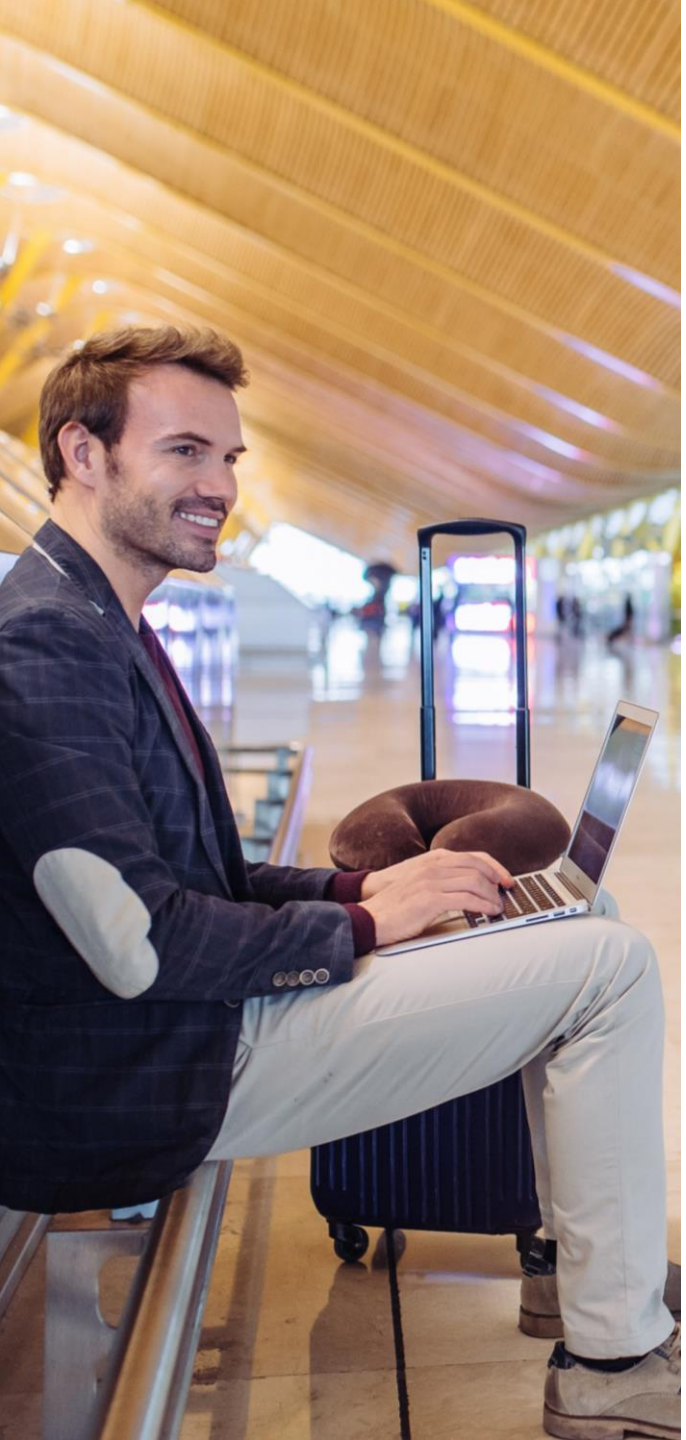
GUIDE
Microsoft Modern Management

MINDCORE



Indhold

Hvad er Modern Management?

Hvorfor investere i Modern Management?

Overvej de rigtige tiltag fra starten

Hvad nu? Hvordan kommer du videre?

MINDCORE

Hvad er Modern Management egentligt?

Device Management har eksisteret længe, men hvad betyder det egentligt, når vi nu begynder at tale om "Modern" Device Management? "Modern" er et populært begreb – særligt når vi taler om Microsoft. Hos Microsoft dækker begrebet over Azure – Microsofts cloud satsning. Med andre ord er løsningen flyttet ud i skyen.

Modern Management (også kaldet Modern Device Management) dækker over Microsofts nutidige anbefalede strategi for at styre Windows 10 enheder og mobile enheder ved hjælp af cloud teknologier.

