

HIGH LEVEL DESIGN

MODERNE WERKPLEK



gemeente Midden-Delfland
Handelsweg 100
2988 DC Ridderkerk

Door:
SoftwareONE
Naritaweg 177
1043 BW Amsterdam

26.08.2021

CONTENTS

1	Gebruikte terminologie	5
2	Project informatie	7
2.1	Introductie.....	7
2.2	Document Historie	7
2.3	Distributie.....	7
3	Scope	8
3.1	Doelgroep.....	8
3.2	In scope	8
3.3	Buiten scope.....	8
4	Architectuur	9
4.1	Concept werkplek van de toekomst	9
4.2	Huidige situatie	10
4.3	Huidige technologieën	11
4.4	Gekozen technologieën	12
5	Roadmap	13
5.1.1	Functie tabel	13
5.1.2	Aanverwante trajecten	16
6	Microsoft 365 ontwerp	17
6.1	Gefaseerde aanpak implementatie Microsoft 365 services	17
6.1.1	Microsoft 365 platform updates.....	20
6.1.2	Microsoft 365 Apps for Enterprise.....	21
6.1.3	Office Online	22
6.1.4	SharePoint Online	23
6.1.5	OneDrive for Business.....	24
6.1.6	Microsoft Exchange.....	24
6.1.7	Microsoft Teams	26
6.2	Microsoft Endpoint Manager	27
6.2.1	Intune	27

6.2.2	AutoPilot	28
6.2.2.1	Enrollment Restrictions.....	28
6.2.2.2	Lokale beheerders.....	29
6.2.2.3	Device Compliance.....	29
6.2.2.4	Device Configuration.....	29
6.2.3	Microsoft Endpoint Configuration Manager.....	30
6.2.4	Desktop Analytics.....	30
7	Infrastructuur	31
7.1	Endpoints	31
7.2	Identiteit.....	31
7.3	Enterprise applicaties.....	35
7.4	Multi Factor Authenticatie	36
7.5	Conditional Access (CA).....	38
7.6	Company Branding.....	39
7.7	Role Based Access Control	40
7.8	Privileged Identity management (PIM).....	40
7.9	Windows 10	42
7.9.1	Installatie.....	43
7.9.2	Windows 10 update	43
8	Beveiliging	46
8.1	Windows Defender Firewall.....	46
8.2	Windows Defender SmartScreen.....	46
8.3	Windows Defender Antivirus	46
8.4	BitLocker	47
8.5	Microsoft Defender	47
8.6	Microsoft Information Protection (MIP).....	48
8.7	Data Loss prevention (DLP).....	49
8.8	Microsoft Cloud App security (MCAS).....	49
8.9	Beveiligingsinformatie en event-management (SIEM)	50
9	Bijlagen	51

9.1	Bijlage 1: Beschrijving Adoptie	51
9.2	Bijlage 2: Cloud exit strategie	53

1 Gebruikte terminologie

Dit document bevat afkorting en terminologie welke niet altijd bekend of duidelijk zijn voor alle lezers ongeacht niveau of kennisgebied. Daartoe is een terminologie overzicht gemaakt met gebruikte termen binnen dit document en een korte uitleg van het concept:

MW – Moderne Werkplek: Een Moderne Werkplek zorgt ervoor dat medewerkers het beste uit zichzelf halen, met elkaar op een veilige manier kunnen samenwerken en flexibel zijn in de keuze van apparaten en apps.

LoB – Line of Business applicatie: Is een algemene term die verwijst naar een product of apps & diensten die een bepaalde zakelijke behoefte dienen voor een organisatie of bedrijfstadak.

HLD – High Level Design: Brengt de overkoepelende systeemarchitectuur in kaart. Het bevat de systemen, het design en beschrijven de relaties tussen de verschillende onderdelen en gewenste functies. In de HLD wordt zichtbaar gemaakt welke systemen waarvoor ingezet worden.

A/V – Audio / Video: Het hebben leveren of verplaatsen van een audio/video signaal. In de context van IT vaak gebruikt voor teleconferentie systemen.

MAM – Mobile Application Management: Microsoft definieert MAM als de suite van Intune-beheerfuncties waarmee mobiele apps geïnstalleerd worden, configureren, beveiligen, bewaken en bijwerken.

MDM – Mobile device management: MDM stelt gebruiker centraal zonder dat veiligheid en eenvoudig beheer in het gedrang komt. Mobile Device Management biedt optimaal gebruiksgemak met grip het gehele apparaat.

MFA – Multi-factor Authenticatie: Wanneer gebruikers toegang willen tot een account of app, moeten deze hun identiteit nog een keer extra verifiëren, bijvoorbeeld via een scan van een vingerafdruk of door het invoeren van een code die is ontvangen op de telefoon.

VDI – Virtual Desktop Infrastructure: Een gebruiker krijgt een eigen virtuele pc met eigen besturingssysteem op de server toegewezen zonder dat hiervoor additionele hardware noodzakelijk is.

AD FS – Active Directory Federation Services: Geeft eindgebruikers single sign-on toegang tot systemen en applicaties. Het maakt gebruik van een op claims gebaseerd autorisatiemodel voor toegangscontrole om de applicatiebeveiliging te behouden en om federatieve identiteiten te implementeren.

WAP – Web Application Proxy: Een van de belangrijkste taken van het WAP is het vooraf verifiëren van toegang tot web toepassingen met behulp van Active Directory Federation Services (AD FS), en in deze hoedanigheid functioneert het WAP als een AD FS-proxy.

SaaS – Software as a Service: Is software die als een online dienst wordt aangeboden. Een organisatie hoeft de software niet aan te schaffen, maar sluit bijvoorbeeld een contract per maand per gebruiker af.

CA – Conditional Access: Zorgt voor voorwaardelijke toegang, deze voorwaarden vaak gebaseerd op locatie, activiteit of risico geven de organisatie de mogelijkheid controle toe te passen gebaseerd op deze parameters.

2 Project informatie

2.1 Introductie

Gemeente Midden-Delfland heeft ruim 200 medewerkers in dienst en heeft recentelijk besloten om voor haar medewerkers een werkplek concept te leveren wat is gebaseerd op de moderne werkplek (MW).

Dit document dient als High Level Design voor een op hoofdzakelijk Microsoft technologie gebaseerde moderne werkplek met als doel medewerkers altijd en overal in staat te stellen om te kunnen werken. Dit document beschrijft de gemaakte ontwerp keuzes voor deze moderne werkplek. In de visie van SoftwareONE is een High Level Design (HLD) bedoeld voor het nemen van noodzakelijke (technische) beslissingen. Maar ook bedoeld voor het vastleggen van een basis inrichting van de moderne werkplek. Het geeft een richting aan de koers die een IT afdeling de komende jaren zou kunnen varen. Het HLD neemt waar nodig technische beslissingen indien dit niet anders kan, in alle andere gevallen wordt er gesproken over een onderwerp op de hoofdlijnen en beslissingen van technische of inrichting aard worden later genomen.

2.2 Document Historie

Datum	Auteur	Versie	Referentie
08-07-2021	Erik Stiphout / Roderick de Ruijter	0.1	Initiële versie
21-07-2021	Erik Stiphout / Roderick de Ruijter	0.2	Verwerken 1 ^e review
25-08-2021	Erik Stiphout / Roderick de Ruijter	0.3	Release kandidaat
26-08-2021	Erik Stiphout / Roderick de Ruijter	1.0	Definitieve versie

2.3 Distributie

Nr	Naam	Functie	Organisatie	Van versie
1	Rogier Winkelhorst	Adviseur informatie voorziening	gemeente Midden-Delfland	0.1
2	Mark Stampraad	Adviseur informatie voorziening	gemeente Midden-Delfland	0.1
3	Djarano Faerber	Project leider	SoftwareONE	0.1
4				
5				
6				
7				
8				
9				

3 Scope

3.1 Doelgroep

Dit document tracht een ontwerp op globaal niveau te leveren als gids voor domein/cloud architecten en technici die betrokken zijn bij het moderne werkplek traject.

3.2 In scope

De omvang van het High Level Design(HLD) is als volgt:

- › Moderne werkplek architectuur
- › Identiteit & veiligheid
- › Office 365
- › Microsoft 365 Apps for Enterprise
- › Office Online
- › SharePoint Online
- › OneDrive for Business
- › Exchange Online
- › Windows 10 / Windows 11
- › Intune

3.3 Buiten scope

Dit document behandelt alleen het bereik dat is gespecificeerd in de sectie '3.2 In scope'. Er moet echter worden opgemerkt dat dit project gebruik maakt van de huidige primaire infrastructuurcomponenten. De hieronder weergegeven infrastructuurcomponenten zijn reeds beschikbaar in de huidige infrastructuur en vallen daarmee buiten scope.

- › Netwerk
- › Active Directory
- › Fysieke werkplekken
- › Telefonie inrichting

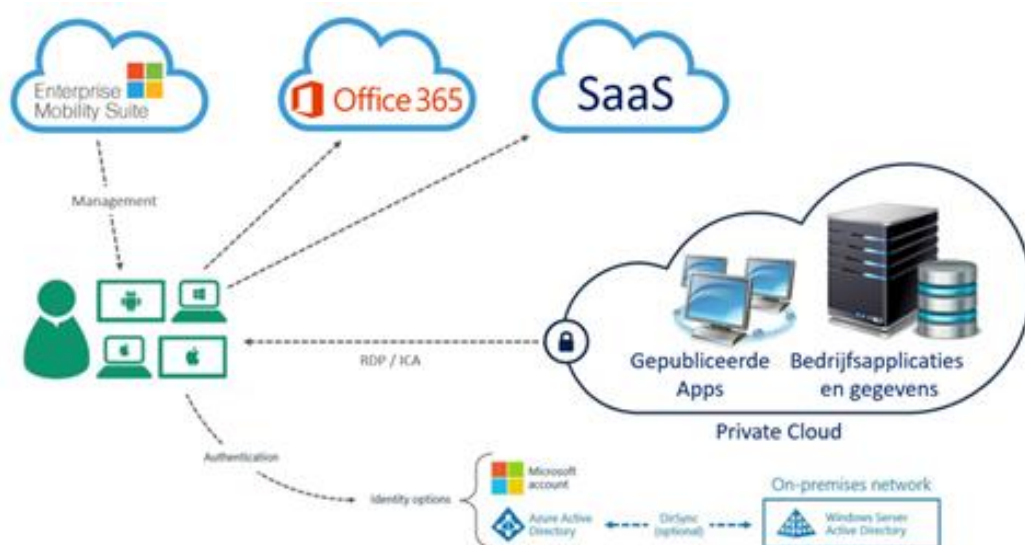
4 Architectuur

4.1 Concept werkplek van de toekomst

Dit hoofdstuk beschrijft in algemene termen de manier waarop SoftwareONE aankijkt tegen het moderne werkplek concept en de bijbehorende architectuur. Hierbij wordt op een hoog niveau een opsomming gedaan van de manier waarop Microsoft 365 gebaseerde clouddiensten samenwerken en daarbij de moderne werkplek vormen. Zoals elk concept is deze aanpasbaar om invulling te geven aan de specifieke wensen van de gemeente Midden-Delfland.

Naar de mening van SoftwareONE is de moderne werkplek gebaseerd op een apparaat in de vorm van een desktop, laptop of tablet met Windows 10 / Windows 11 waarop zowel lokale als cloud applicaties beschikbaar zijn. Voor legacy en high secure apps is een connectie met de Remote Desktop Services werkplek (of vergelijkbaar concept zoals VDI) de meest voor de hand liggende oplossing. De gemeente Midden-Delfland heeft specifiek gekozen voor het concept met een non-persistent werkplek in de vorm van Citrix i.c.m. Ivanti omdat dit aansluit bij de visie die de organisatie.

Interactie (broker / bestandsuitwisseling) tussen de moderne werkplek en de Citrix werkplek vindt straks plaats via OneDrive for Business. Alle persoonlijke bestanden verhuizen daarom naar OneDrive for Business en niet meer op de netwerk gebaseerde schijf binnen de on-premises fileserver omgeving.



De Windows moderne werkplek wordt uitgerold via Autopilot in combinatie met Intune policy's. Intune zal tevens ingezet worden voor software deployment en het beheer van de moderne werkplek.

Dankzij Windows AutoPilot zijn gebruikers zelf in staat om Windows 10 naar fabriek instellingen te resetten en zo gebruiksvriendelijk mogelijk het apparaat opnieuw in te schrijven als moderne werkplek apparaat. De serienummers benodigd voor Windows AutoPilot worden verzameld en handmatig geüpload naar de Microsoft Store for Business. In de nabije toekomst zal de gemeente Midden-Delfland hardware

aanschaffen waarbij de leverancier direct de serienummers aanlevert of zelfs rechtstreeks in de Windows Store for Business plaatst. Binnen de huidige roadmap zal dit binnen 4 jaar gerealiseerd kunnen worden.

Apps worden bij voorkeur aangeboden als SaaS, via Ivanti of uit de Windows Store for Business vanwege de beperkte beheerinspanning. Indien dit niet mogelijk is wordt er een MSI/EXE installatiepakket gebouwd of in uiterste nood vindt er een handmatige installatie plaatst. De Microsoft 365 Apps for Enterprise worden standaard geïnstalleerd op de moderne werkplek.

De moderne werkplek zal beheerd worden door de IT afdeling, de medewerker heeft voor het gebruik geen beheer rechten nodig en kan altijd via de supportdesk ondersteuning vragen bij installatie van randapparatuur en software. Dit laatste met de kanttekening dat deze software een bedrijfsdoel dient. De Citrix werkplek heeft een eigen beheer scenario waarbij gebruik gemaakt wordt van een referentie image. Met die referentie image kan er aan elke nieuwe gebruikers sessie een schone image gepresenteerd worden.

