Microsoft

De Overheidswerkplek powered by Microsoft 365

De digitale werkplek van de toekomst

De Overheidswerkplek

Introductie

Goed nieuws! Vanaf 1 februari 2019 kunnen alle Nederlandse gemeenten gebruik maken van de VNG Overheidswerkplek. Deze werkplek bestaat uit nieuwe juridische gemeentelijke voorwaarden, een op maat gemaakte VNG-Microsoft Overheidswerkplek en gunstige commerciële voorwaarden. Het doel van de overeenkomst is om de gemeenten verder te ondersteunen met het vergroten van het samenwerkend vermogen. Daarnaast biedt de Overheidswerkplek versterking van het security & compliance niveau en verbetert het de medewerkerstrevredenheid doordat technologische verschillen tussen werk en privé worden verkleind. Tot slot verlaagt het de kosten door de standaardisatie en rationalisatie.

Ontwikkeling

Organisaties staan in een spagaat. Gebruikers wensen een productiviteits- en communicatieplatform om in- en extern snel en effectief te kunnen samenwerken. Bij voorkeur op ieder device en vanaf elke locatie. Dit betekent voor security; het oude kasteelprincipe (oftewel perimeter beveiliging) brokkelt af en de organisatie wordt blootgesteld aan nieuwe informatiebeveiligingsrisico's. Daarnaast legt nieuwe wet- en regelgeving extra druk op het aantonen van compliance.

Standaardisatie

Gemeentes en deelnemingen kiezen steeds vaker voor een best-of-suite benadering. Hierbij worden technologische oplossingen geselecteerd waarbij consolidatie, integratie en eenvoud het winnen van specifieke (technische) requirements. Zeker nu het kasteelprincipe afbrokkelt zijn er nieuwe en geavanceerde security & compliance technologieën nodig om in controle te blijven.

$7.2M
gemiddelde besparing in TCO

40%
lager beveiligingsrisico

2.3 uur
tijdsbesparing per gebruiker per week

Forrester, "The TEI™ Of The Modern Desktop With Microsoft 365" 2018

De Overheidswerkplek

Microsoft 365 Security & Compliance

Microsoft 365

Het Microsoft 365 E3 platform biedt best-of-suite technologie voor productiviteit en samenwerken inclusief basiscomponenten voor security & compliance. Om de nieuwe risico's te mitigeren zijn aanvullende security & compliance technologieën noodzakelijk, welke zijn opgenomen in Microsoft 365 E5. Op basis van de overeenkomst kunnen gemeenten en deelnemingen onder gunstige voorwaarden gebruik maken van een aanvullende set van security & compliance technologie.

Stimuleert creativiteit

Gebouwd voor samenwerken

Geïntegreerd voor eenvoud

security & compliance

Eenmalige actie tot 1 april 2019*

Profiteer direct van de korting op de Security & Compliance bundel door minimaal 10% van de gebruikers te activeren en maak daarnaast direct gebruik van de juridische voorwaarden!