Windows 10

Windows 10 er skabt til at styres via et MDM værktøj som Intune, og "enrolles" uden ekstra agenter, der sløver maskinen

MacOS

Giv dine Mac brugere adgang til virksomhedens data uden at gå på kompromis med sikkerheden eller din virksomheds data

iOS/iPadOS

Giv mulighed for BYOD (Bring your own device) uden risiko for at gå på kompromis med sikkerheden og din virksomheds data

Android

Der understøttes fire styringsscenarier til Android, hvor der ikke gås på kompromis med sikkerheden og din virksomheds data.

Men hvorfor skal man som virksomhed egentligt skifte til Modern Management, hvilke overvejelser bør man gøre sig inden man starter, og hvordan kommer man godt i gang?

Denne guide indeholder nogle af de svar, som kan hjælpe din virksomhed godt i gang med fremtidens Device Management.

Moderne styringsprincipper bygger på at sikre den dynamiske arbejdsplads, hvor arbejde ikke foregår på en bestemt lokation, men kan udføres hvor som helst, når som helst, sikkert og produktivt. Vi skaber rammerne.

Forstå de vigtigste nøglebegreber

En lille ordbog for at kunne forstå de vigtigste begreber og deres relation til hinanden.

Active Directory (AD)

Den nok mest udbredte Microsoft platform til administration af identiteter/brugere.

AD er traditionelt hostet on-premises

Co-management

Det første skridt mod en Intune løsning, hvor man fastholder Configuration Manager og samtidig begynder, at tage cloud i brug. Co-management vælges ofte pga. compliance politiker som kan benyttes som ekstra sikkerhed mod ubudne gæster.

Intune

Modern Device Management cloud løsning der kan styre iOS, iPadOS, MacOSX, Android og Windows

Autopilot

Onboarding proces fra ny-indkøbt enhed til styret enhed der er tilknyttet virksomhedens Azure Tenant. Giver en god brugeroplevelse og lavere omkostninger til IT Support

Config Manager (SCCM)

En del af Microsoft Endpoint Manager (MEM). Tidligere kendt som System Center Configuration Manager. En schweizer kniv inden for device management.

Microsoft Endpoint Manager (MEM)

Den overordnede paraply beskrivelse for Microsoft Endpoint Configuration Manager og Intune

Azure tenant

Microsofts cloud platform, begrænset til en specifik virksomhed eller organisatorisk enhed, og som indeholder alle komponenter i PaaS, IaaS, SaaS mv.

Hybrid Joined

Et begreb der bruges når enheder er registreret i både det traditionelle AD, men også i Azure AD

Tenant Attached

En metode til at binde Config Manager sammen med en Azure Tenant. Det gør enheder kan styres fra Intune, men uden de er enrollet i Intune. Denne mekanisme benytter Config Manager motoren til at udføre arbejdet på klienterne

MINDCORE

Hvorfor skal man investere i Modern Management?

Modern Management bidrager til at skabe en bedre digital oplevelse for virksomhedens brugere gennem forbedret enhedsadministration med et mindre infrastrukturfodaftryk, der reducerer omkostninger, kompleksitet, tid og kræfter.

Mere **Brugerorienteret**

Modern Management inkluderer muligheden for at erstatte klassiske management løsninger med en brugercentreret tilgang gennem Autopilot. Dette understøtter brugeroplevelsen ved at gøre det nemmere at udrulle og vedligeholde enheder, samt sikre, at brugerne kan arbejde hvor, hvornår og hvordan de vil uden reduceret funktionalitet eller oplevelse.

Mindre **infrastruktur**

Da Modern Management styring foregår gennem cloud-tjenester, er der ikke længere behov for en lokal infrastruktur. Det gør vedligeholdelsen nemmere, og kompleksiteten markant lavere for organisationen. Endvidere opnås høj sikkerhed og beskyttelse.

Lavere **omkostninger**

Mindre infrastruktur at vedligeholde samt brugen af Autopilot og Intune, der forenkler alle dele af Windows-enheders livscyklus, både for IT og slutbrugere. Det vil reducere de samlede omkostninger til implementering, administration og pensionering af enheder ved at reducere tid og kompleksitet.

Mere **automatisering**

Samarbejdet mellem Azure AD (administration af brugere i skyen) og andre Microsoft-produkter som Autopilot og Intune muliggør automatisering af utallige opgaver, som før var tungt og bøvlet. Det bidrager igen til, at der bruges mindre tid på at styre både enhederne og de værktøjer, der bruges til at styre dem.