Omdat er koppeling is tussen twee werkplekken (full client & non-persistent werkplek) moet het voor de gebruiker helder zijn wanneer ze een lokale app starten en wanneer een Citrix app. Hierin levert een adoptie programma voor de moderne werkplek een belangrijke bijdrage.

De moderne werkplek heeft connectiviteit met het interne draadloze netwerk van de gemeente Midden-Delfland. Op locaties waar dit netwerk niet beschikbaar is kan de medewerker gebruik maken van een regulier draadloos of bekabeld netwerk welke toegang geeft tot het internet. Vrijwel alle gebruikte diensten zoals Exchange Online, Teams, Intune, OneDrive for Business, Windows AutoPilot, etc. vereisen een stabiele en moderne internetverbinding voor volledige functionaliteit.

Naast de laptop, desktop en tablet apparaten welke worden uitgegeven door de gemeente Midden-Delfland kan de medewerker ook gebruik maken van privé apparatuur. Hoewel privé apparatuur tot op heden is toegestaan heeft de gemeente Midden-Delfland het beleid om gebruik van privé apparatuur te ontmoedigen. Los van dit beleid is het mogelijk om informatie op privé apparatuur te beveiligen door gebruik te maken van Intune App Protection. Hiermee voert de gemeente Midden-Delfland altijd de regie over de data en zijn ze in staat om hier beleid op te voeren. Alle overige (privé) apparatuur zoals PC's hebben geen toegang tot Gemeente Midden-Delfland data.

De Moderne Werkplek voor de gemeente Midden-Delfland is opgesteld op basis bouwblokken die goed op elkaar aansluiten en flexibel inzetbaar zijn.

4.2 Huidige situatie

Om de werkplek van de toekomst te kunnen bouwen moet eerst worden gekeken naar het heden. Voor de Gemeente Midden-Delfland is recentelijk een architectuur sessie gegeven omtrent dit onderwerp, hierbij was vertegenwoordiging van het management en de IT-afdeling van de gemeente Midden-Delfland aanwezig.

gemeente Midden-Delfland heeft een complex IT-landschap welke historisch is gegroeid door eisen en wensen vanuit de organisatie. Dit betekent dat de IT-organisatie maximaal belast is met beheer taken. Daarnaast is de organisatie bezig met consolidatie werkzaamheden van alle IT-onderdelen omdat de

infrastructuur/resources van de gemeente Midden-Delfland op sommige punten gedeeld wordt met gemeenten Leidschendam-Voorburg en Westland.

De huidige werkplek van de Gemeente Midden-Delfland bestaat uit een Citrix oplossing i.c.m. Ivanti workspace welke alle eindgebruikers door middel van thin client werkplek een non-persistent Citrix desktop serveert op basis van het Windows 10 O.S. Non-persistent wil zeggen dat alleen gebruikers specifieke data wordt opgeslagen en dat sessie data na uitloggen verdwijnt.

gemeente Midden-Delfland maakt reeds of deels gebruik van diverse cloud gebaseerde oplossingen en diensten zoals Azure MFA en Exchange Online, dit cloud platform verzorgt opslag en afhandeling van alle email, contacten en kalenders van eindgebruikers.

Overige onderdelen die zijn besproken tijdens de workshop, of nadien aangeleverd, worden verder in het HLD beschreven.

4.3 Huidige technologieën

De onderstaande tabel is een overzicht van de huidige technologie inrichting van gemeente Midden-Delfland dit is een verkort overzicht van alle producten die nu in het directe landschap van de moderne werkplek vallen. Er zijn uiteraard nog meerdere andere producten en technologieën waarmee gewerkt wordt deze worden echter hier niet genoemd omdat deze buiten de scope van de architectuur vallen.

Onderdeel	Gekozen technologieën
Identiteit & Authenticatie	<ul style="list-style-type: none"> › Active Directory Services › Azure Active Directory › Azure AD Connect › Authenticatie federatie (AD FS)
OS uitrol	<ul style="list-style-type: none"> › VMWare i.c.m. Citrix
Apparaat- en applicatiebeheer	<ul style="list-style-type: none"> › Ivanti
Beveiliging	<ul style="list-style-type: none"> › Pointsharp MFA › TrendMicro endpoint protection › Cryptshare / Zorgmail › FortiMail Secure Email Gateway
Productiviteit	<ul style="list-style-type: none"> › Office 2016
Werkplek	<ul style="list-style-type: none"> › Windows 10 Non-persistent desktop (Citrix) › Ivanti › Fslogix

4.4 Gekozen technologieën

Onderstaande tabel geeft een totaalopsomming van de gekozen technologieën die betrekking hebben op de moderne werkplek. Hierbij is rekening gehouden met de licentie keuze van de gemeente Midden-Delfland.

Onderdeel	Gekozen technologieën
Identiteit & Authenticatie	<ul style="list-style-type: none"> › Active Directory Services › Azure Active Directory › Azure AD Connect › Password Hash synchronisatie
OS uitrol	<ul style="list-style-type: none"> › AutoPilot (Windows 10 uitrol op full clients) › Citrix (image beheer voor non-persistent desktops)
Apparaat beheer	<ul style="list-style-type: none"> › Microsoft Intune › Windows AutoPilot
Beveiliging	<ul style="list-style-type: none"> › Windows Defender Firewall › Windows Defender anti-virus › TrendMicro Endpoint protection › Client harddisk encryptie › Azure MFA › Microsoft Information Protection › Privileged Identity Management › E-mail encryptie (veilig mailen)
Productiviteit	<ul style="list-style-type: none"> › Microsoft 365 workloads (Exchange, Teams, SharePoint etc)(NIEUW) › Ivanti (applicatie/user management op non-persistent desktops) › Microsoft 365 Apps for Enterprise

5 Roadmap

Naast de genoemde oplossing en technologieën is SoftwareONE gevraagd om een roadmap op te stellen voor implementatie van de moderne werkplek en technologieën binnen de IT-omgeving van gemeente Midden-Delfland.

Het doel van deze roadmap is om de organisatie te helpen om het volgende te bereiken:

- › Het zorgt ervoor dat het IT-team begrijpt waar naartoe gewerkt wordt, mede door de technologie af te stemmen op de korte- en lange termijn doelen van de organisatie;
- › Het maakt een effectieve toewijzing van tijd, geld en mensen mogelijk door verwachtingen, prioriteiten en schema's te communiceren;
- › Het vormt een basis voor het stellen van prioriteiten en biedt een focus voor de organisatie.

In dit stadium van het project is het echter niet mogelijk om al tijdsblokken te gaan definiëren waarin iets gemigreerd of geïmplementeerd kan worden, dit zal gedurende het traject inzichtelijk gemaakt kunnen worden.

	In gebruik	Q2 2021	Q3 2021	Q4 2021	Q1 2022	Q2 2022	Q3 2022	Q4 2022	Q1 2023	Q2 2023	Q3 2023	Q4 2023	Q1 2024	Q2 2024	Q3 2024	Q4 2024	Q1 2025	Q2 2025
Authenticatie																		
Beveiliging																		
Governance / DLP																		
Intune (MAM & MDM)																		
AutoPilot																		
SharePoint																		
OneDrive																		
M365 Apps for Ent.																		
Exchange Online																		
Teams																		
Power Platform																		
Forms																		
Planner																		
Stream																		
SIEM																		

Legenda	Kwartaal
Workload in gebruik	
Workload niet in gebruik	

Als eerstvolgende stap voor de gemeente Midden-Delfland zou SoftwareONE voorstellen om de uitrol van een nieuw office pakket te starten in de vorm van Microsoft 365 Apps for Enterprise. Dit ter ondersteuning van de inzet van meer cloud diensten in de komende maanden zoals Exchange Online en OneDrive.

De uiteindelijke roadmap items worden gedurende dit project gezamenlijk met de gemeente Midden-Delfland opgesteld zodat deze optimaal aansluit bij de gewenste strategie.

5.1.1 Functie tabel

Naast bovengenoemde oplossing en technologieën heeft SoftwareONE een roadmap opgesteld voor de implementatie van de hybride cloud werkplek en technologieën binnen de IT-omgeving van de gemeente Midden-Delfland. SoftwareONE heeft een reeks basisfuncties voor eindgebruikers geïdentificeerd die tijdens de workshop zijn besproken en beschikbaar moeten zijn voor eindgebruikers.

Basis Functies

MS365-Word	
MS365-Excel	
MS365-PowerPoint	
MS Teams	<p>Dynamic Teams-sites</p> <p>Creëren Teams-sites</p> <p>Templates voor Teams-sites</p> <p>Apps</p> <ul style="list-style-type: none"> - Trello - Planner - OneNote <p>Connectors/ Webhooks</p> <p>Public Teams-sites</p> <p>Deelnemen in Teams-sites</p>
Meeting (video/ audio)	<p>Instant channel meetings (meet now)</p> <p>Call /chat</p> <p>Geplande meeting deelname</p> <p>Organiseer meetings</p> <p>Live event organisatie</p> <p>Teams meeting rooms (met room hardware)</p>
Chat	<p>Individuele chat</p> <p>Groupchat</p> <p>File sharing</p> <p>Yammer</p>
Kalender	<p>Organiseer geplande meetings</p> <p>Organiseer live-events</p> <p>Sharing meeting links</p> <p>Meeting starten uit de Outlook kalender</p>
Files	Upload

	<p>Deel</p> <p>Edit</p> <p>Collaboratie</p> <p>Download/Sync</p>
Planner/Trello	<p>Creëer een Teams based takenlijst</p> <p>Voeg notities toe aan een taak</p> <p>Taken toewijzen</p>
Stream	<p>Upload videos en call recordings</p> <p>Delen met collega's</p>
Wiki pages	
OneNote	
Screen sharing	
Forms	
Data governance	Labeling van alle relevant data in de workloads welke sensitieve data bevatten.
Data Loss Prevention	Polities tegen onwillekeurig delen van data
Externe toegang in Teams	External access binnen teams door guest (organisaties)
Externe toegang voor video conferences	Nodig gasten uit voor Teams conference meetings
Reporting	Teams gebruik of gebruik in SharePoint
Multi-factor authenticatie	Providing an additional layer of security

Uitgebreide functionaliteit	
Tooling voor Communities	Yammer
(kamer) reserveren	Booking

Whiteboard	Microsoft Whiteboard
Power Platform (Automate, Apps, BI)	
Information security	Bepalen welke gegevens waar worden opgeslagen, door een set labels te definiëren die de inhoud onderzoekt en veilige opslag en delen mogelijk maakt
Informatie retentie	Protect data with policies that are combined with organization governance labels
Telefonische vergadering toegang	Telefonisch inbellen op vergaderingen
Guest access	Delen van documenten met guests.
Self-service password reset	Zelf redzaamheid voor eindgebruikers om een password reset te doen

5.1.2 Aanverwante trajecten

Naast het moderne werkplek concept lopen er diverse andere vernieuwings-trajecten op ICT gebied welke (deels) van invloed kunnen zijn op het moderne werkplek concept. Een overzicht hiervan is:

- › **FSLogix implementatie**
Met FSLogix technologie kan de cache van bijvoorbeeld OneDrive en Exchange Online buiten het gebruikersprofiel geplaatst worden. Hierdoor blijft de gebruikers cache bewaard en hoeft deze niet bij elke nieuwe Citrix sessie opnieuw opgebouwd worden. Het vasthouden van deze cache draagt aanzienlijk bij aan een goede gebruikers ervaring.
- › **Telefonie project, vervanging van de telefonie centrale.**
Het is mogelijk om telefonie te integreren met bijvoorbeeld Teams en eventueel aanvullende software voor call routing. Daar dit vaak opzichzelfstaande complexe trajecten zijn valt deze buiten de scope van de moderne werkplek maar zijn er wel raakvlakken de bij een dergelijk traject onderzocht dienen te worden.

6 Microsoft 365 ontwerp

Microsoft 365 bestaat uit een verzameling van verschillende diensten geconcentreerd over werkplek diensten en achterliggende veiligheids- en infrastructuur-diensten. Per dienst wordt er beschreven hoe deze ingezet kan worden bij de gemeente Midden-Delfland. Per dienst of configuratie zal een ontwerpkeuze worden beschreven.

6.1 Gefaseerde aanpak implementatie Microsoft 365 services

Een groot onderdeel van Microsoft 365 services zijn gericht op productieve diensten die in verschillende licenties vormen afgenomen kunnen worden.



Omdat de Microsoft 365 E3 licentie bestaat uit een grote diversiteit aan componenten is het vrijwel onmogelijk om alle componenten direct aan de medewerkers van gemeente Midden-Delfland aan te bieden.

Het advies is om via een gefaseerde aanpak nieuwe componenten te introduceren. Hierdoor kan aan elke component de juiste aandacht worden geven waardoor een hoog adoptie niveau wordt gerealiseerd.

Daarnaast is er via deze methode grip op het gebruik van de componenten door de medewerkers, en kan er gepaste ondersteuning geboden worden zonder dat de beheerders achter de feiten aan lopen.

In de navolgende tabel staat een overzicht van alle componenten uit de Microsoft 365 suite. Per component staat een bondige beschrijving en wordt vermeld of het component wordt geactiveerd voor de gemeente Midden-Delfland medewerker. Deze keuzes komen voort uit de workshop die gehouden is voorafgaand aan het schrijven van het HLD.