* vraag het Microsoft team naar de voorwaarden

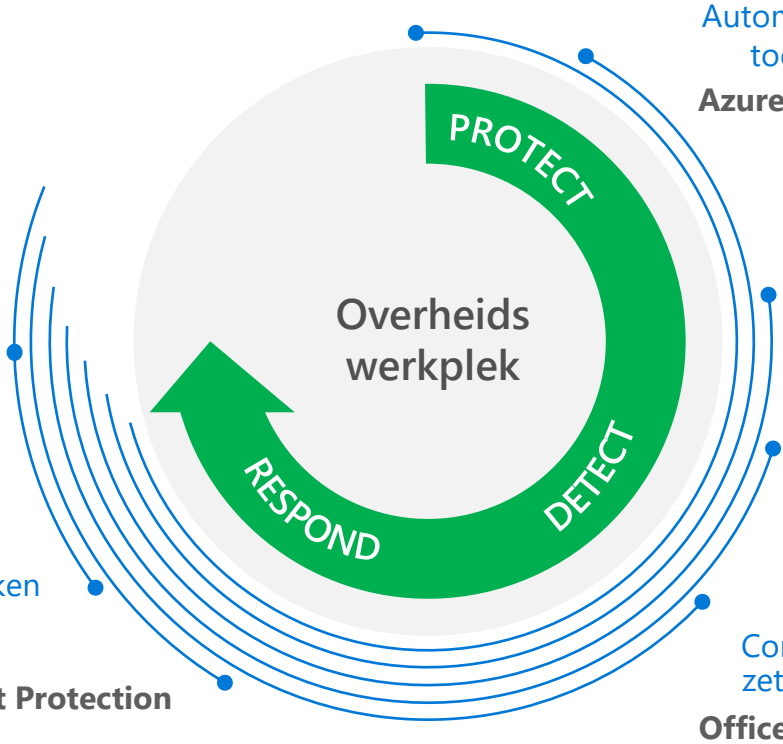
De Overheidswerkplek

Microsoft 365 Security & Compliance

Veilige email, bijlagen, weblinks en upload van bestanden
Office 365 Advanced Threat Protection

Automatische datarubricering en toegangscontrole op data
Azure Information Protection Plan 2

Preventieve beveiliging, detectie na inbreuken, geautomatiseerd onderzoek en respons
Windows 10 Advanced Threat Protection



Actuele dreigingsinformatie & simulatie van aanvallen
Office 365 Threat Intelligence

Controle en grip op het gebruik van cloud apps
Microsoft Cloud App Security

Detecteren en onderzoeken van geavanceerde identiteitsaanvallen
Azure Advanced Threat Protection

Compliance onderzoeken & zet een digitale archivaris in
Office 365 Advanced Compliance

Veilig gebruik van Microsoft cloud diensten en controle van identiteiten
Azure Active Directory Plan 2

De Overheidswerkplek powered by Microsoft 365

Overheidswerkplek – Security & Compliance

Office 365 Advanced Threat Protection (O365 ATP)

Iedere dag zijn er weer nieuwe malware-aanvallen. O365 ATP beveiligt realtime mailboxen, bestanden, online opslag en toepassingen tegen nieuwe, geavanceerde aanvallen. O365 ATP biedt een holistische bescherming in Microsoft Teams, Word, Excel, PowerPoint, Visio, SharePoint Online en OneDrive voor Bedrijven. O365 ATP biedt beveiliging tegen onveilige bijlagen en continue beveiliging tegen schadelijke webkoppelingen en bescherming tegen phishing aanvallen, en is daarmee een aanvulling op de beveiligings-functies van Exchange Online Protection voor betere beveiliging tegen zero-day-aanvallen.

- Realtime email beveiliging tegen nieuwe, geavanceerde aanvallen
- Beveiliging van onveilige bijlagen en schadelijke links naar het internet
- Sandboxing/detonatie analyse scanning van bestanden die geüpload worden
- Bescherming tegen phishing aanvallen

Azure Information Protection Plan 2 (AIP P2)

Controleer en beveilig e-mails, documenten en gevoelige informatie die intern en/of extern gedeeld wordt. Van eenvoudige & automatische rubricering tot ingesloten labels en machtigingen; verbeter de gegevensbescherming op ieder moment met AIP P2, waar de gegevens ook zijn opgeslagen en met wie ze ook worden gedeeld.

- Automatische datarubricering en toegangscontrole op data op basis van gevoeligheid
- Biedt bescherming op documentniveau waaronder lees, print of doorstuur rechten
- Scan en rubriceer automatisch bestaande onpremise databronnen
- Rubricering reist met het document mee, ongeacht het platform of type opslag

Office 365 Threat Intelligence (O365 TI)

O365 TI is een verzameling van inzichten en informatie die beschikbaar is in het Office 365 Security & Compliance Center. Met deze inzichten kan het beveiligingsteam de organisatie beschermen tegen aanvallen. O365 TI controleert signalen en verzamelt gegevens uit meerdere bronnen, zoals gebruikersactiviteit, authenticatie, e-mail, besmette pc's en beveiligingsincidenten. Beheerders van Office 365, beveiligingsbeheerders en beveiligingsanalisten kunnen gebruik maken van de informatie om bedreigingen voor gebruikers en intellectueel eigendom te begrijpen en adequaat te kunnen reageren.