MINDCORE

Overvej de rigtige tiltag fra starten

Fem tiltag, der er centrale at overveje inden din organisation går i gang med Modern Management

Beskyt brugernes identitet og virksomhedens data

Multi Factor Authentication (MFA)

Conditional access

Identity protection

Mobile Application Management (MAM)

Opdater og beskyt dine enheder

Microsoft Endpoint Manager

Co-Management

Tenant attach

Applikationer

Onboard nye maskiner hvor som helst

Autopilot

Co-Management

Cloud Politikker

God og hurtig support

Microsoft Teams

Quick assist

Indsigt og proaktive handlinger

Governance

Hardware livs cyklus

Software livs cyklus

MINDCORE

Beskyt brugernes identitet og virksomhedens data

Når vi starter på cloud rejsen, eksponerer vi brugerens identitet og data mod en større flade af trusler på internettet.

Det kræver sikkerhedstiltag for at sikre identiteten, så identitetstyveri undgås. Her anbefales en to-faktor løsning, hvor man autentificerer enten via tilsendt SMS, eller endnu bedre ved benyttelse af Microsofts to-faktor autentificerings app, "Authenticator" via den enkelte medarbejders mobil.

Når det kommer til virksomhedens data, skal virksomheden beslutte, hvordan data skal gøres tilgængelig for virksomhedens medarbejdere. Den valgte strategi har forskellige afledte konsekvenser for brugeren og sikkerheden. Nedenfor er de 3 mest udbredte strategier skitseret.

Scenarie 1

Strategi, hvor alle der skal have adgang til mail, bliver styret

Hvis man vælger, at alle skal styres, så lukker man både firmaejede og private enheder ind i sit management system.

Her skal man overveje, om brugerne virkelig vil synes, at det er i orden, at firmaet skal bestemme, hvilken passwordsikkerhed, compliance niveau med mere, de enkelte brugere skal have på deres egen private enhed.

Scenarie 2

Strategi, hvor alle må hente mails uanset, om de er styret eller ej

Brugerne kan tilgå deres firmamail uanset, hvilken enhed de bruger. De bliver ikke bedt om beskyttelse eller nogen anden form for sikkerhed.

Det gør det nemt for brugerne, men er ikke nødvendigvis den mest sikre løsning for virksomheden, da virksomheden skal kunne sikre data, særligt i forbindelse med ophør af arbejdsforhold eller tyveri.

Scenarie 3

Strategi, hvor man opdeler enhederne i kategorier - firmaejet og privat

En todelt strategi, der på den ene side holder virksomhedsejede enheder i lidt strammere snor end alt andet, og samtidig stiller nogle krav til private enheder, som forsøger at tilgå mail og anden virksomhedsrelateret data.

Denne løsning giver samme beskyttelse som scenarie 1, men giver større frihed for brugerne. Skulle der ske ændringer i arbejdsforhold, eller enheden bliver tabt eller stjålet, kan data nemt slettes.

MINDCORE

Opdater og beskyt dine enheder

Det er en naturlig del af virksomhedens IT drift, at enheder skal opdateres, men hvorfor gør man egentligt det?

- ✓ Virksomheden ønsker at minimere risikoen for indbrud i virksomhedens infrastruktur, hvilket kan forårsage katastrofale følger
- ✓ Fejl og problemer i operativsystemet skal patches og rettes
- ✓ Brugeren skal have adgang til forbedringer til eksisterende funktionalitet eller helt ny funktionalitet

Traditionelt har virksomheder brugt funktionalitet som WSUS (Windows Server Update Services) eller Configuration Manager Software Update Point, hvor opdateringer hentes ned i virksomhedens infrastruktur, for derefter at blive distribueret til enheder via LAN / VPN. Denne metode er ikke optimal i forhold til båndbredde, tidsforbrug og brugervenlighed, og slet ikke, når der er tale om opdateringer/patches, der skal hentes og distribueres månedligt.

Modern Management har i stedet et centralt fokus på **automatisering**, foruden **applikationer** og løbende **sikring** af virksomhedens enheder.

Automatisering:

Modern Management bygger i langt højere grad på **automatisering,** hvor det er muligt. Windows Update for Business (WUfB) er et udtryk mange måske har hørt om, men ikke nødvendigvis har erfaring med. Det handler dybest set om at minimere de ressourcer, som virksomheden bruger på udrulning af opdateringer/patches, så virksomheden i stedet kan koncentrere sig om at udvikle og forbedre på andre punkter. Microsoft har efterhånden bygget så meget funktionalitet til WUfB, at det for langt de fleste vil være det rigtige valg.