Component	Beschrijving	Geactiveerd
To-Do	Intelligente Taken-App. Opvolger van Wunderlist.	Nee
Microsoft Forms	Microsoft Forms is een eenvoudige, lichtgewicht app waarmee u eenvoudig enquêtes, toetsen en peilingen kunt maken.	Ja

Stream for Office 365	Maak, ontdek en deel video's op een veilige manier in de hele organisatie.	Ja
Microsoft StaffHub	<p>Bedoeld voor medewerkers zonder vaste werkplek. Bevat functionaliteit voor planning en diensten, het plaatsen van notities en het delen van documenten aan kleine teams. Biedt managers een web omgeving voor het maken van roosters en de planning. Medewerkers kunnen hun roosters zien. Ook kunnen zij via de app diensten ruilen, vrij vragen of ziekmelden en hun beschikbaarheid aangeven.</p> <p>Bovendien biedt de mobiele app van Microsoft Staffhub een chatfunctie (een professionele versie van WhatsApp). Je kunt een-op-een met collega's of met het hele team chatten.</p>	Nee
Power Automate	Microsoft Power Automate is een product waarmee u geautomatiseerde werkstromen tussen uw favoriete apps en services kunt instellen om onder andere bestanden te synchroniseren, meldingen te ontvangen en gegevens te verzamelen.	Ja
PowerApps for Office 365	PowerApps is een service voor het bouwen en gebruiken van aangepaste zakelijke apps waarmee u verbinding met uw gegevens kunt maken en zowel via internet als mobiel kunt werken - zonder dat u tijd en kosten hoeft te besteden aan de ontwikkeling van aangepaste software.	Nee
Microsoft Teams	Microsoft Teams is een werkruimte in Office 365 die speciaal voor chatten is bedoeld. Het biedt één locatie voor personen, gesprekken, bestanden en hulpmiddelen, zodat iedereen direct toegang heeft tot alles wat ze nodig hebben.	Ja
Microsoft Planner	Met Planner kan je team eenvoudig nieuwe plannen maken, taken organiseren en toewijzen, bestanden delen, chatten over het werk en updates over de voortgang ontvangen.	Ja
Sway	Sway is een App waarmee u gemakkelijk interactieve rapporten, persoonlijke verhalen, presentaties en meer kunt maken en delen.	Nee
Yammer Enterprise	Yammer is een besloten sociaal netwerk voor organisaties en is gebaseerd op open communicatie. U kunt hiermee bijvoorbeeld problemen met ondersteuning oplossen, feedback over projecten	Nee

	en documenten verzamelen en aanbevolen procedures rondsturen. Yammer-groepen zijn een plek waar leden sneller met een project kunnen starten, kunnen deelnemen aan discussielijnen en klanten en leveranciers kunnen betrekken in gesprekken. Yammer helpt u tevens bij het vinden van relevante informatie, groepen, bestanden en personen, zodat iedereen zijn of haar kennis kan delen, los van afdelingen en tijdzones.	
Azure Rights Management	Deze Cloud service gebruikt beleidsregels voor versleuteling, identiteit en verificatie om uw bestanden en e-mail te beveiligen op meerdere apparaten, zoals telefoons, tablets en pc's.	Ja
Microsoft 365 Apps for Enterprise (voorheen genoemd Office 365 Pro Plus)	Microsoft 365 Apps for Enterprise is een volledige Office-versie die gebruikers kunnen downloaden en lokaal installeren. De cloud-variant van Office is vergelijkbaar met de Office 2019 versie die nu on-premises beschikbaar is. De functionaliteit van de beide Office-versies is vergelijkbaar en Microsoft 365 Apps for Enterprise en bevat dezelfde applicaties als Office 2019. Toch zijn er behoorlijk wat verschillen tussen beide versies, die zich met name uiten in verschillende manieren van licenseren en implementeren. Waar de Office 2019-applicatie een device based licentiestructuur kent die op de RDS manier via een MSI package wordt geïnstalleerd, werkt Microsoft 365 Apps for Enterprise via een user based-abonnement en de implementatiemethode is wezenlijk anders.	Ja
Office Online	Online versie van Microsoft 365 Apps for Enterprise welk volledig in de webbrowser wordt uitgevoerd. Er is geen lokale installatie nodig.	Ja
SharePoint Online	Organisaties gebruiken SharePoint voor het maken van websites. SharePoint is een veilige locatie voor het opslaan, organiseren, delen en gebruiken van informatie vanaf elk apparaat. U hebt alleen een webbrowser nodig.	Ja
Exchange Online	Exchange Online is de Cloud e-maildienst. Met Exchange Online krijgt u toegang tot e-mails, agenda's en contactpersonen en dit op alle mogelijke soorten toestellen (desktop, laptop, tablet of mobiele telefoon).	Ja
OneDrive for Business	OneDrive for Business biedt een locatie in de Cloud waar u uw werkbestanden kunt opslaan, delen en synchroniseren. U kunt	Ja

	met OneDrive voor Bedrijven uw bestanden vanaf elk apparaat bijwerken en delen. U kunt ook gelijktijdig met anderen aan Office-documenten werken.	
Whiteboard	Microsoft Whiteboard is een digitaal canvas met vrije vormen, waar personen, inhoud en ideeën samenkomen. U kunt whiteboard gebruiken om samen te werken met uw team om verschillende activiteiten uit te voeren.	Ja

6.1.1 Microsoft 365 platform updates

Er worden met regelmaat nieuwe functies en service-updates doorgevoerd op Office 365. Hiervoor is geen vast release schema gedefinieerd. Wel heeft gemeente Midden-Delfland grip op volgorde waarop deze verbeteringen worden doorgevoerd voor haar medewerkers. De mogelijkheden staan hieronder opgesomd.

Standard release: Ontvang updates wanneer deze algemeen beschikbaar worden.

Targeted release voor iedereen: Vroege updates ontvangen voor uw hele organisatie

Targeted release voor geselecteerde gebruikers: Kies personen om voorbeelden van updates te bekijken, zodat uw organisatie is voorbereid.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
1	De release-voorkeur staat ingesteld op: Targeted release voor geselecteerde gebruikers.	Door een specifieke selectie van gemeente Midden-Delfland medewerkers eerder te voorzien van nieuwe functies en service-updates worden mogelijke productie verstoringen voor gemeente Midden-Delfland tijdig gesignaleerd.

Microsoft 365 apps for Enterprise wordt geleverd via het internet. Om hiervan gebruik te maken dient het moderne werkplek apparaat toegang te hebben tot internet. Microsoft heeft alle URL's en IP adressen waarop ze haar Office 365 diensten levert gepubliceerd op de website <http://aka.ms/o365ip>. Voor een goede werking van cloud diensten dienen deze URL's ongehinderd (maar wel gemonitord) vanaf het interne netwerk naar het Microsoft platform verbinding te kunnen leggen.

Deze URL's en IP adressen muteren met regelmaat en het verdient aanbeveling om niet op IP adressen te filteren maar op URL niveau voor zover dit mogelijk is.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
---	---------------	-----------

2	Alle MW apparaten op het interne gemeente Midden-Delfland netwerk hebben toegang tot alle URL's en IP adressen zoals beschreven op de website: https://aka.ms/0365ip .	Toegang tot Office 365 URL's en IP adressen zijn randvoorwaardelijk voor een goede werking van de Microsoft cloud oplossingen.
---	---	--

6.1.2 Microsoft 365 Apps for Enterprise

Microsoft 365 Apps for Enterprise is een component uit de door gemeente Midden-Delfland afgenomen Microsoft 365 E3 suite en is een volledige Office-versie die gebruikers kunnen downloaden en lokaal installeren. Deze cloud-variant van Office is vergelijkbaar met de laatste Office versie die on-premises beschikbaar is.

Microsoft levert maandelijks feature updates voor Microsoft 365 Apps for Enterprise. Via de Microsoft 365 Apps for Enterprise update channels worden de feature updates per groep medewerkers verspreid.

Microsoft 365 Apps for Enterprise omvat de navolgende componenten.

- Access
- Excel
- OneDrive for Business (Next Gen Sync Client)
- Outlook
- OneNote
- PowerPoint
- Publisher
- Teams
- Word

Elke gebruiker binnen de Office 365 tenant welke is voorzien van een Microsoft 365 E3 licentie, heeft recht om Microsoft 365 Apps for Enterprise te gebruiken. Per gebruikerslicentie mag Microsoft 365 Apps for Enterprise 5x geactiveerd worden.

- Microsoft 365 Apps for Enterprise wordt door Microsoft Intune met de navolgende parameters geïnstalleerd op de moderne werkplek.

Component	Instelling
Access	Uit
Excel	Aan
OneDrive for Business (Groove)	Uit
OneDrive for Business (Next Gen Sync Client)	Aan
OneNote	Aan
Outlook	Aan
PowerPoint	Aan

Publisher	Aan
Skype for Business	Uit
Teams	Aan
Word	Aan
Office versie	64-bit
Update Channel	Monthly Enterprise Channel (voor alle werkplekken) / (Current channel Preview voor de pilot/beheer groep)
Automatically accept the app end user license agreement	Ja
Use shared computer activation	Ja (voor Citrix) Nee voor full clients
Language	Nederlands (NL-NL) en English (EN-US)

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
3	Microsoft 365 Apps for Enterprise wordt standaard geïnstalleerd op de moderne werkplek.	Microsoft 365 Apps for Enterprise behoort nu al tot de basis set van applicaties die dagelijks door alle medewerkers wordt ingezet.

Impact van Microsoft 365 Apps for Enterprise (M365 AfE) uitrol

Tijdens de workshop is specifiek gesproken over de impact van de inzet van Microsoft 365 Apps for Enterprise ten opzichte van de huidige Office 2016 omgeving. Op basis van de huidige werkplek zal de verandering voor eindgebruikers nagenoeg onzichtbaar zijn, omdat Office 2016 en M365 AfE qua gebruikersinterface gelijk is (zelfde ribbon bijvoorbeeld). Ook gebruikte VBA macro's en add-ins zullen voor 99% compatible zijn. Eventueel heeft Microsoft een [toolkit](#) gepubliceerd waarmee dit geverifieerd kan worden indien dit wenselijk is.

De echte impact is op beheer niveau waar het verschil in licensering en beheertaken naar voren zal komen. Het kiezen van een release ring zorgt ervoor dat het IT beheer team naar verwachting vaker een update moet installeren op bijvoorbeeld de Citrix images. Daar staat tegenover dat hiermee de veiligheid verhoogd wordt en gebruikers sneller kunnen beschikken over nieuwe functies.

6.1.3 Office Online

Office Online is een component uit de Office 365 suite en bestaat uit de applicaties Word Online, Excel Online, PowerPoint Online en OneNote Online. Deze applicaties worden ontsloten via de webbrowser.

Deze applicaties bevatten de basis functionaliteit ten opzichte van de desktopversie welke geleverd wordt vanuit Office 365 Pro Plus.

Office Online applicaties zijn niet in staat om macro's en scripts uit te voeren. Ook tref je geen 'opslaan' knop aan omdat alle mutaties direct worden weggeschreven in SharePoint Online of OneDrive for Business. Office Online kan geen bestanden opslaan of openen vanuit andere bronnen.

Office Online is ideaal voor medewerkers welke Office bestanden moeten bekijken of bewerken op een apparaat waar geen Office (Microsoft 365 Apps for Enterprise) op is geïnstalleerd.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
4	Office Online wordt aangeboden aan alle medewerkers	Office Online behoort tot de standaard uitrusting van de moderne werkplek en de uitgekozen methode van document verwerking vanaf werkplekken die buiten het beheer van gemeente Midden-Delfland vallen (bijvoorbeeld prive-PC's)

6.1.4 SharePoint Online

Microsoft SharePoint Online is een component uit de Office 365 suite en biedt een samenwerkingsplatform waarin bestanden zoals project- en afdelingsbestanden kunnen worden opgeslagen en gedeeld.

De reden voor inschakelen is de inzet van OneDrive for Business. OneDrive for Business is gebouwd op SharePoint Online waardoor het noodzakelijk is om SharePoint Online in te schakelen om gebruik te kunnen maken van OneDrive for Business.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
5	SharePoint Online is ingeschakeld, wordt veelvuldig gebruikt.	Het inschakelen van SharePoint Online is nodig voor het gebruik van Teams en OneDrive for Business.

6.1.5 OneDrive for Business

Microsoft OneDrive for Business is een component uit de Office 365 suite welke wordt ingezet voor de opslag van persoonlijke bestanden. OneDrive for Business levert standaard maximaal 1 TB opslagruimte per medewerker. Dit is op te hogen naar maximaal 5 TB per medewerker en via MS support nog hoger afhankelijk van de aangekochte licentie vorm (M365 E3 is aangemerkt als onbeperkt) d.w.z. er kan onbeperkt via support om verhoging worden gevraagd.

OneDrive for Business maakt in de achtergrond gebruik van de SharePoint Online platform. Hierdoor is de gebruikers ervaring voor de medewerker tussen OneDrive for Business en SharePoint Online op een aantal punten (bijna) gelijk.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
6	OneDrive for Business is geïmplementeerd en wordt gebruikt voor alle persoonlijke opslag.	De inhoud van legacy home shares kan hierdoor verhuisd worden naar een cloud variant voor de opslag van persoonlijke data. OneDrive for Business biedt meer flexibiliteit en functies dan de legacy home shares.

6.1.6 Microsoft Exchange

Microsoft Exchange Online is een component uit de Office 365 suite. Het is mogelijk om hiervan gebruik te maken en een gedeelte van, of alle postbussen te migreren van de on-premises Exchange infrastructuur naar Exchange Online.

Om een migratie naar Exchange Online mogelijk te maken is een Hybride Exchange infrastructuur benodigd. Met behulp van de Hybride Exchange technologie wordt de bestaande on-premises Exchange organisatie en Exchange Online samengesmolten tot één virtuele Exchange organisatie welke vrijwel geheel transparant werkt voor de gebruiker.

