



# Enterprise Mobility + Security

Beheer en beveiliging van devices, applicaties en data

Met het toenemende aantal cloudgebaseerde applicaties dat we altijd, overal en op elk device willen gebruiken, groeit ook de vraag naar beheer en beveiliging. Met Microsoft Enterprise Mobility + Security (EMS) wordt de data beheerd en wordt bepaald hoe de data gelezen, beschreven en gedeeld mag worden. Daarbij kan er afgedwongen worden wat het beveiligingsniveau van een device is en op welke wijze de data beschikbaar mag komen. EMS beheert zowel de data, de applicatie als de toegangsvoorwaarden van het device.

## Beheer en databeveiliging in één oplossing

EMS is een oplossing die speciaal is ontwikkeld voor beheer en beveiliging van devices, applicaties en data. Je hebt altijd en overal beveiligde toegang tot jouw informatie waardoor je klanten snel en efficiënt kunt helpen zonder dat je je zorgen hoeft te maken over de veiligheid van bedrijfsgegevens. De oplossing is op te delen in vijf losse onderdelen zodat je zelf kan kiezen om een deel van de oplossing te gebruiken, een combinatie van onderdelen of de complete oplossing. Deze onderdelen zijn:

- ▶ Identiteit gerichte beveiliging
- ▶ Identiteit- en toegangsbeheer
- ▶ Informatiebeveiliging
- ▶ Bureaubladvirtualisatie
- ▶ Beheer van mobiele apparatuur en applicaties

## Identiteit gerichte beveiliging

Dit is een holistische en innovatieve benadering van databeveiliging. Traditionele beveiligingsmethodes zijn door het veranderde cloud-landschap niet langer toereikend. Om je business echt goed te beschermen, heb je een oplossing nodig die beschermt, bedreigingen opspoorst en het juiste antwoord vindt op deze bedreigingen, zowel on-premise als in de cloud. Door voor elke medewerker een eigen identiteit te creëren en die goed te beschermen heeft Microsoft een goed antwoord gevonden op deze nieuwe uitdagingen.

## Identiteit- en toegangsbeheer

Dit onderdeel biedt de oplossing voor eenvoudig en veilig toegangsbeheer. Nu medewerkers steeds vaker hun eigen apparaten zakelijk gebruiken en daarnaast ook steeds meer SaaS-applicaties gebruiken, is dit voor veel IT-afdelingen een grote uitdaging geworden. Identiteit- en toegangsbeheer helpt de IT-afdeling om de bedrijfskritische data te beschermen dankzij zaken als Multi Factor Authentication (MFA). Het instellen van proactieve waarschuwingen helpt om potentiële issues te snel op te lossen en dankzij geavanceerde rapportages kunnen toekomstige problemen worden voorkomen.

## Informatiebeveiliging

Via deze oplossing kan je jouw data classificeren op basis van gevoeligheid en kan de meest kritische data onder permanente bewaking gehouden worden. Deze data kan vervolgens versleuteld worden en je kan gebruikersrechten toevoegen. Dit alles kan op een eenvoudige manier zonder de dagelijkse werkzaamheden te beperken.

## Bureaubladvirtualisatie

Met dit onderdeel optimaliseer je de beleving voor gebruikers. Waar ze ook inloggen en ongeacht het device kunnen ze altijd met dezelfde vertrouwde desktop werken die vergelijkbaar is met een lokale desktop. Hierdoor is het voor de IT-afdeling ook eenvoudig om applicaties voor de gebruikers te activeren.