Lyder det ikke tiltalende at lave en udrulningsstrategi, og glemme alt om opdateringer? Det kan selvfølgeligt ikke helt lade sig gøre, men WUfB gør det simplere. Med den rigtige opsætning vil du kunne få alle fordelene ved en evergreen platform fra månedlige kvalitetsopdateringer, zero day opdateringer og halvårlige funktionsopdateringer.

Applikationer:

Applikationer er en stor del af processen. At skulle håndtere tredjeparts opdateringer, for at sikre huller, er mindst lige så vigtigt, som at få operativ system opdateringer, og bør således altid prioriteres af virksomheden, og indgå i virksomhedens strategi.

Sikring af enheder:

Af og til sker det, at man er nødt til at lukke bestemte protokoller, eller andre komponenter, på en enhed. Det skal være sådan, at man hurtigt kan reagere og lukke ned for den trussel, eller usikkerhed, uden at man behøver at benytte VPN, eller andre metoder, for at komme i kontakt med virksomhedens infrastruktur.

MINDCORE

Onboard nye maskiner hvor som helst

Inden virksomheder begynder at onboarde nye maskiner, er det vigtigt, at de beslutter, hvordan dette skal gøres – enten Azure AD Registered, Hybrid AD Joined eller Azure AD Joined. Valget kan være udfordrende, også selvom Microsofts anbefaling er helt klar.

En typiske reaktion er at *"vi skal køre Hybrid Joined"*, fordi man nødigt vil i gang med at sortere ud i 20 års ophobet gruppepolitiker eller komplekse login scripts, der mapper drev-bogstaver og printere.