Een Hybride Exchange infrastructuur kan gevormd worden met behulp van Exchange 2010, Exchange 2013, Exchange 2016 en Exchange 2019. In alle gevallen is het verplicht om te voldoen aan het N-1 patch beleid. Indien er geen postbussen staan op de on-premises Exchange server waarmee de Hybride koppeling is gerealiseerd, dan is deze Exchange Server licentie gratis (m.u.v. Exchange 2019). Dit wordt een Hybride Exchange licentie genoemd.

Het is verplicht om een Hybride Exchange server te hebben geïmplementeerd indien er gebruik gemaakt wordt van Azure AD Connect.

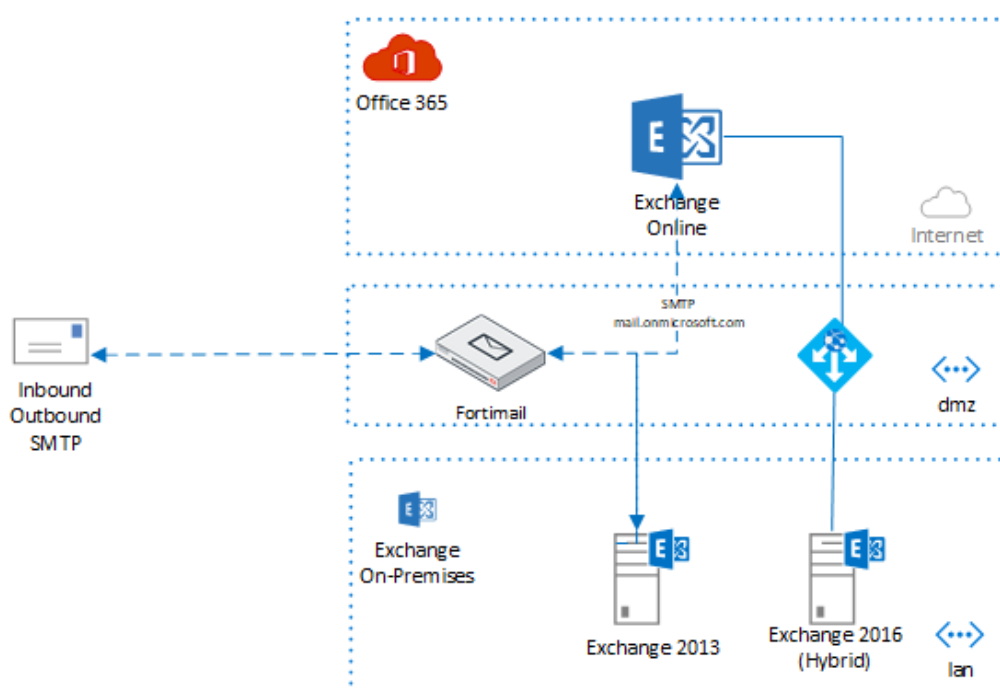
Microsoft staat niet toe om een 3rd party e-mail toepassing te plaatsen tussen Exchange on-premises en Exchange Online. Indien het noodzakelijk is om al het verkeer via het Perimeter netwerk te routeren dan is de Edge Transport server de enige oplossing voor SMTP verkeer. Voor EWS, ActiveSync, OWA, etc. (HTTPS)

dient een reverse proxy oplossing in het Perimeter netwerk gebruikt te worden. Hiervoor kan de Microsoft Web Application Proxy (WAP) ingezet worden. De WAP servers vereisen een load balancer voor een redundante implementatie.

Indien er gebruik gemaakt wordt van Outlook, dan moet de gebruikte Outlook versie in mainstream support zijn. Op het moment van schrijven betreft dit Outlook 2016, Outlook 2019 en Outlook 365.

Omdat alle Outlook clients een directe connectie opbouwen naar Office 365 is het noodzakelijk dat er een betrouwbare en robuuste netwerk en internetverbinding aanwezig is. Voor de optimalisatie hiervan adviseert Microsoft om SSL-inspectie op de firewall uit te schakelen voor alle Office 365 diensten. Daarnaast heeft het de voorkeur om geen forward proxy oplossing in-lijn te hebben.

Architectuur tekening mailflow



Ontwerp keuzes:

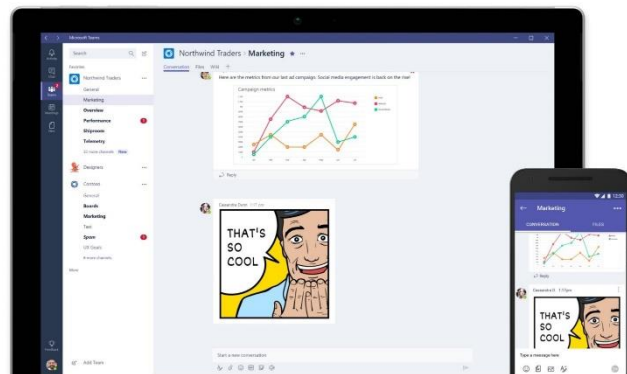
#	Ontwerp keuze	Motivatie
7	Er is een Hybride Exchange implementatie	gemeente Midden-Delfland heeft reeds alle postbussen gemigreerd naar Exchange Online. Omdat er ook gebruik gemaakt wordt van Azure AD Connect is het verplicht om een Hybride Exchange omgeving te implementeren.
8	Exchange 2016 wordt ingezet als Hybride Exchange Server	gemeente Midden-Delfland beschikt reeds over een Exchange 2016 infrastructuur.

9	Fortimail wordt ingezet als anti-spam/virus appliance tot verloop van het contract waarna EOP zal voor vervanging zal zorgen	gemeente Midden-Delfland heeft besloten om na de looptijd van het contract de Fortimail niet te verlengen en de functionaliteit te betrekken uit de Microsoft diensten Exchange Online Protection (EOP) en Defender for O365 (voormalig ATP)
10	Er wordt een reverse proxy ingezet in het Perimeter netwerk.	Inzet van een reverse proxy in het Perimeter netwerk is verplicht conform beleid gemeente Midden-Delfland.
11	Er vindt geen SSL-inspectie plaats voor verkeer naar Microsoft 365	Het uitzetten van SSL-inspectie bevordert de performance.
12	Er is geen forward proxy geïmplementeerd voor al het verkeer naar Office 365	Het uitzetten van de forward proxy bevordert de performance.

6.1.7 Microsoft Teams

Microsoft Teams is een applicatie waarin verschillende functionaliteiten samenkomen met als primair doel effectiever samenwerken.

Middels Microsoft Teams hebben gebruikers beter contact en zijn ze productiever. Gebruikers beschikken over de benodigde inzichten en tools om effectiever te communiceren en samen te werken.



Gecentraliseerde communicatie en samenwerking

- › **Communiceer effectiever**
Zorg ervoor dat jouw teams optimaal samenwerken met group chat, online vergaderingen, telefoneren en web conferencing.
- › **Werk beter samen**
Deel bestanden met ingebouwde Office 365-applicaties zoals Word, Excel, PowerPoint en SharePoint.
- › **Pas jouw werkplek aan**
Voeg jouw favoriete Microsoft-applicaties en diensten van derden toe om zakelijke vooruitgang te blijven boeken.

- › **Houd jouw team veilig**
Zorg voor end-to-end beveiliging, administratieve controle en conformiteit — alles mogelijk gemaakt door Office 365.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
13	Inzet van Microsoft Teams als primaire teleconferentie, chat en collaboratie applicatie.	Binnen de gemeente Midden-Delfland organisatie wordt veelvuldig gebruik gemaakt van Microsoft Teams, hierin komt geen verandering. Wel zal worden gekeken naar de instellingen en veiligheid rondom de inzet van MS Teams binnen de gemeente Midden-Delfland.
14	Teams telefonie integratie wordt (nog) niet opgezet	Er is tijdens de workshops gesproken over telefonie en het wisselen tussen de bestaande oplossing en Microsoft Teams, deze functionaliteit zal verder niet binnen dit document behandeld worden gezien er een separaat traject loopt binnen de gemeente Midden-Delfland.

6.2 Microsoft Endpoint Manager

Microsoft Endpoint Manager is de Microsoft oplossing voor het managen van alle devices. Microsoft Endpoint Manager bestaat uit de onderstaande Microsoft management oplossingen.

- › Microsoft Intune
- › Autopilot
- › Configuration Manager
- › Desktop analytics
- › Microsoft Defender for Endpoints

6.2.1 Intune

Intune is een clouddienst voor het beheren van bedrijfsmobiliteit (Enterprise Mobility Management, EMM) die medewerkers in staat stelt om productief te zijn terwijl zakelijke gegevens veilig blijven. Met Intune is het navolgende mogelijk:

- › De mobiele apparaten beheren die door medewerkers worden gebruikt voor toegang tot bedrijfsgegevens.
- › De mobiele apps beheren waarvan uw medewerkers gebruikmaken.
- › Bedrijfsgegevens beschermen door te bepalen hoe medewerkers toegang hebben tot de gegevens en deze delen.
- › Garanderen dat apparaten en apps compatibel zijn met de beveiligingsvereisten van het bedrijf.

Intune is nog niet geïmplementeerd en momenteel wordt Mobile Iron ingezet voor het beheren en beveiligen van alle mobile devices. Daarnaast is er met Ivanti software voor Windows clients een configuratie en beveiligingsbeleid gemaakt en wordt daarmee gecontroleerd op de naleving hiervan.

Voor de gemeente Midden-Delfland betekent de inzet van Intune effectief dat alle mobiele apparaten unmanaged devices kunnen zijn en deze met MAM zullen werken. Managed devices zoals laptops kunnen ook opgenomen worden in het Intune beheer.

Intune kan apparaten beheren met de navolgende besturingssystemen: Windows 7, 8, 10, 11 iOS, MacOS en Android.

Het is mogelijk om Intune te integreren met System Center Configuration Manager (SCCM), dit biedt voordelen aan organisaties die hun bestaande werkplek reeds beheren met SCCM. Met een hybride koppeling tussen SCCM en Intune kan per component het beheer overgeheveld worden naar Intune.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
15	Gemeente Midden-Delfland heeft aangegeven om begin volgend jaar de overstap te maken naar Microsoft Intune.	Intune is het standaard cloud Enterprise Mobility Management EMM platform van Microsoft en zit in scope van de moderne werkplek. Inrichting van voor de werkplekken (full-client) is ten tijde van het schrijven van dit document nog niet gebeurd maar al wel gepland.

6.2.2 AutoPilot

Voordat een apparaat (computer) beheerd kan worden door Microsoft Intune is het noodzakelijk om het apparaat in te schrijven in Microsoft Intune.

Microsoft Intune – Device Enrollment beleid bepaalt de restricties omtrent het inschrijven van apparaten in de tenant.

Het inschrijven van een moderne werkplek computers zal door de gebruiker zelf plaats vinden. Het voordeel hiervan is dat nieuwe computers zonder interactie direct aan de eindgebruiker overhandigd kunnen worden.

De hardware leverancier zal gegevens van de computer (hardware hash) vooraf aanleveren of invoeren in het Windows AutoPilot programma. Op basis hiervan krijgt de gebruiker een zou eenvoudig mogelijke uitrol ervaring.

6.2.2.1 Enrollment Restrictions

De Moderne Werkplek is gebaseerd op Windows 10.

Standaard is het binnen Azure AD en Microsoft Intune voor elke gebruiker mogelijk om nieuwe apparaten in te schrijven. Dit geldt voor Windows (10/11) maar ook Android, iOS en MacOS apparaten.

Om eventueel misbruik te voorkomen is het binnen gemeente Midden-Delfland verplicht om Azure MFA af te dwingen tijdens het inschrijven van een nieuw apparaat.

Gemeente Midden-Delfland zal ook Android en iOS apparaten ondersteunen. Hiervoor is het wel van belang dat gebruikers zelf het apparaat kunnen registreren & de-registreren.

6.2.2.2 Lokale beheerders

Nadat De Moderne Werkplek is geïnstalleerd zal de gebruiker welke de inschrijving heeft uitgevoerd automatisch lokale beheerder rechten ontvangen op Windows 10.

Vanuit het oogpunt voor (uitzonderlijk) lokaal Windows 10 beheer wordt voor elke moderne werkplek computer ook lokale beheerdersrechten (Windows 10 local Administrator) gegeven aan bepaalde beheerders.

Het is niet mogelijk om deze rechten uit te delen op basis van groepslidmaatschap. Daarnaast zijn Global Administrators automatisch lokale beheerder op alle MW computers.

6.2.2.3 Device Compliance

Microsoft Intune Device Compliance beleid stelt de organisatie in staat om te controleren of een apparaat voldoet aan bepaalde eisen. De resultaten van deze controle worden gerapporteerd aan Microsoft Intune en op basis hiervan kunnen er maatregelen getroffen worden.

Microsoft Intune kan bijvoorbeeld controleren of er een bepaalde Windows 10 Feature Update is geïnstalleerd of dat BitLocker aan staat.

6.2.2.4 Device Configuration

Microsoft Intune Device Configuration beleid stelt de organisatie in staat om instellingen en features van het OS op het apparaat te beheren.

De Moderne Werkplek maakt gebruik Windows 10 Device Configuration beleid en wordt in overleg geïmplementeerd.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
16	Autopilot zal worden ingezet voor de uitrol van de full-client werkplekken	Het beheer van Windows gebaseerde werkplekken kan worden uitgevoerd met Microsoft Intune. Onderdeel hiervan is het Autopilot installatie principe welke met de Out-of-the-box installatie direct contact zoekt met de eigen tenant en de noodzakelijke configuratie aanpassingen maakt.

6.2.3 Microsoft Endpoint Configuration Manager

Microsoft Endpoint Configuration Manager (voormalig System Center Configuration Manager SCCM) is vanaf versie 1910 onderdeel van Microsoft Endpoint Manager.

