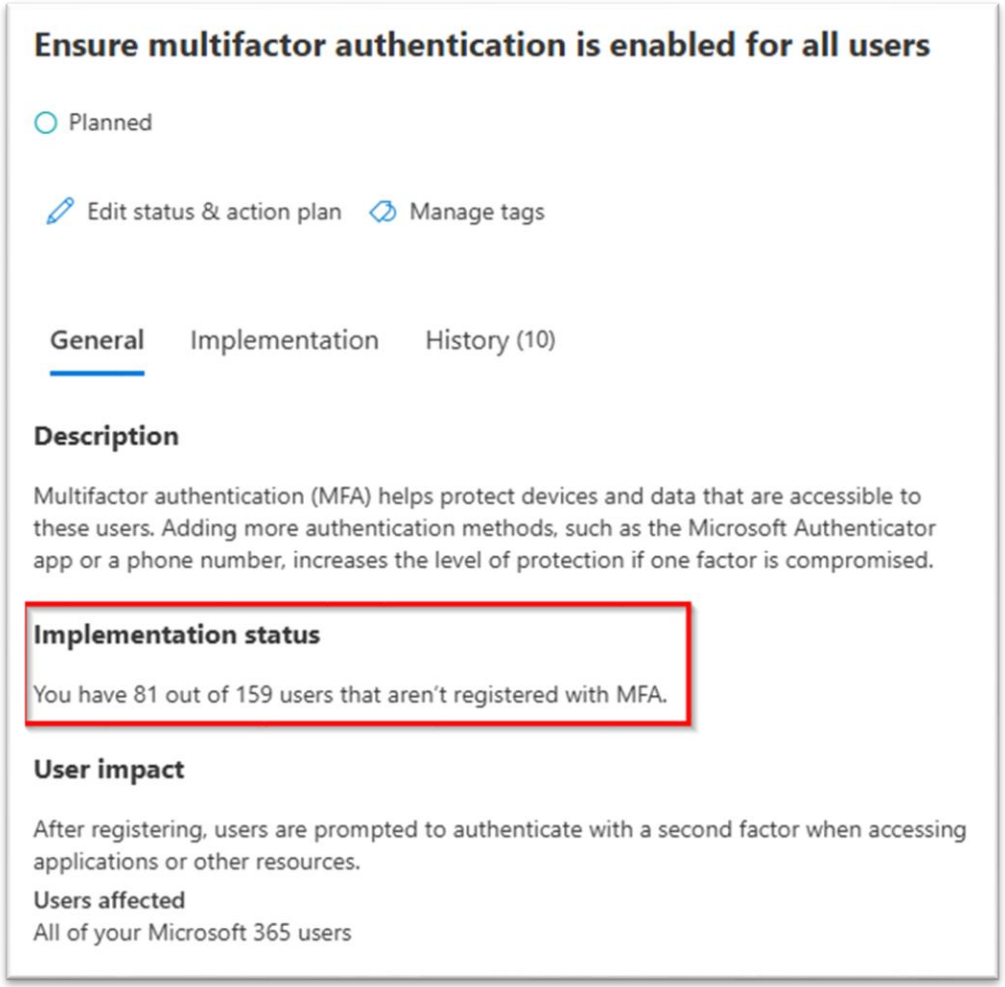


# De klassiske 5 huller (MFA)



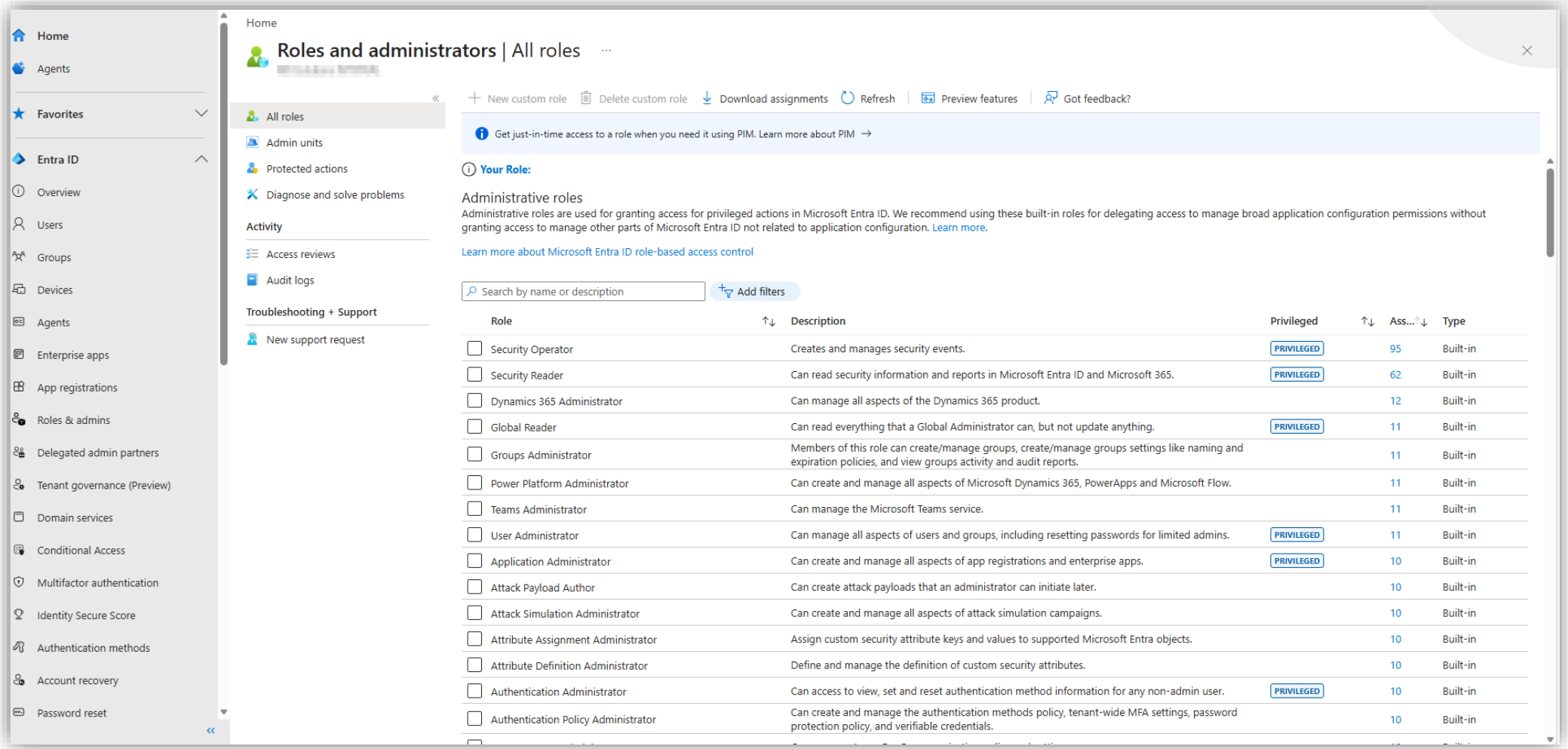

- **MFA-policy - brugere med aktiveret MFA**
- **MFA kræves ikke altid ved login (fx fra kontoret)**
- **Brugere kan eksistere uden MFA i lang tid**
- **Hacker kan selv opsætte MFA efter password-kompromittering**