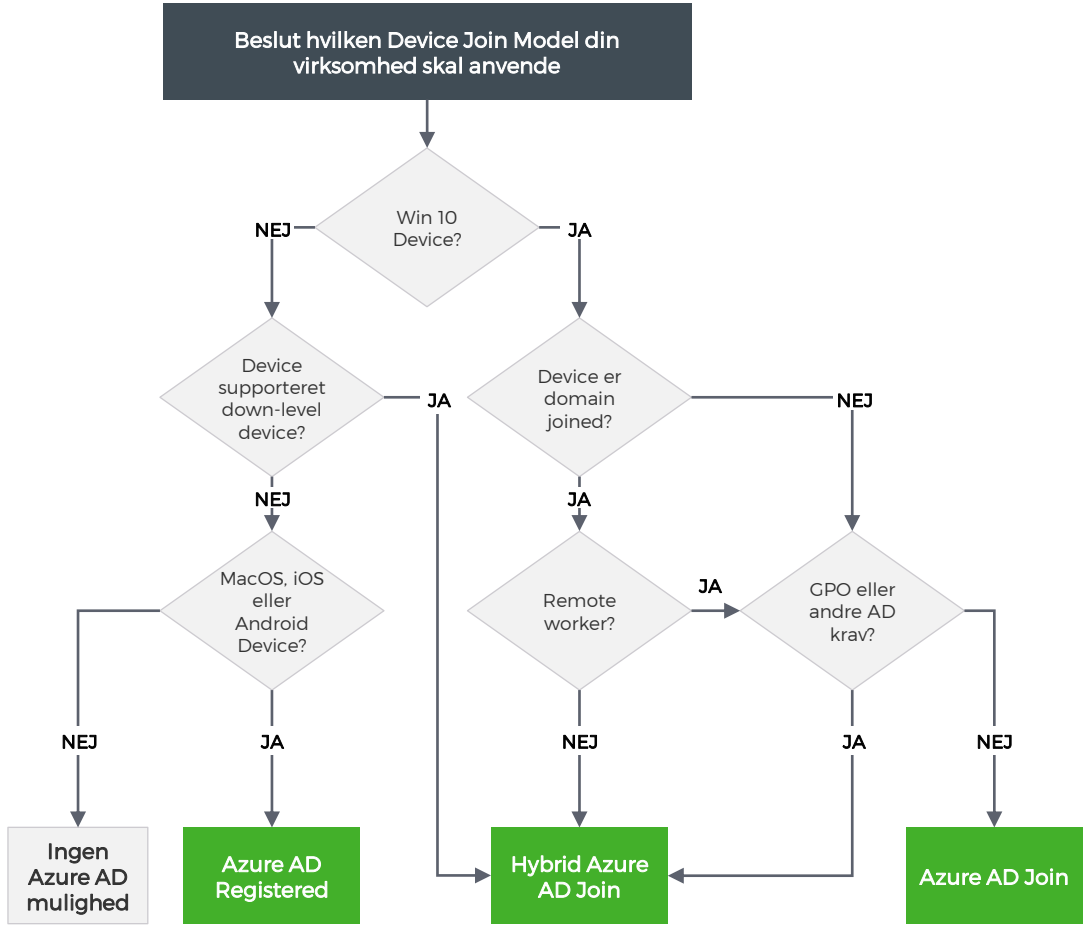
Vi anbefaler Azure AD Joined

Azure AD Joined er fremtiden, men uanset det er det vigtigt, at man får sat en klar strategi for, hvad man vil analysere for at komme til den rigtige destination. Husk på, at vi bygger Modern Management, fordi vi ønsker mere gennemsigtighed, nemmere styring, og mere selvbetjening – med andre ord, keep it simple!

Det er vigtigt, at virksomheden ikke alene ser cloud vejen som "lift and shift", men at man griber muligheden for at gentænke løsningen rigtigt med fokus på simplicitet og vedligehold. Det medfører engang imellem, at man må starte forfra.

Vælger man at onboarde enheder via Autopilot, så er det helt klart det simpleste at bygge sin infrastruktur op omkring at enhederne kun ligger i Azure AD og at fokusere på brugerens adgang til interne systemer fungere som var den tilknyttet traditionel AD.

Der er mange veje til at blive klar til Autopilot, men for at Autopilot bliver en succes hos jer, så kræver det, at en masse komponenter er på plads inden. En klassisk fejl, som mange begår, er at tænke en én-til-én overgang fra det man har i dag, hvor brugeren er vandt en fuldt klargjort enhed, som brugeren "bare" logger på og bruger. Der er andre måder at løse dette, hvor den gode brugeroplevelse fortsat er understøttet.



God og hurtig support

Modern Management handler i sidste ende om at servicere brugerne bedst muligt, og med størst mulig sikkerhed. Netop derfor er support vigtigt. Men hvad indebærer det egentligt?

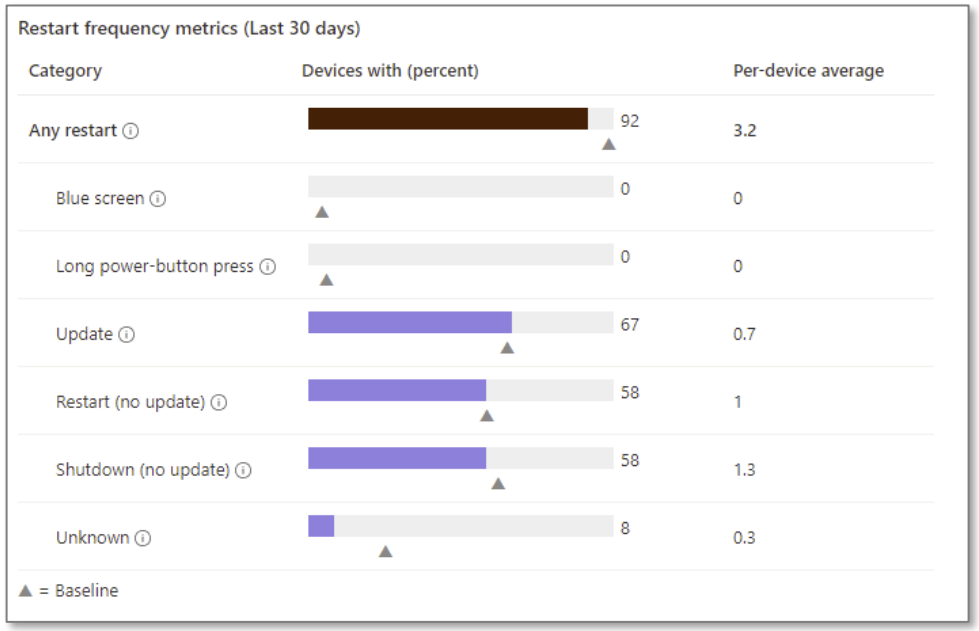
I dag sidder brugeren ofte på en internetlinje, og det kan derfor være vanskeligt at yde support på den traditionelle måde.