6.2.4 Desktop Analytics

Desktop Analytics is een op cloud gebaseerde dienst die integreert met Configuration Manager. De dienst biedt u inzicht en intelligentie om beter geïnformeerde beslissingen te nemen over de updategereedheid van uw Windows-clients. Het combineert gegevens van uw organisatie met gegevens die zijn geaggregeerd vanaf miljoenen apparaten die zijn aangesloten op Microsoft cloud diensten.

Met Desktop Analytics in combinatie met Configuration manager is het mogelijk om een inventarisatie te draaien van apps die in de organisatie draaien, om deze vervolgens te controleren op compatibiliteit in combinatie met Windows 10 feature updates. Kwetsbaarheden en eventuele andere problemen worden op voorhand geïdentificeerd, op basis van suggesties worden mogelijke oplossingen aangedragen.

Van vitaal belang voor het beheer team is dat hierin een dashboard in Azure wordt verzorgd welke belangrijke informatie weergeeft.

7 Infrastructuur

Het hoofdstuk infrastructuur is bedoeld voor het geven van inzicht voor de ontwerpkeuzes van de gemeente Midden-Delfland met betrekking tot Microsoft 365 moderne werkplek ontwerp.

7.1 Endpoints

De (fysieke) endpoints waarop de (remote) applicaties beschikbaar kunnen worden gesteld worden hier toegelicht. De Laptop Endpoints dienen een één-op-één relatie te hebben met een medewerker.

ThinClient: De ThinClient computer wordt ingezet als ontsluiting voor SBC of VDI infrastructuur.

Laptop: De laptop computer kan plaats onafhankelijk worden ingezet voor het uitvoeren van lokale applicaties of kan als ontsluiting dienen tot de SBC of VDI infrastructuur.

Mobiele apparaten: Mobiele apparaten (smartphones, tablets, etc.) kunnen plaats onafhankelijk worden ingezet voor het gebruik van Apps. Deze Apps bieden toegang tot de gemeente Midden-Delfland (cloud) resources.

#	Ontwerp keuze	Motivatie
17	gemeente Midden-Delfland heeft reeds een aankoop gepland van full-client laptops, deze zullen als moderne werkplek worden ingezet.	De ThinClient zal voor de korte termijn ingezet worden als standaard werkplek. De full-client laptops worden gefaseerd uitgerold om meer performance te kunnen bieden aan moderne applicaties zoals Microsoft Teams.

7.2 Identiteit

Identiteit vormt het fundament van elke werkplek. In een on-premises infrastructuur wordt deze dienst geleverd door Active Directory. Hierin zijn alle gebruikersaccounts inclusief wachtwoorden, maar ook groepen en computers opgeslagen. Microsoft Cloud oplossingen maken gebruik van de Azure Active Directory voor alle identiteit diensten.

Voor gemeente Midden-Delfland moet speciale zorg worden gedaan voor non-organisatie identiteiten zoals gast accounts of cloud-only accounts omdat voor deze groep diensten geleverd moeten worden voor de uitvoering van taken binnen de organisatie.

Om ervoor te zorgen dat identiteiten (accounts en groepen) in zowel Active Directory als Azure Active Directory gelijk zijn dient Azure AD Connect te worden ingezet.

Deze tool synchroniseert (een selectie van) OU's van Active Directory naar Azure Active Directory. Azure AD Connect synchroniseert alle objecten 1x per 30 minuten en kent geen implementatie mogelijkheid op basis van hoge beschikbaarheid. Indien deze tool niet meer functioneert blijven alle reeds gesynchroniseerde

objecten in Azure AD behouden, maar is het niet meer mogelijk om mutaties te synchroniseren naar Azure AD.

Voor het geval van calamiteiten (disaster recovery) is het mogelijk om een tweede Azure AD Connect server te installeren in Staging mode. Deze server heeft een exact gelijke configuratie als de primaire Azure AD Connect server, maar fungeert in een read-only mode. Indien er zich een calamiteit voor doet en de primaire Azure AD Connect server is definitief niet meer beschikbaar dan kan de Staging server eenvoudig omgezet worden tot nieuwe primaire Azure AD Connect server.

Azure AD gebruikt een inlognaam in de vorm van gebruiker@domein.tld. Microsoft gebruikt het User Principal Name (UPN) attribuut uit Active Directory als inlognaam voor Azure AD.

Dit heeft als gevolg dat de UPN van elk object moet voldoen aan de richtlijnen voor een inlognaam in Azure AD.

Om de integratie met Exchange Online makkelijk te maken en alle klanten een voorspelbare login ervaring te kunnen geven adviseert Microsoft om de navolgende spelregel te hanteren voor deze diensten.

- › UPN is gelijk aan het primaire e-mailadres van de gebruiker.

Naast het synchroniseren van identiteiten moet er ook een methode voor het authenticeren van deze identiteiten gekozen worden. Hiervoor heeft Microsoft drie verschillende methodes ontwikkelt. Deze staan opgesomd in de navolgende tabel.

Voor niet gesynchroniseerde cloud gebruikers zal voorziening worden getroffen tijdens de inrichting zodat deze kunnen blijven werken zoals dat in de huidige situatie ook geldt.

Methode	Toelichting	Voordeel	Nadeel
Password Hash Sync	Wachtwoord hash wordt door Azure AD Connect samen met het gebruikersaccount van Active Directory naar Azure Active Directory gesynchroniseerd. Het wachtwoord hash is in Azure Active Directory geencrypt opgeslagen.	<p>Zeer eenvoudig</p> <p>Robuust, het authenticatie proces is niet afhankelijk van on-premises infrastructuur</p>	<p>Het wachtwoord hash staat (geencrypt) in Azure Active Directory</p> <p>Werkt alleen voor Office 2013 of hoger.</p>
Pass-through Authentication	Er wordt op één of meerdere on-premises servers de PTA agent geïnstalleerd. Deze agent bouwt een connectie op met Azure AD. Alle authenticatie verzoeken worden vanuit Azure AD doorgestuurd naar de PTA Agent. De PTA Agent stuurt authenticatie verzoeken door naar Active Directory	<p>Eenvoudig</p> <p>Automatische load balancing door meerdere agents te installeren.</p> <p>Het wachtwoord hash staat niet in Azure AD</p>	<p>Afhankelijk van on-premises infrastructuur voor authenticatie proces.</p> <p>Werkt alleen voor Office 2013 of hoger.</p>
AD FS	Er wordt een AD FS server en WAP server geïnstalleerd in de on-premises	Werkt voor Office 2010 of hoger.	Afhankelijk van on-premises infrastructuur

	<p>infrastructuur. WAP wordt op internet gepubliceerd.</p> <p>Azure AD zal alle authenticatie verzoeken doorsturen naar WAP. WAP stuurt authenticatie verzoek door naar AD FS. AD FS stuurt authenticatie verzoek door naar Active Directory</p>	<p>Het wachtwoord hash staat niet in Azure AD</p> <p>3rd party SaaS leveranciers kunnen hiervan ook gebruik maken.</p>	<p>voor authenticatie proces.</p> <p>Complex</p> <p>SSL-certificaat nodig</p> <p>Load balancer nodig voor redundante implementatie.</p>
--	--	--	---

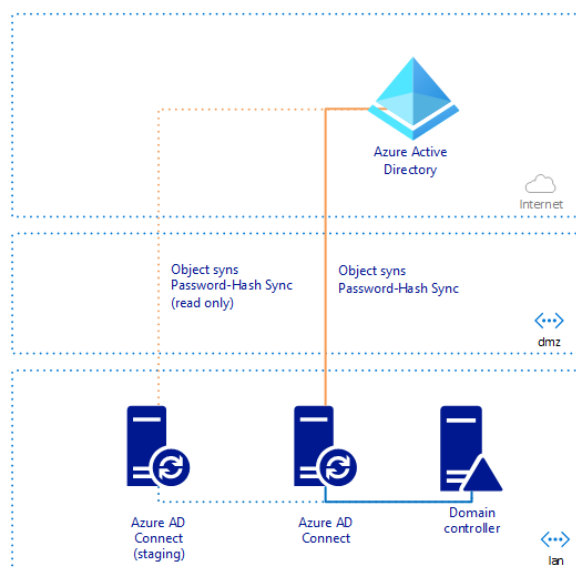
Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
18	Azure AD Connect is geïmplementeerd.	Azure AD Connect is geïmplementeerd om ervoor te zorgen dat alle identiteiten slechts eenmaal in Active Directory aangemaakt en beheerd moeten worden.
19	Naast de primaire Azure AD Connect server word op termijn ook een staging server geïmplementeerd.	De Azure AD Connect Staging server maakt het mogelijk om tijdens calamiteiten snel en gecontroleerd een nieuwe Azure AD Connect server in te zetten. Hierdoor heeft de gemeente Midden-Delfland tijd vrij voor andere taken tijdens de calamiteit.
20	Alle relevante OU's zijn/worden gesynchroniseerd naar Azure AD.	Alleen OU's met daarin accounts, contacten en groepen welke ingezet worden in Office 365 en Intune worden gesynchroniseerd. On-premises beheer en serviceaccounts worden niet gesynchroniseerd.
21	De UPN van alle gebruikers objecten is gelijk aan het primaire e-mailadres van de gebruiker.	Hiermee wordt voldaan aan Microsoft best practice en wordt de best mogelijke gebruikers ervaring geleverd.
22	Password-Hash Authenticatie methode is geïmplementeerd.	Password-Hash Synchronisatie is een meest eenvoudige en robuuste methode voor authenticatie. Deze methode van authenticatie zal worden ingezet ter vervanging van AD FS.

23	Er moet een 'break glass' account aanwezig zijn. Dit is een cloud-only account.	In geval van calamiteiten kan met dit account altijd volledige toegang tot de tenant verkregen worden. Dit account is niet bedoeld voor dagelijks beheer en zal op een veilige plek in bewaring worden genomen (bijvoorbeeld een kluis).
----	---	--

Architectuur tekening

In de onderstaande tekening zijn twee servers met Azure AD Connect weergegeven.



7.3 Enterprise applicaties

Enterprise Applicaties binnen de Azure AD biedt de mogelijkheid om autorisatie te verzorgen voor eindgebruikers op een andere methode dan middels AD FS waar momenteel gebruik van wordt gemaakt. Door inzet van de Azure AD en Enterprise Applicaties melden gebruikers zich eenmaal aan voor een veilige en naadloze toegang tot deze toepassingen. Applicaties en de aanmelding op applicaties zijn middels Conditional Access en MFA beter te beveiligen. Vanuit dezelfde portal zijn er veel meer inzichten in het gebruik, of misbruik, van de applicaties.

Een voorbeeld van de voor gemeente Midden-Delfland belangrijkste applicaties welke AD FS gebruiken is hieronder benoemd.

- › JIM Social Intranet
- › SmartDocuments Web
- › Zaaksysteem.nl

Per applicatie kan bepaald worden of MFA wordt ingeschakeld, die gebeurt op basis van conditional access. Dit zal altijd in overleg moeten gaan de applicatieleverancier.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
24	Applicaties worden opgenomen als Enterprise applicaties	Applicaties worden centraal beheerd, beveiligd en gemonitord vanuit de cloud
25	MFA wordt voor alle applicaties ingeschakeld	Voor een betere beveiliging wordt geadviseerd om MFA voor alle applicaties in te schakelen.
26	Elke gebruiker te voorzien van een Azure AD Premium P1 licentie.	Azure AD Premium P1 licentie is benodigd om Enterprise apps te mogen gebruiken. Azure AD Premium P1 is een onderdeel van de EM+S E3 suite dat daarbij onderdeel is van Microsoft 365 E3/E5.

7.4 Multi Factor Authenticatie

Standaard wordt voor het authenticatie proces van elke gebruiker één verificatie stap gebruikt, namelijk de combinatie van gebruikersnaam en wachtwoord. Deze verificatie stap is erg kwetsbaar doordat medewerkers wachtwoorden hergebruiken, ergens noteren of slechte wachtwoorden kiezen. Deze verificatie stap is niet meer van deze tijd en door veel leveranciers, waaronder Microsoft, wordt geadviseerd om hiervan af te stappen. Alternatief voor het wachtwoord is een biometrische verificatie stap waarbij bijvoorbeeld een irisscan of gezichtsherkenning wordt toegepast. Deze mag voor mobiele apparaten worden ingezet binnen gemeente Midden-Delfland.

Op dit moment ondersteunt veel hardware en software deze verificatie methode nog niet. Waardoor het op dit moment beste keuze is om een tweede verificatie stap toe te voegen aan het wachtwoord.

Dit wordt Multi-Factor Authentication (MFA) genoemd.

Het authenticatie proces van de gebruiker ziet er dan als volgt uit.

- › Stap 1: Gebruikersnaam en wachtwoord (iets wat je weet)
- › Stap 2: SMS / Telefoonoproep / Push notificatie op Microsoft Authenticator App (iets wat je hebt)

Microsoft levert een MFA Clouddienst genaamd Azure MFA. Azure MFA is toepasbaar op de volgende systemen.

- › Microsoft Cloud Apps (Office 365): werken rechtstreeks met Azure MFA
- › On-Premises App (VPN, Citrix, NetScaler, Ivanti) werken via een NPS server of MFA Server.

Het gebruik van Azure MFA vereist minimaal een Azure AD Premium P1 licentie per gebruiker.

Om Azure MFA toe te passen op Microsoft Cloud Apps is geen extra server benodigd. Voor de implementatie van Azure MFA op On-Premises Apps is een on-premises Microsoft Network Policy Server (NPS) benodigd. Deze NPS server wordt voorzien van de Azure MFA Extensie om aan te sluiten op de Azure MFA omgeving.