# De klassiske 5 huller (MFA)

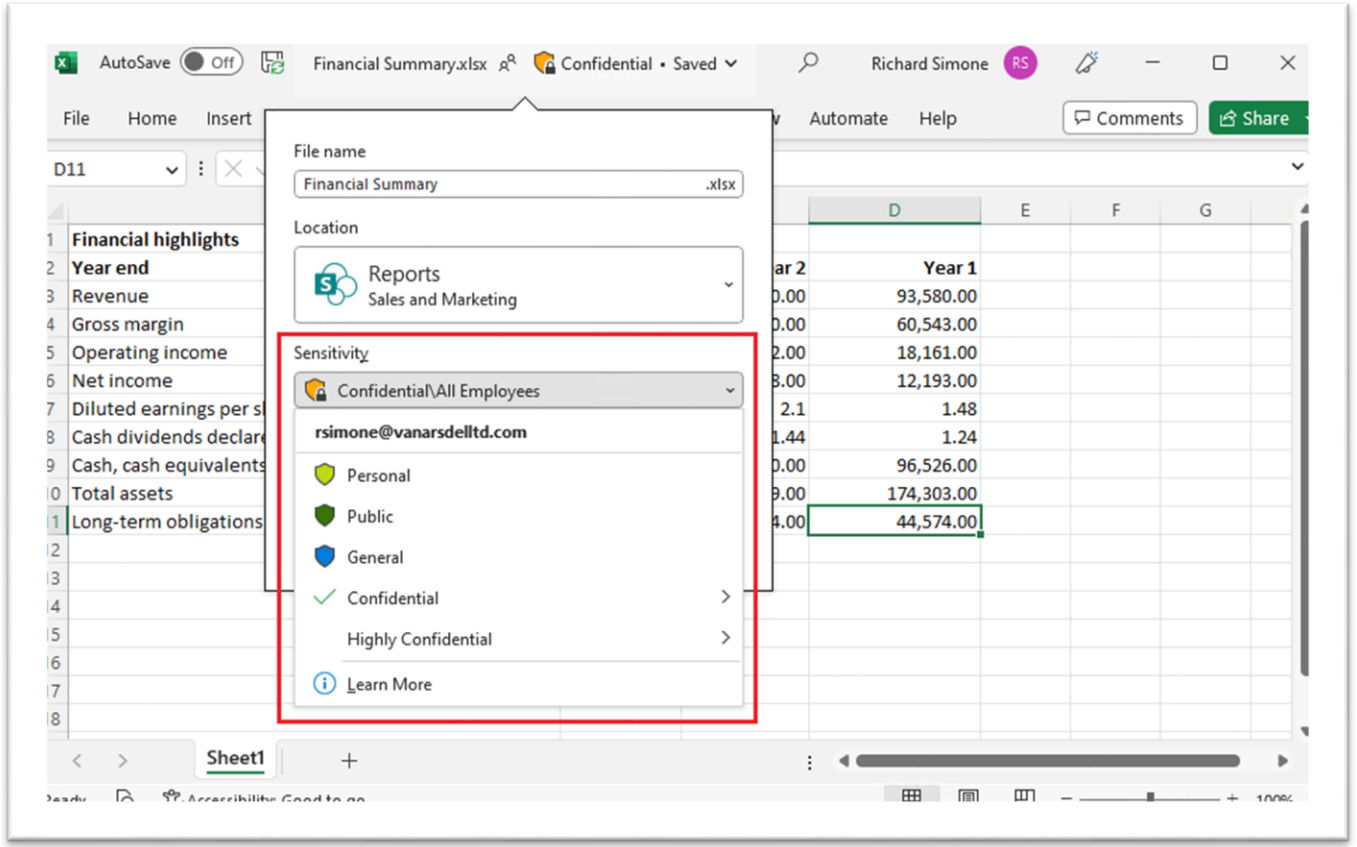



- **MFA-policy - brugere med aktiveret MFA**
- **MFA kræves ikke altid ved login (fx fra kontoret)**
- **Brugere kan eksistere uden MFA i lang tid**
- **Hacker kan selv opsætte MFA efter password-kompromittering**

# De klassiske 5 huller (Adgang til admin portaler)



# De klassiske 5 huller (Data Sikkerhed & AI)




- **AI arbejder direkte på virksomhedens data**
- **Sensitivity labels styrer hvad AI må bruge**
- **Klassificér data - Offentligt / Internt / Fortroligt**
- **Klassificering kan startes simpelt (2–3 labels)**

MB Solutions