Igen skal vi have en strategi, og tænke ud af boksen. Der er mange måder at yde support på, og der er egentligt frit valg på alle hylder. Spørgsmålet er, om man vil betale ekstra for værktøjer til dette, eller om man kan "nøjes" med de indbyggede metoder, som er ganske udmærkede.

Microsoft Quick Assist er den mest oplagte metode til at supportere remote brugere.

Microsoft Teams er et andet godt alternativ. Teams er efterhånden særdeles udbredt, og da man typisk vil være i dialog med brugeren samtidig med, at de supporteres, fungerer løsningen godt.

Der findes også en lang række tredjepartsløsninger, som bl.a. **Teamviewer,** der har en connector, som kan supportere alle typer af enheder, og som Modern Management supporterer.



Foruden de nævnte supportværktøjer har Microsoft Intune indbygget Endpoint Analytics, som er en del af Microsoft's produktivitetsscore.

Som billedet til venstre viser, kan Endpoint Analytics give indsigt i opstartstider, applikationer som sløver enheden, bluescreens problematikker, og meget andet. Det skaber grundlag for en langt mere proaktiv support af brugerne.

MINDCORE

Tænk governance ind fra begyndelsen

I forbindelse med udrulningen af Modern Management platformen bør virksomheden have en klar strategi for governance af management platformen. Governance er vigtig, da det tvinger virksomheden til at tænke over, hvordan platformen skal styres fremadrettet. Hvis ikke dette tænkes ind fra starten, er det umuligt at sikre en ensartet platform, hvor regler og politikker overholdes.

Governance kan dække over rigtig mange ting. Men igen er det vigtigt at holde det simpelt, og fokusere på de vigtigste ting, og så kan man udvikle sin governance strategi over tid. Det er overvejelser såsom følgende;

- ✓ Hvor tit skal vi udskifte hardware?
- ✓ Hvordan skifter vi hardware?
- ✓ Hvad hvis enheden går i stykker og skal repareres?
- ✓ Hvis en medarbejder stopper, hvordan sletter vi så data?
- ✓ Hvis en enhed bliver stjålet, hvordan sletter vi så data?
- ✓ Skal vores brugere være lokale administratorer?
- ✓ Hvordan styres software og opgradering?
- ✓ Hvordan styres licenser?
- ✓ Hvilke rettigheder må helpdesk have?
- ✓ Osv

Governancemodellen skal sikre ”best practice” og en ensartet adfærd, hvor man er sikker på, at de kritiske opgaver rent faktisk bliver udført! Modellen skal være realistisk, klart beskrevet, og have tydeligt ejerskab. Og så skal der være en proces for løbende at opdatere og vedligeholde governancemodellen.

Måske tænker du ”ja det er alt sammen meget godt, men på nuværende tidspunkt er vi ikke klar til at gå fuldt efter en cloud løsning”

Er min virksomhed overhovedet klar til en fuld cloud løsning?

Hos Mindcore er vi godt klar over at det ikke er alle kunder der på nuværende tidspunkt har mulighed for at forfølge et fuldt cloud management setup.

Heldigvis er der en lang række muligheder for at komme i gang uden at gå all-in fra start, og skal vi være helt ærlige så er det ofte der vi ender i samarbejdet med vores kunder.

Eksempler på hvorfor mange virksomheder ikke er klar til et fuldt cloud management setup …

- Når en Win10 computer udleveres til medarbejderne forventes det at maskinen er umiddelbart klar til brug og med alle brugerens applikationer installeret.
- Der er for mange applikationer med traditionel AD integration
- Fortsat ønske om at anvende Endpoint Configuration Manager
- Licens krav til f.eks. Endpoint Manager
- Specielle netværksforhold, som f.eks. klienter der ikke kan tilgå internettet eller som er forbundet med satellit-forbindelser
- Politikker der endnu ikke er tilgængelige med Endpoint Manager og hvor script alternativer ikke er en acceptabel løsning
- Krav til f.eks. VPN løsning uden mulighed for split tunneling (ikke ideelt)
- Der benyttes løsninger med godkendelses flow oven på eksisterende on-premesis produkter

Kom i gang uden at gå all-in fra start. Her nogle typiske eksempler på kombinationsmuligheder vi har hjulpet vores kunder med at implementere …