De koppeling tussen de On-Premises App en de NPS server vindt plaats op basis van het RADIUS protocol.

De Microsoft NPS server kent geen clustering mogelijkheid voor redundantie. Er zijn twee methodes om NPS hoog beschikbaar aan te bieden.

- › Twee NPS servers ontsluiten via een load balancer.
- › Twee NPS servers opgeven als RADIUS server in de On-Premises App. De applicatie zorgt hierbij zelf voor load balancing.

Een gevolg van de keuze voor de NPS server i.c.m. Azure MFA is dat alleen een telefoonoproep en de Microsoft Authenticator Push Notificatie verificatie opties worden ondersteund.

Azure MFA kent een aantal generieke configuratie opties die het gedrag voor de gebruiker bepalen. Hieronder staat een overzicht van de opties en een toelichting.

Custom Voice Message:

Bij een telefoonoproep heeft Microsoft de teksten ingesproken. Indien gewenst is het mogelijk om zelf teksten in te spreken in de huisstijl van de gemeente Midden-Delfland .

Trusted IP:

Trusted IP stelt gemeente Midden-Delfland in staat om altijd de tweede verificatiestap te omzeilen indien een authenticatie verzoek komt van een specifiek publiek IP-adres.

App Passwords:

Sommige (vaak oudere) applicaties kunnen met maar één verificatiestap omgaan. Indien Azure MFA wordt ingeschakeld voor een gebruiker die gebruik maakt van deze legacy applicaties is het niet meer mogelijk om van deze legacy applicaties gebruik te maken.

Om dit te omzeilen, en toch een twee verificatiestap aan te kunnen bieden heeft Microsoft App Passwords geïntroduceerd.

Een App Password is een éénmalig, willekeurig gegenereerd wachtwoord van 16 karakters. Dit wachtwoord kan worden ingezet voor legacy applicaties.

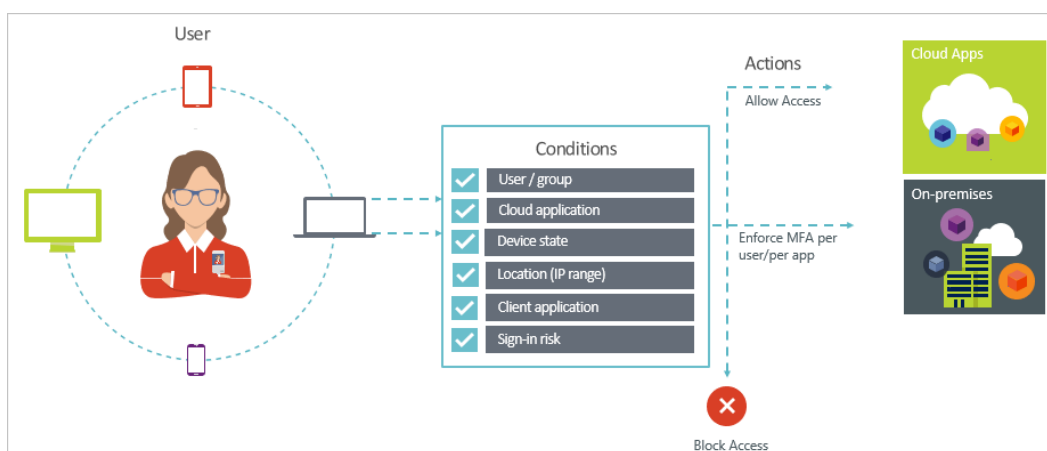
Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
27	Azure MFA wordt ingeschakeld voor alle gebruikers, inclusief externe leveranciers.	gemeente Midden-Delfland beleid vereist dat elk account is voorzien van een tweede verificatie methode. En gebruikt hiervoor reeds Azure MFA
28	Elke gebruiker is voorzien van een Azure AD Premium P1 licentie.	Azure AD Premium P1 licentie is benodigd om Azure MFA te mogen gebruiken. Azure AD Premium P1 is een onderdeel van de EM+S E3 suite of de Microsoft M365 E3/5 licenties.
29	De aangeboden verificatie methodes zijn telefoonoproep en Microsoft Authenticator App push notificatie	Alleen telefoonoproep en de Microsoft Authenticator push notificatie worden ondersteund door de NPS server.
30	Self-Service Password Reset (SSPR) zal worden ingezet om wachtwoorden in de cloud te laten herstellen.	SSPR heeft als voordeel dat gebruikers zelf wachtwoorden in op het Microsoft platform kunnen veranderen, hiermee wordt de druk bij een ondersteuningsafdeling verlicht.
31	Fraude Alert notificatie is ingesteld op: EMAILADDRESS	Dit e-mail adres is conform de wens van de klant.
32	Custom Voice Message word niet ingeschakeld	De standaard Microsoft Voice Message is toereikend voor gemeente Midden-Delfland .

33	Trusted IP is niet ingeschakeld	Het omzeilen van Azure MFA op basis van Publieke IP is niet de wens van gemeente Midden-Delfland . Het omzeilen van Azure MFA dient te worden uitgevoerd op basis van een 'Trusted' device gemarkeerd door Intune. Dit wordt mogelijk gemaakt door een Conditional Access policy.
34	App Passwords zijn niet ingeschakeld	gemeente Midden-Delfland beleid vereist dat er alleen van moderne applicaties gebruik wordt gemaakt. Dit komt ook ten goede aan de gebruikers ervaring.

7.5 Conditional Access (CA)

Conditional Access (CA) is een functie van Azure AD. Met deze oplossing is het mogelijk om gedetailleerd toegangsbeheer te configureren met behulp van een voorwaardelijk toegangsbeleid om bedrijfsgegevens van de organisatie te beveiligen, terwijl eindgebruikers de mogelijkheid wordt geboden om op elk apparaat en op elke locatie optimaal te presteren. Door middel van een voorwaardelijk toegangsbeleid kunnen voorwaarden opgegeven worden die de toegang tot bedrijfsgegevens beperken op basis van de locatie, de apparaat- en gebruikersstatus en de gevoeligheid van een toepassing.



Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
35	Conditional access wordt geïmplementeerd.	Conditional access helpt bij het flexibel geven van toegang tot Microsoft cloud resources.
36	MFA wordt afgedwongen voor alle eindgebruikers welke zich buiten het netwerk van	Bij de inrichting van CA en de MFA policy voor eindgebruikers wordt gezorgd dat deze altijd ingesteld zijn wanneer er gewerkt wordt met het Microsoft platform buiten het gemeente Midden-Delfland netwerk.

	gemeente Midden-Delfland bevinden.	
37	MFA wordt altijd afgedwongen voor beheer rollen	Indien een account beschikt over beheer rollen zal deze gedwongen worden voor elke sessie een MFA actie te voltooien.
38	Compliant Intune Windows 10 apparaten hebben volledige toegang.	Dit zijn apparaten waar gemeente Midden-Delfland eigenaar van is.
39	Niet-compliant Intune apparaten hebben 'niet-download' toegang en vereisen Azure MFA.	Voorkomt dat informatie van gemeente Midden-Delfland (per abuis) opgeslagen wordt op apparaten die niet van gemeente Midden-Delfland
40	iOS en Android apparaten hebben alleen toegang via MAM.	gemeente Midden-Delfland wil alle iOS en Android apparaten beheren via MAM.
41	Legacy protocollen zijn niet toegestaan.	Conform Microsoft best practices wordt basic authenticatie niet toegestaan.

7.6 Company Branding

Company branding binnen Azure Active Directory zorgt ervoor dat de gemeente Midden-Delfland huisstijl aan de medewerker wordt getoond bij alle authenticatie pogingen op Microsoft Cloud diensten. Dit heeft als voordeel dat het de herkenbaarheid voor de medewerker vergroot.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
42	Company branding is geïmplementeerd.	Company branding verhoogd de herkenbaarheid voor de medewerker.

7.7 Role Based Access Control

Role Based Access Control (RBAC) stelt gemeente Midden-Delfland in staat om beter beveiligingsbeheer mogelijk te maken voor administratieve toegang tot componenten zoals Azure AD, Office 365 en Intune.

De administratieve toegang wordt verleend op basis van rollen. Een beheerder kan één of meerdere rollen hebben. Microsoft levert een standaard set aan rollen welke direct in gebruik genomen kunnen worden. Daarnaast is het voor sommige componenten ook mogelijk om nieuwe (aangepaste) rollen te definiëren.

Dankzij RBAC heeft een beheerder alleen administratieve toegang tot componenten welke nodig zijn voor de werkzaamheden.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
43	Role Based Access Control is geïmplementeerd voor de producten Azure, Intune, Exchange Online, SharePoint Online (OneDrive for Business) en Skype for Business Online	Administratieve rechten worden gekoppeld aan beheer rollen. Op deze manier heeft een beheerder alleen toegang tot de componenten welke nodig zijn om de werkzaamheden uit te voeren.

7.8 Privileged Identity management (PIM)

Privileged Identity Management (PIM) is een service in Azure AD waarmee een organisatie de toegang tot belangrijke resources in de organisatie kan beheren, controleren en bewaken. Deze resources omvatten resources in Azure AD, Azure en andere Microsoft Online Services zoals Microsoft 365 of Microsoft Intune.

Privileged Identity Management biedt op tijd gebaseerde en/of op goedkeuring gebaseerde rolactivering om de risico's van buitensporige, onnodige of misbruikte toegangsrechten voor resources te beperken. Hier zijn enkele van de belangrijkste kenmerken van Privileged Identity Management:

- › Just-in-time toegang bieden tot Azure AD- en Azure-resources;
- › Tijdgebonden toegang tot resources toewijzen met behulp van start- en einddata;
- › Goedkeuring vereisen om geprivilegieerde rollen te activeren;
- › Multi-factor authenticatie afdwingen om een beheer rol te activeren;
- › Gebruik motivering om te begrijpen waarom gebruikers de rol activeren;
- › Ontvang meldingen wanneer bevoorrechte rollen zijn geactiveerd;
- › Voer toegangsbeoordelingen uit om ervoor te zorgen dat gebruikers nog steeds rollen nodig hebben;
- › Download auditgeschiedenis voor interne of externe audit.

Om accounts met veel privileges beter te beschermen tegen kwaadwillenden en cyberaanvallen, kan Azure Active Directory Privileged Identity Management (PIM) worden gebruikt om de blootstellingstijd van

bevoegdheden te verlagen en de zichtbaarheid van het gebruik ervan te vergroten door middel van rapporten en waarschuwingen. PIM helpt bevoorrechte accounts te beschermen door just-in-time bevoorrechte toegang tot Azure AD- en Azure-resources te bieden. Toegang kan tijdgebonden zijn, waarna privileges automatisch worden ingetrokken.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
44	PIM is een gewenst onderdeel van binnen de Azure AD tenant, echter zal dit niet bij het moderne werkplek project worden geïmplementeerd	Administratieve rechten uitdelen op regels is een wens van de gemeente Midden-Delfland organisatie, echter tijdens de workshop is besproken dat deze implementatie eerst bij het IAM project zal worden getrokken en dus buiten het MW project valt.

7.9 Windows 10

Windows 10 werd voor het eerst uitgebracht in 2015 en is meest recente Microsoft besturingssysteem voor desktops, laptops, tablets, mobiele telefoons en IoT-apparaten (Internet of Things).

Windows 10 wordt geleverd met sterk verbeterde beveiligingsfuncties, een nieuwe browser en tal van functies om het werken productiever en efficiënter te maken.

Beveiligingsrisico's worden steeds belangrijker voor bedrijven. Windows 10 biedt volledig nieuwe methoden voor de beveiliging van systemen en gegevens. Het is ontwikkeld om gegevens, apparaten en identiteiten van de grootste en meest veeleisende bedrijven en overheden over de hele wereld te beschermen.

Windows 10 heeft ook een geïntegreerd verdedigingsmechanisme voor het beschermen van kritieke bedrijfsgegevens tegen indiscretie, diefstal en scheidt bedrijfsgegevens van persoonlijke gegevens.

Technologieën zoals Secure Boot en Device Guard en Credential Guard zorgen voor bescherming vanaf het inschakelen van uw apparaat tot het weer wordt uitgeschakeld.

Vóór Windows 10 bracht Microsoft om de paar jaar nieuwe versies van Windows uit. Dit traditionele implementatieschema legde gebruikers een trainingsbelasting op omdat de functierevisies vaak aanzienlijk waren. Het betekende ook lang wachten zonder nieuwe functies - een scenario dat niet werkt in de snel veranderende wereld van vandaag. Windows as a service levert twee keer per jaar kleinere functie-updates.

Het implementeren van Windows 10 is eenvoudiger dan bij eerdere versies van Windows. Wanneer u migreert van eerdere versies van Windows, kunt u eenvoudig een lokaal upgradeproces uitvoeren om alle apps, instellingen en gegevens automatisch te behouden. Nadat Windows 10 is uitgevoerd, is de implementatie van Windows 10 Feature Updates eenvoudig. Windows 10 is compatibel met de meeste hardware en software die op Windows 7 of later kunnen worden uitgevoerd. Vanwege deze hoge mate van compatibiliteit kan het testen van de app-compatibiliteit aanzienlijk worden vereenvoudigd.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
45	Windows 10 wordt geïnstalleerd op alle moderne werkplek apparaten.	Windows 10 is de huidige standaard in de markt en bij gemeente Midden-Delfland wanneer de full-clients beschikbaar komen zullen deze ook worden voorzien van Windows 10.

7.9.1 Installatie

Er zijn diverse installatie methodes mogelijk voor Windows 10 Pro.