- Geeft het Security Operations Team relevante en actuele dreigingsinformatie vanuit de Microsoft Cybersecurity Groep
- Diverse tools om aanvallen te simuleren (bijv. Phishing e-mails) waardoor de bewustwording van medewerkers verhoogt en het risico van een gerichte aanval mitigeert

Microsoft Cloud App Security (MCAS)

Met MCAS houdt de organisatie controle op het gebruik van SaaS-applicaties dankzij inzicht en controlemogelijkheden. MCAS brengt Shadow-IT in kaart en beschikt over de mogelijkheden om risico's te beoordelen, beleid af te dwingen, activiteiten te onderzoeken en bedreigingen te stoppen. Door MCAS kan de organisatie veiliger overstappen naar de cloud terwijl de controle over essentiële gegevens wordt behouden.

- Monitoren en beschermen tegen bedreigingen van SaaS-applicaties
- Bescherm kritieke gegevens in SaaS-applicaties. Bijvoorbeeld: het opslaan van hoog gerubriceerde documenten of PII-data naar opslaglocaties als Dropbox en Google Drive wordt tegengehouden of direct versleuteld
- Breng schaduw-IT in kaart waarna op basis van een risico score van de SaaS-applicatie het mogelijk is om beleid af te dwingen, activiteiten te onderzoeken en bedreigingen te stoppen

Overheidswerkplek – Security & Compliance

Office 365 Advanced Compliance: Advanced eDiscovery (O365 AeD)

O365 AeD is gebaseerd op de standaard zoekfuncties voor inhoud en eDiscovery. Na het aanmaken van een eDiscovery-case, worden alle gegevens die mogelijk op de case van toepassing zijn verzameld. Vervolgens kunnen de gegevens verder geanalyseerd worden met behulp van tekstanalyse, machine-learning en de codeermogelijkheden van O365 AeD. Dit helpt de organisatie duizenden e-mailberichten, documenten en andere soorten gegevens snel te verwerken en die items te vinden die relevant zijn voor een specifiek geval.

- Op basis van intelligentie snel inzicht verkrijgen in digitale informatie voor compliance, een integriteitsonderzoek en/of een WOB/AVG verzoek
- Middels tekstanalyse en de inzet van machine-learning snel en effectief resultaat

Office 365 Advanced Compliance: Advanced Data Governance (O365 ADG)

Omdat de hoeveelheid elektronische gegevens exponentieel groeit, stellen veel organisaties zichzelf bloot aan risico's door onnodige gegevens te bewaren. Organisaties bewaren bijvoorbeeld de persoonlijke gegevens van voormalige werknemers die lang geleden het bedrijf hebben verlaten. O365 ADG past machine-learning toe om belangrijke gegevens te vinden, te behouden en tegelijkertijd dubbele, overtollige en verouderde gegevens te verwijderen.

- Proactieve beleidsaanbevelingen en automatische gegevensrubricering
- Uitvoeren van automatisch retentie- en verwijderingsacties tijdens de gehele data lifecycle
- In te richten volgens Nationale en/of Europese archief wet- en regelgeving

Office 365 Advanced Compliance: Privileged Access Management (PAM)

PAM beschermt de organisatie tegen inbreuken die bestaande specifieke beheerders-accounts kunnen gebruiken, door fijnmazige toegangscontrole over beheertaken in Office 365. Veelal zijn dit de accounts met permanente toegang tot gevoelige gegevens of toegang tot kritieke configuratie-instellingen. Nadat toegangsbeheer is ingeschakeld, moeten gebruikers via een workflow just-in-time toegang aanvragen om specifieke taken uit te voeren. Hierbij wordt een duidelijke scope aangebracht en de toegang is tijdsgebonden. Dit geeft gebruikers net voldoende toegang om de taak uit te voeren, zonder de blootstelling van gevoelige gegevens of kritieke configuratie-instellingen te riskeren.