- Co-management mellem Endpoint Configuration Manager og Endpoint Manager
- Cloud Management gateway til Configuration Manager
- Autopilot white glove
- Windows Autopilot og hybrid Azure Active Directory (Azure AD)-joined enheder
- Windows Virtual Desktop (WVD) – f.eks. til understøttelse af forretningsapplikationer med AD integration der ikke kan løses på anden måde
- Azure AD Application Proxy til publicering af applikationer mod Internettet
- Og mange flere muligheder

Endelig er det naturligvis også stadig muligt at forblive på en traditionel management platform som Configuration Manager og se helt bort fra cloud, med de udfordringer og begrænsninger det kan give.

MINDCORE

Hvad nu? Hvordan kommer du videre?

Vil du gerne vide, hvad der kunne være løsningen lige netop for din organisation?

Vi laver en 1-dags workshop – den er konkret og fokuseret på at give indsigt, overblik og klare handlingsrettede anbefalinger til at komme videre. Ræk ud og hør mere!

Du kan også **gå på opdagelse i vores Tekniske Blog**, der indeholder en lang række dybdegående tekniske artikler om Infrastruktur, Sikkerhed, Klient Administration og Cloud.

Herunder kan du finde links til konkrete blogs der relaterer sig til Microsoft Endpoint Manager mv. … og der kommer hele tiden flere til.

Image devices without need of infrastructure: https://blog.mindcore.dk/2021/03/osdcloud-image-devices-without-need-of.html
MEMCM debug using Azure blob: https://blog.mindcore.dk/2021/02/memcm-debug-using-azure-blob.html
Transition from legacy WSUS to Windows Update for Business: https://blog.mindcore.dk/2021/01/transition-from-legacy-wsus-to-windows.html
How I manage my device from Endpoint Manager - taste your own medicine - Part 1 of 4: https://blog.mindcore.dk/2020/11/how-i-manage-my-device-from-endpoint.html
How I manage my device from Endpoint Manager - taste your own medicine - Part 2 of 4: https://blog.mindcore.dk/2020/12/how-i-manage-my-device-from-endpoint.html
How I manage my device from Endpoint Manager - taste your own medicine - Part 3 of 4: https://blog.mindcore.dk/2020/12/how-i-manage-my-device-from-endpoint_11.html
How I manage my device from Endpoint Manager - taste your own medicine - Part 4 of 4: https://blog.mindcore.dk/2020/12/how-i-manage-my-device-from-endpoint_18.html
Patch management – Windows SSU and LCU bundled into one cumulative update: https://blog.mindcore.dk/2020/12/patch-management-windows-ssu-and-lcu.html
Manage security polices directly from the cloud without co-management: https://blog.mindcore.dk/2020/11/manage-security-polices-directly-from.html
Modern Roaming Profile - Enterprise State Roaming (ESR) + UE-V: https://blog.mindcore.dk/2020/08/modern-roaming-profile-enterprise-state.html
Microsoft Endpoint Analytics – Proactive remediations: https://blog.mindcore.dk/2020/08/microsoft-endpoint-analytics-proactive.html
Step by step Autopilot scenarios: https://blog.mindcore.dk/2020/08/step-by-step-autopilot-scenarios.html
MSIX Modern Packaging – Part 1: https://blog.mindcore.dk/2021/02/msix-modern-packaging-part-1.html

Mindcore Teknisk Blog udgiver dybdegående tekniske artikler om Infrastruktur, Sikkerhed, Klient Administration og Cloud.

https://blog.mindcore.dk

LinkedIn Group
MODERN ENDPOINT MANAGEMENT
Official Contributor
2021

Mattias Melkersen, konsulent hos Mindcore, er også "Official Contributor" i Modern Endpoint Management gruppen på LinkedIn, hvor han løbende skriver indlæg.

Kontakt os endelig hvis du vil høre mere

· MINDCORE ·
Lottenborgvej 26A, 2. tv, 2800 Kongens Lyngby

Mattias Melkersen

Microsoft 365 Konsulent
E-mail: mm@mindcore.dk
Mobil: +45 31 31 57 73

Lars Lohmann Blem

Partner
E-mail: ll@mindcore.dk
Mobil: +45 31 20 51 20

Jacob Guldager-Løve

Partner
E-mail: jgl@mindcore.dk
Mobil: +45 52 15 01 14

MINDCORE