- › Windows 10 Pro geleverd door hardware leverancier (OEM)
- › Installatie met OEM installatie media (USB-stick)
- › Light-Touch installatie met behulp van Microsoft Deployment Toolkit
- › Zero-Touch installatie met behulp van Microsoft System Center Configuration Manager (SCCM)

In alle gevallen is het advies om OEM (probeer) software te verwijderen. Dit resulteert in een uniforme inrichting van alle werkplekken. Indien nodig kan een computer opnieuw geïnstalleerd worden. Dit kan door de gebruiker zelf geïnitieerd worden, hiervoor zijn wel beheerdersrechten op de werkplek benodigd.

Een beheerder kan deze actie ook uitvoeren via de Intune Portaal.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
46	Windows 10 wordt uitgerold via een light touch installatie wanneer Autopilot niet mogelijk is.	De gemeente Midden-Delfland beschikt niet over een Microsoft deployment tool zoals SCCM. Uitrol van Windows 10 images gebeurt momenteel via VMware Horizon. Uitrol van nieuwe full-client werkplekken zal via autopilot plaats vinden. Voor de tussenfase is de meest praktische oplossing om MDT te gebruiken.

7.9.2 Windows 10 update

Windows 10 maakt gebruik het Windows as Service model en Windows Update for Business voor het gecontroleerd verspreiden van updates voor Windows 10.

Windows 10 krijgt twee keer per jaar, in maart en september een nieuwe Feature Update. In deze Feature Update implementeert Microsoft nieuwe mogelijkheden in Windows 10.

Elke Feature Update wordt voor 18 maanden ondersteund door Microsoft.

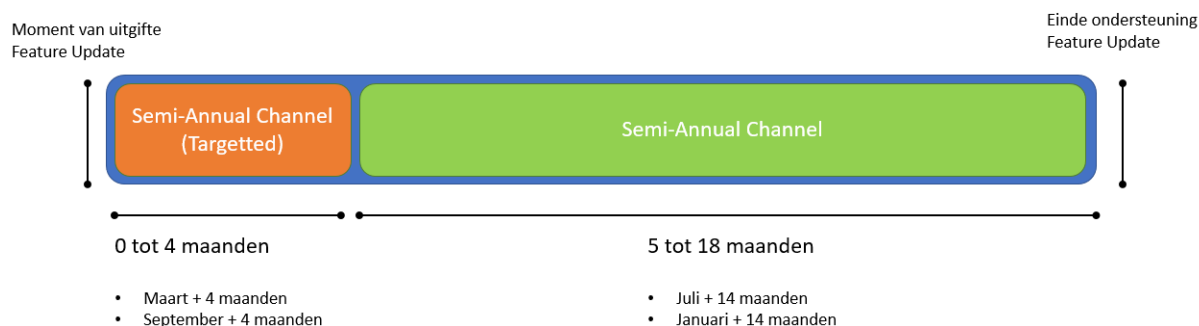
Elke maand wordt Windows 10 voorzien van een Quality Update welke beveiliging-, betrouwbaarheid- en probleemoplossingen (bugfixes) bevat in één cumulatief updatepakket. Microsoft brengt alleen Quality Updates uit voor Feature releases welke in ondersteuning zijn.

Met behulp van Windows Update for Business is het mogelijk om Feature en Quality Updates te verspreiden over alle Windows 10 werkplekken.

Om de Feature Updates in een Pilot vorm te kunnen aanbieden zijn er twee Service Channels beschikbaar:

- **Semi-Annual Channel (Targeted):** bevat de Windows 10 Feature Update release vanaf moment van uitgifte tot en met 4 maanden daarna.
- **Semi-Annual Channel:** bevat de Windows 10 Feature Update vanaf 5 maanden na uitgifte tot en met 18 maanden na uitgifte.

Schematische weergave Windows 10 updateproces:



Update: Vanaf de 1809 feature update zal de jaarlijkse september Feature update voor Windows 10 Enterprise en Windows 10 Education niet 18 maanden, maar 30 maanden ondersteund worden.

Met behulp van de Service Channels is voor De Moderne Werkplek het navolgende Windows 10 updateschema opgesteld. Dit schema bestaat uit update ringen welke worden gekoppeld aan een groep van gebruikers. gemeente Midden-Delfland is zelf verantwoordelijk voor het aanleveren van deze gebruikers.

Indien een Feature Update of een Quality Update zorgt voor problemen, dan kan verdere verspreiding voor een navolgende ring tijdelijk gepauzeerd worden. Dit geeft gemeente Midden-Delfland de mogelijkheid om het probleem op te lossen.

Ring	Service Channel	Uitstellen Feature Updates	Uitstellen Quality Updates	Opmerking
Preview	Semi-Annual Channel (Targeted)	7	0	Inzet bij ICT-afdeling voor eerste De Moderne Werkplek testen en bevindingen.
Pilot: Klein	Semi-Annual Channel (Targeted)	31	1	Inzet bij een selectie van MW gebruikers. Dit zijn gebruikers welke actief meewerken aan De Moderne Werkplek zoals IT-coördinatoren, applicatiebeheerders en gebruikers met veel kennis van IT.
Pilot: Standaard	Semi-Annual Channel (Targeted)	62	1	Inzet bij een aantal standaard gebruikers welke willen participeren in de Pilot. Deze gebruikers moeten actief betrokken zijn en bereidwillig zijn om incidenten te melden.

Productie: Klein	Semi- Annual Channel	14	1	Uitrol op productie, ongeveer 1% van de populatie.
Productie: Middel	Semi- Annual Channel	28	4	Uitrol op productie, ongeveer 10% van de populatie.
Productie: Groot	Semi- Annual Channel	42	7	Uitrol op productie, complete populatie.

Windows 10 Update zal worden aangevuld met de navolgende update instellingen.

- › Microsoft Product Update: toegestaan
- › Windows Drivers: toegestaan
- › Automatisch updategedrag: automatisch installeren binnen onderhoudsvenster.
- › Productie uren (herstart voor updates wordt niet aanboden): 08.00 – 16.00
- › Download methode: HTTP blended with peering behind same NAT.
 - Deze optie reduceert het bandbreedte gebruik doordat computers de Windows Feature en Quality updates automatisch intern naar elkaar verspreiden.

8 Beveiliging

Beveiliging is een integraal onderdeel van de Moderne Werkplek. De Moderne Werkplek is voorzien van de navolgende beveiligingsmaatregelen. In dit hoofdstuk staan de genomen beveiliging maatregelen en de bijbehorende instellingen.

8.1 Windows Defender Firewall

De Windows Defender Firewall blokkeert ongeautoriseerd netwerkverkeer van en naar de computer.

Component	Instelling
Windows Defender Firewall	Enable
Inbound notifications	Enable
File Transfer Protocol	Block
Conditional Access	Windows Defender moet geactiveerd zijn ook op kantoor locaties van gemeente Midden-Delfland. Hierbuiten moet Windows Defender Firewall ingeschakeld zijn.

8.2 Windows Defender SmartScreen

Windows Defender SmartScreen voorkomt het uitvoeren van bestanden en websites welke mogelijk niet-legitiem zijn, SmartScreen zal standaard worden ingesteld.

Component	Instelling
SmartScreen for apps and files	Enable
Unverified files execution	Block
SmartScreen for Microsoft Edge	Require
Malicious site access	Block
Unverified file download	Block

8.3 Windows Defender Antivirus

Windows Defender Antivirus voorkomt dat bekende malafide software schade aan een computer van de gemeente kan veroorzaken.

Component	Instelling
Real-time monitoring	Enable
Behavior monitoring	Enable
Network Inspection System (NIS)	Enable
Scan all downloads	Enable
Scan scripts loaded in Microsoft web browsers	Enable
End-user access to Defender	Block
Signature update interval (in hours)	2

Days before deleting quarantined malware	7
CPU usage limit during a scan	25
Scan archive files	Enable
Scan incoming mail messages	Enable
Cloud-delivered protection	Enable
Time extension for file scanning by the cloud	30
Prompt users before sample submission	Send all data without prompting
Time to perform a daily quick scan	12 PM
Actions on detected malware threats	Enable
Low severity	Quarantine
Moderate severity	Quarantine
High severity	Quarantine
Severe severity	Quarantine

8.4 BitLocker

BitLocker verzorgt de encryptie van alle informatie op de harde schijf / SSD. Hierdoor is het voor een ongeautoriseerd persoon niet mogelijk om de informatie welke lokaal staat opgeslagen in te zien.

BitLocker vereist een encryptie sleutel voor het zichtbaar maken van alle informatie voor geautoriseerde personen. Deze encryptie sleutel wordt opgeslagen in de TPM-chip van de computer. Om deze reden is de aanwezigheid van een TPM-chip in de computer verplicht om gebruik te kunnen maken van BitLocker.

BitLocker wordt standaard aangezet op De Moderne Werkplek.

Component	Instelling
Encrypt devices	Require
Configure encryption methods	Enable
Encryption for operating system drives	XTS-AES 128-bit
Encryption for fixed data-drives	XTS-AES 128-bit
Encryption for removable data-drives	XTS-AES 128-bit
Additional authentication at startup	Require
BitLocker with non-compatible TPM chip	Block
OS drive recovery	Enable

8.5 Microsoft Defender

Naarmate bedreigingen complexer en ingewikkelder worden, is het voor het IT team moeilijker om overzicht te houden en alle melding bij te houden. Microsoft 365 Defender maakt gebruik van het Microsoft 365-beveiligingsportfolio om automatisch bedreigingsgegevens over domeinen heen te analyseren en een compleet beeld van elke aanval op één dashboard te creëren.

Microsoft Defender is er in drie varianten.

- › **Identiteiten:** Beheert en beveilgt hybride identiteiten en vereenvoudig de toegang voor werknemers, partners en klanten.

- › **Endpoints** : Bied preventieve bescherming, detectie na een inbreuk, geautomatiseerd onderzoek en respons voor W10 werkplekken.
- › **E-mail en documenten**: Beveilig e-mail, bijlagen en samenwerkingstools met Microsoft Defender voor Office 365.

#	Ontwerp keuze	Motivatie
47	Defender tools zullen worden uitgerold voor Office 365 en Endpoints.	Inzet van Defender for Endpoints en Office 365 biedt de gemeente Midden-Delfland de meeste kans om cyberbedreigingen te vermijden en inzicht te krijgen in eventuele besmettingen binnen de organisatie.

8.6 Microsoft Information Protection (MIP)

Met de grootschalige verschuiving naar gedistribueerde teams en volledig werken op afstand, is de mogelijkheid voor werknemers om samen te werken met anderen, zowel binnen de organisatie buiten de organisatie, als op verschillende apparaten, apps en services, van cruciaal belang om het werk gedaan te krijgen. Wanneer die gegevens gaan zwerven, zijn IT-beheerders verantwoordelijk om ervoor te zorgen dat dit op een veilige, beschermde manier gebeurt die voldoet aan het bedrijfsbeleid van de gemeente Midden-Delfland organisatie.

Het punt is dat niet alle gegevens vertrouwelijk zijn en dus niet dezelfde controles toe te passen zijn op een lunchmenu van het bedrijfsrestaurant als op een zeer vertrouwelijke spreadsheet met informatie over bijvoorbeeld de kwartaalinkomsten. Het is zelfs zo dat het toepassen van onnodige beperkingen uiteindelijk averechts werken en een negatieve invloed hebben op de gebruikersacceptatie en ertoe leiden dat mensen zich tot andere, niet-goedgekeurde tools wenden voor collaboratie.

Microsoft Information Protection (MIP) is de uniforme labeling tool in Microsoft 365 en biedt organisaties een meer geïntegreerde en consistente aanpak voor het maken, configureren en automatisch toepassen van uitgebreid beleid om uw gegevens te beschermen en te beheren, op verschillende apparaten, apps, cloudservices en on-premises.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
48	AIP-inrichting is gewenst voor de gemeente Midden-Delfland echter zal eerst een migratie van documenten moeten plaats vinden naar de cloud diensten zoals SharePoint	Inzet van sensitivity labels dient als basis voor het onder controle krijgen van data governance en retentie. De gemeente Midden-Delfland heeft de wens uitgesproken om stappen te willen zetten voor de implementatie van AIP/MIP binnen de moderne werkplek.

8.7 Data Loss prevention (DLP)

Data Loss Prevention (DLP) maakt gebruik van regels en beleid om te bepalen welke bestanden en gegevens als vertrouwelijk, kritiek of gevoelig worden beschouwd en vervolgens om te voorkomen dat deze bestanden worden gedeeld of verzonden.

DLP detecteert gevoelige informatie en kan deze data identificeren (zoals een creditcard- of BSN-nummer) zonder dat dit gevolgen heeft voor mensen die met de rest van de inhoud werken. Zodra een DLP-beleidsregel is gemaakt wordt deze gesynchroniseerd met de volgende Office 365 diensten:

- › Exchange online
- › OneDrive for business
- › SharePoint Online
- › Microsoft Apps for Enterprise desktop-programma's

De DLP Policy tips zijn meldingen in de desktopversie van Word, Excel of Outlook. Een policy tip wordt weergegeven in bijvoorbeeld de outlook cliënt op het moment dat een eindgebruiker mogelijk gevoelige informatie gaat versturen.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
49	Inzet van DLP is gewenst op basis van het kunnen scannen van documenten op vertrouwelijke informatie	Voor het scannen van DLP matches op on-premises file servers word een scanner geïnstalleerd welke gebruikt kan worden voor inzet bij DLP governance.