Office 365 Advanced Compliance: Customer Lockbox

In het geval van een issue kan een ondersteuningstechnicus van Microsoft ingeschakeld worden om het issue op te lossen. In bepaalde gevallen moet de ondersteuningstechnicus toegang hebben tot de Office 365-inhoud. Met Customer Lockbox kan geregeld worden of de ondersteuningstechnicus deze toegang krijgt. Er is ook een verlooptijd op het verzoek en de toegang tot inhoud kan verwijderd worden nadat de ondersteuningstechnicus het issue heeft opgelost.

Customer Key

Customer Key is gebaseerd op service encryptie en stelt de organisatie in staat encryptiesleutels te leveren en te beheren die worden gebruikt om gegevens (data-at-rest) in Office 365 te versleutelen.

Azure Active Directory Plan 2 (AAD P2)

AAD P2 biedt risk-based conditional access tot apps en kritieke bedrijfsgegevens op basis van de identiteit van de medewerker. Tevens biedt AAD P2 Privileged Identity Management voor het detecteren, beperken en bewaken van beheerders en hun toegang tot Microsoft diensten door de inzet van 'Just-In-Time-toegang'.

- Veilig gebruik van Microsoft cloud diensten en controle van identiteiten
- Zorgt voor synchronisatie en bescherming tussen onpremise en cloud identiteiten
- Helpt diefstal van digitale identiteiten te voorkomen door inzicht in gedrag en risico
- Geeft beheerders beperkt en tijdelijke toegang en activiteiten worden gemonitord

Azure Advanced Threat Protection (Azure ATP)

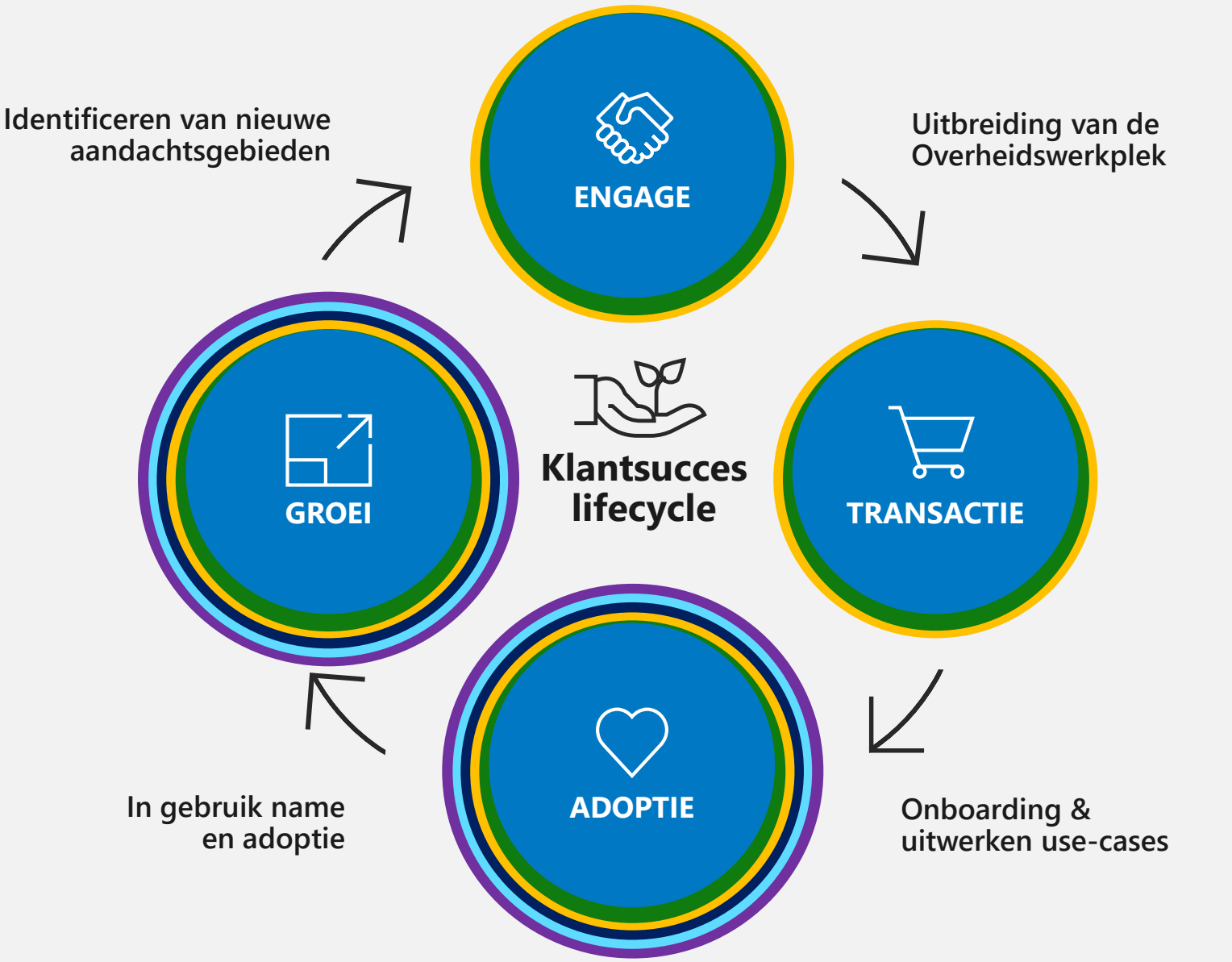
Azure ATP bewaakt het gedrag van gebruikers, apparaten en resources en detecteert afwijkingen. Dankzij de ingebouwde intelligentie levert Azure ATP snel inzicht in geavanceerde bedreigingen zowel onpremise als in de cloud.