## Beheer van mobiele apparatuur en applicaties

Dit laatste onderdeel van de oplossing wordt geboden met behulp van Microsoft Intune, een meer traditionele oplossing voor beheer van mobiele devices die met de toevoeging van andere onderdelen binnen EMS één van de meest geavanceerde oplossingen voor een beheerd mobiel platform is geworden. Je kan zelf de keuze maken of je de apparaten en applicaties beheert vanuit de cloud of lokaal, alles via één console. Om veilige mobiele productiviteit te kunnen garanderen, is Intune zelf opgedeeld in drie losse onderdelen:

### 1. Mobile Device Management

Een cloud gebaseerde oplossing die de complexiteit van het beheer van mobiele devices vermindert. Het biedt veilig beheer van devices, ongeacht of ze privé-eigendom of eigendom van de organisatie zijn. Alle populaire platforms (Windows, iOS, macOS en Android) worden volledig ondersteund. Indien er uitrol plaatsvindt van applicaties, kan dit via Intune eenvoudig geregeld worden. Daarnaast kan je de toegang tot bedrijfsapplicaties op onbeheerde devices beperken. In het geval van verlies of diefstal kan je op afstand het wachtwoord van het device resetten, het device blokkeren, de data versleutelen of het device volledig wissen.

### 2. Mobile Application Management

Intune stelt beheer en databescherming direct beschikbaar in de mobiele kantoorapplicaties waar gebruikers vertrouwd mee zijn. Om de kans op het uitlekken van bedrijfskritische data tegen te gaan, kan je gebruikers beperken in acties als kopiëren, knippen, plakken en opslaan tussen door Intune beveiligde applicaties en persoonlijke applicaties. Daarnaast kan je de toegang tot specifieke applicaties en URL-adressen op mobiele devices beperken. Om bedrijfsinformatie nog verder te beveiligen kan je selectief beheerde applicaties en de bijbehorende data wissen van onbeheerde, verloren, gestolen of ongebruikte devices.

### 3. PC Management

Intune beheert niet alleen mobiele devices zoals telefoons, tablets en notebooks, maar ook desktops. Met behulp van integratie met andere beheertools van Microsoft kan de IT-afdeling de mogelijkheden verder uitbreiden. Hierdoor krijg je ook informatie over de configuraties en de geïnstalleerde software op de beheerde computers.

## Productiever, efficiënter en veiliger.

EMS is een complete cloudoplossing, die de beveiliging en het beheer op een hoger plan tilt. De functionaliteiten zijn uitgebreid en maken je organisatie productiever, efficiënter en veiliger. Mobiele apparaten en applicaties in het organisatienetwerk worden moeiteloos beheerd en beveiligd, zonder dat dit ten koste gaat van productiviteit en keuzevrijheid. Integendeel: EMS vergroot juist die productiviteit doordat medewerkers met hun persoonlijke voorkeursdevices toegang hebben tot alle benodigde applicaties. Als organisatie geef je op deze manier invulling aan het 'Nieuwe Werken' en 'Bring Your Own Device' en tegelijkertijd beperk je eventuele 'Shadow IT' tot een minimum.

De optimale mix van gebruiksgemak voor de gebruikers en beveiliging van jouw kostbare bedrijfsinformatie.

## Noodzakelijke tool

In het huidige digitale tijdperk is EMS eigenlijk een noodzakelijke tool voor organisaties. Je wordt in staat gesteld om data en apparatuur adequaat te beschermen en de productiviteit te verbeteren zonder concessies te doen aan de gebruikerservaring. Het is een belangrijke stap voorwaarts in het verhogen van de veiligheid, zeker met het oog op de Algemene Verordening Gegevensbescherming (AVG) die in mei 2018 zal ingaan en waar elke organisatie mee te maken krijgt.

### Garanties en voordelen:

Beheer van alle apparatuur; vast of mobiel

Veilig beheer, ongeacht het besturingssysteem

Beperking van de toegang vanuit ongeautoriseerde devices

Remote wachtwoord reset, device lock, encryptie of volledig wissen

Voorkomt het uitlekken van bedrijfsdata door beperkingen in acties als kopiëren, plakken en opslaan

Beveiligt applicaties op onbeheerde apparatuur

Faciliteert uitrol op afstand van gewenste applicaties