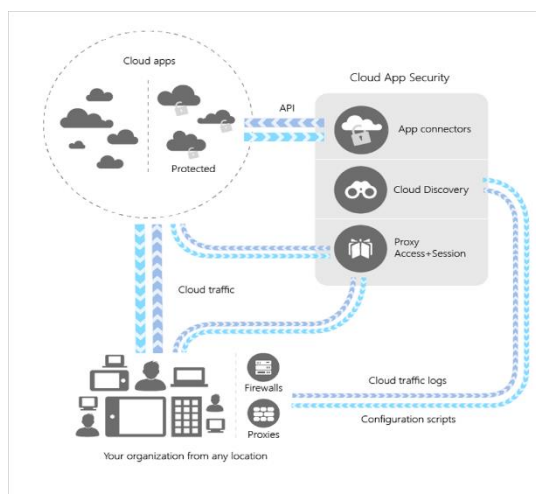
8.8 Microsoft Cloud App security (MCAS)

Microsoft Cloud App Security (MCAS) is een Cloud die Office 365-audit gegevens kan opnemen en ernaar kan handelen.

De huidige lijst ondersteunde apps omvat:

- › SharePoint Online.
- › OneDrive for Business.
- › Exchange Online.
- › Teams.
- › Dynamics365

Microsoft Cloud App Security werkt als een controletool, een firewall en een authenticatietool die gegevens en toepassingen te allen tijde beschermt.



Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
50	Inrichting van MCAS is besproken tijdens de workshop en aangemerkt als gewenste technologie	De opzet van MCAS hangt deels samen met de inrichting van DLP/MIPS en met de uitrol van full client werkplekken. Daarnaast zal onderzocht moeten worden hoe discovery kan worden ingezet voor apps zoals toegang tot log collectors.

8.9 Beveiligingsinformatie en event-management (SIEM)

Microsoft Azure Sentinel is een schaalbaar, cloudeigen oplossing voor Security Information Event Management (SIEM) en Security Orchestration Automated Response (SOAR). Azure Sentinel levert intelligente beveiligingsanalyses en bedreigingsinformatie voor de hele onderneming en is daardoor één oplossing voor waarschuwingdetectie, zichtbaarheid van bedreigingen, proactieve opsporing en reactie op bedreigingen.

Met Azure Sentinel hebben IT-teams overzicht over de hele onderneming, waardoor geavanceerdere aanvallen en de toenemende hoeveelheden waarschuwingen en de lange duur voordat oplossingen worden gevonden.

- › Verzamel relevante gegevens op grote schaal voor alle gebruikers, apparaten, toepassingen en infrastructuur, zowel on-premises als in meerdere clouds.
- › Detecteer eerder “zero-day” bedreigingen en minimaliseer de kans op valse meldingen “zg. false positives” met behulp van de analyses en ongeëvenaarde bedreigingsinformatie van Microsoft.
- › Onderzoek bedreigingen met behulp van kunstmatige intelligentie en speur naar verdachte activiteiten voor gebruik in de cyberbeveiliging.
- › Snellere reactie op incidenten met automatisering van gestandaardiseerde taken.

Ontwerp keuzes:

#	Ontwerp keuze	Motivatie
51	Een SIEM inzetten is gewenst maar nog niet praktisch inzetbaar binnen gemeente Midden-Delfland	Een SIEM is momenteel nog een wens die op de roadmap staat, er is nog geen onderzoek naar gedaan en er heeft geen pakket selectie plaatsgevonden. Verwachting is dat dit eind 2021 als project zal worden opgepakt.

9 Bijlagen

9.1 Bijlage 1: Beschrijving Adoptie

SoftwareONE kan de gemeente Midden-Delfland helpen bij alle aspecten van de transformatie naar de Moderne Werkplek en Microsoft 365. SoftwareONE heeft een 6-fasenaanpak ontwikkeld met behulp van onze gestructureerde projectmanagementmethodologie, die ervoor zorgt dat veranderingen worden beheerd via een gecontroleerde, logische, mijlpaal gedreven routekaart. Dit terwijl de focus ligt op het realiseren van de zakelijke voordelen van het project, waardoor het rendement op de investering van de gemeente Midden-Delfland wordt gemaximaliseerd.

Als een organisatie wil overstappen naar een nieuwe technologie, is het belangrijk om de medewerkers bij dit proces te betrekken. Maar hoe doe je dat en waar moet je beginnen? SoftwareONE helpt u graag bij het succesvol uitvoeren van deze missie. Bij SoftwareONE werken Prosci & Microsoft gecertificeerde adoptieadviseurs met ruime ervaring. We maken gebruik van de bewezen veranderingsmethodiek van Prosci. De methodiek van Prosci maakt gebruik van het ADKAR-model. Het ADKAR-model is bedoeld als een coaching instrument om medewerkers te helpen en bij te staan tijdens veranderingsprocessen binnen organisaties.

Het werken met nieuwe technologie heeft een grote impact op medewerkers. Het vraagt om een nieuwe manier van werken. Verandering vraagt om veerkracht en kan in sommige gevallen op weerstand stuiten. Het ADKAR-model biedt houvast, structuur en de juiste instrumenten om verandering te begeleiden tijdens een verandering. De Prosci-methodologie heeft tot nu toe veel organisaties ondersteund bij succesvolle veranderingen. Het bijbehorende ADKAR-model maakt gebruik van vijf elementen, die samen het acroniem ADKAR vormen, wanneer de vijf elementen van verandermanagement met succes worden doorlopen. De vijf elementen van ADKAR staan voor:

- ▶ **Awareness – zich bewust zijn van de noodzaak van verandering**
Deze stap is gericht op het bewust maken van de medewerkers van de noodzaak tot verandering. Waarom is gekozen voor Office 365? Het is belangrijk dat medewerkers een antwoord krijgen op deze vraag. Als er geen of te weinig aandacht wordt besteed aan het beantwoorden van de ‘waarom’-vraag, kan dit later in het project veel weerstand oproepen.
- ▶ **Desire – de wil en het besluit om deel te nemen aan de verandering**
Nadat de vraag waarom is beantwoord en de noodzaak van het project en de verandering is gecommuniceerd, is het tijd om ervoor te zorgen dat medewerkers tijdens de verandering bewuste keuzes kunnen maken. Dit kan worden bereikt door het beantwoorden van de vraag “wat brengt deze verandering mij persoonlijk op?
- ▶ **Knowledge – de kennis om te veranderen**
Vanaf het moment dat men een duidelijk idee heeft van wat de verandering zal brengen en men uitkijkt naar de verandering, is het tijd om te leren hoe de nieuwe functionaliteiten te gebruiken. Hoe werkt de nieuwe tool, waar klik je op, hoe werk je samen, hoe werken de verschillende onderdelen. Dit alles wordt uitgelegd in instructiemateriaal of trainingssessies.

► **Ability – de vaardigheden en competenties voor de nieuwe situatie**

Elke werknemer heeft andere behoeften en competenties. Daarom is het belangrijk om goed te kijken naar individuele behoeften. Deze stap is gericht op het krijgen van mensen die nog steeds in de weer zijn tegen verandering. Weerstand ontstaat vaak met een reden. Denk bijvoorbeeld aan de overstap van e-mail naar het bellen van klanten. Iemand met telefonische angst zal in het verzet blijven. Dit is het moment om te kijken naar de individuele competenties van medewerkers en, indien nodig, mensen individueel te begeleiden of te coachen.

► **Reinforcement – de maatregelen om de verandering veilig te stellen**

De hele organisatie is nu volledig aan boord en kent het gewenste gedrag en heeft de juiste vaardigheden. De laatste fase, die gekenmerkt wordt door het veiligstellen van de verandering. Dit lukt wanneer successen worden gevierd, barrières worden weggenomen en medewerkers worden gevraagd hoe tevreden ze zijn met de verandering.

Voor een succesvolle adoptie van nieuwe technologie is meer nodig dan alleen een goed ontwerp van de technologie. Minstens zo belangrijk is dat de medewerkers die deze technologie moeten gebruiken over de nodige kennis beschikken. Veel projecten zijn mislukt omdat medewerkers niet wisten hoe ze met de nieuwe oplossing moesten werken. Dit leidt tot ontevredenheid. En zeker nu er continu een stroom van nieuwe functionaliteiten en online diensten aan het Microsoft 365 platform wordt toegevoegd, is het belangrijk om veel aandacht te besteden aan de medewerkers die met Microsoft 365 werken. In ons partnership, met de adoptie- en verandermanagementactiviteiten, leggen we een stevige basis voor de start van de beoogde verandering. De activiteiten bestaan uit het volgende:

- **Live Webinars:** voor werknemers om de volledige mogelijkheden van Microsoft 365 te gebruiken om meer te doen in minder tijd. Webinars worden opgenomen en gedeeld met gemeente Midden-Delfland. In een tijdspan van één dag is dit inclusief 4 Webinars van elk 1 uur voor 2 verschillende onderwerpen. Onderwerpen om uit te kiezen zijn bijvoorbeeld OneDrive for Business, Teams, SharePoint Online of Outlook;
- **Begeleiding van de organisatie:** bij het verbeteren van het gebruik van de Microsoft 365-toepassingen en -licenties;
- **Diepgaande sessies:** over nieuwe functies en werklust. Een enkele sessie heeft een tijdspan van een halve dag;
- **Roadmap strategie en prioritering:** van de vast te stellen werklust;
- **VIEW sessies voor het champions team of eindgebruikers:** op basis van de specifieke wensen van de eindgebruikers, besteden we tijdens de sessie aandacht aan de scenario's die relevant zijn voor uw organisatie. Een VIEW-sessie kan door maximaal 10 medewerkers worden bijgewoond. Er kan rekening gehouden worden met een halve dag inzet per sessie;
- **Creatie van een communicatiepakket:** in het communicatiepakket is de communicatie voorzien waarmee de kampioenen en de organisatie de verandering kunnen communiceren. Dit zijn onder andere e-mailtemplates, one-pagers en flyers. De organisatie kan deze naar wens aanpassen en inzetten.

9.2 Bijlage 2: Cloud exit strategie

Een goed geplande cloud exit-strategie verlicht de druk van mogelijke vendor lock-in. Zelfs als een organisatie de cloud-workloads nooit daadwerkelijk terug op locatie verplaatst, kan een exit-strategie de onderhandelingen met providers begeleiden en het applicatieontwerp beïnvloeden.

Dankzij de hybride connectiviteit tussen de on-premises Active Directory en Azure AD zijn postvakken over het algemeen gemakkelijk naar on-premises terug te zetten. De enige echte overweging is de hoeveelheid opslagruimte die mogelijk moet worden ingezet om inkomende mailboxen te accepteren, omdat gebruikers misschien gewend zijn geraakt aan grote mailboxquota die door Exchange Online worden toegewezen.

Als vuistregel voor exit-strategieën zijn mailboxen en documenten meestal gemakkelijk te verplaatsen, maar al het andere is daarentegen moeilijk.

Wanneer bijvoorbeeld document labels (via MIP) worden geïmplementeerd om Microsoft 365-gegevens te beschermen, kan het moeilijk worden om toegang te krijgen tot beveiligde inhoud die weer on-premises is verplaatst, omdat het niet langer mogelijk is om die inhoud te ontsleutelen. In dat geval helpt een hybride configuratie opnieuw om verbinding te houden met de Azure Information Protection-service. Ook moet elke aanpassing die aan Exchange Online is gemaakt, weer on-premises worden verplaatst, zodat zaken als PowerShell-scripts, transportregels, regels voor preventie van gegevensverlies, bewaarbeleid en -tags, enzovoort.

Met de keuze voor Microsoft Teams als samenwerkingsplatform met of zonder telefonie integratie zijn er limitaties bij het migreren naar een on-premise oplossing. Gewoonlijk kunnen deze communicatiekanalen worden verplaatst naar Skype voor Bedrijven Server of een oplossing van derden en kunnen documenten verplaatst worden naar SharePoint Server, maar het gespreks- en chatgedeelte van Teams is alleen in de cloud beschikbaar, inclusief opnames van Teams-gesprekken en vergaderingen.

Veel van de functionaliteit die beschikbaar is in Microsoft 365 is alleen beschikbaar in de cloud en er zijn geen tools om gegevens te verplaatsen naar een formulier dat kan worden gebruikt door een on-premises toepassing. Het blijft mogelijk om de impact te minimaliseren door Microsoft 365 Groups te synchroniseren met een hybride on-premises omgevingen, waar ze verschijnen als standaard e-maildistributielijsten.

Groepen bestaan echter niet on-premises (wat ook geldt voor andere gebruikersgerichte functies zoals MyAnalytics). Het is moeilijk om te weten hoe de informatie in groepsgesprekken, gedeelde notebooks en documentbibliotheken kunnen worden opgehaald omdat er geen exporthulpprogramma's bestaan, daarom zal dit waarschijnlijk een aanzienlijke handmatige inspanning vergen om gegevens uit de cloud te herstellen.

Over het algemeen is het raadzaam om een hybride connectiviteit te behouden, maar als dit niet de vereiste gegevens dekt of als de connectiviteit niet mogelijk is, moet de organisatie misschien overwegen dat sommige gegevens onherroepelijk verloren zijn gegaan of moet ze vooraf overwegen om het gebruik van deze workloads niet toe te staan.

Disclaimer

This publication contains confidential and proprietary information that is protected by copyright. SOFTWAREONE reserves all rights thereto. SOFTWAREONE shall not be liable for obvious typing and arithmetic errors in any document provided by SOFTWAREONE. Liability for damages directly and indirectly associated with the supply or

use of this document is limited in accordance with the supply or use of this document is excluded as far as legally permissible.

The SOFTWAREONE Services Statement of Work presented herein is intended exclusively as a guide to enable [Company Name] 's representatives to evaluate the offering of SOFTWAREONE. It must not be copied, reproduced, passed to third parties or used for engineering purposes without the express permission of SOFTWAREONE.

Copyright © 2018 by SOFTWAREONE. All rights reserved. SOFTWAREONE is a registered trademark of SoftwareONE AG. All other trademarks, service marks or trade names appearing herein are the property of their respective owners.