- Detecteren en onderzoeken geavanceerde persistente bedreigingen over lokale, cloud-en hybride omgevingen voordat ze schade veroorzaken
- Identificeer verdachte activiteiten van gebruikers en apparaten o.b.v. detectie met bekende technieken en gedragsanalyse
- Geeft duidelijke geprioriteerde informatie over aanvallen weer op een tijdslijn

Windows Defender Advanced Threat Protection (WIN ATP)

WIN ATP is een platform voor intelligente beveiliging, automatische detectie, onderzoek en respons mogelijkheden (oftewel een Endpoint Detection and Response (EDR) oplossing). WIN ATP beschermt endpoints (clients en servers) tegen cyberbedreigingen, detecteert geavanceerde aanvallen en gegevenslekken, automatiseert beveiligingsincidenten en verbetert de beveiligingspositie.

- Risicobeheersing en mitigatie door de inzet van automatische intelligentie
- Gebruik de kracht van de cloud om use-cases te definiëren waar directe acties aan worden gekoppeld om security analisten te ontlasten en te kunnen laten focussen
- Geeft inzicht in gecompromitteerde devices en/of systemen waarna er een geautomatiseerd onderzoek gestart kan worden voor het bepalen van de impact. Opvolgend kan een geautomatiseerde oplossing de aanval blokkeren.



Account Executive (AE): ontwikkelen & behouden klantrelatie
Account Technology Strategist (ATS): technologische roadmap en consumptie

Solution Specialist (SSP): functioneel specialist Overheidswerkplek
Technisch specialist (TSP): technisch specialist Overheidswerkplek

Customer Success Manager (CSM): adoptie & realiseren klantdoelstellingen

One Channel Partner (OCP): opleiden & up-to-date houden partner ecosysteem

Microsoft Consultancy Services (MCS): ondersteuning tijdens digitale transformatie
Premier Support (PS): reactief support en inzet gestandaardiseerde diensten