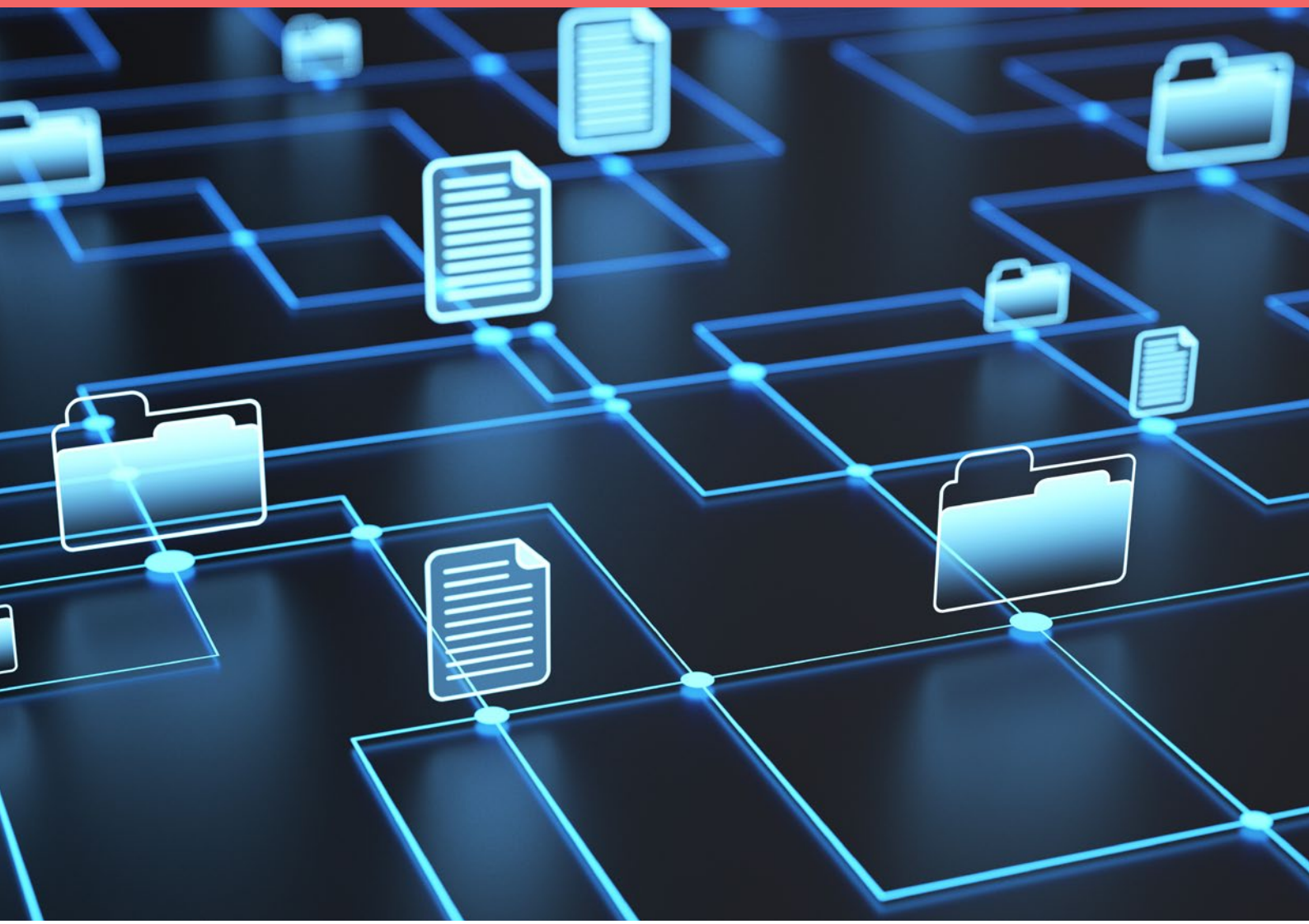
ikwil mobiel werken

Devices beheren 2.0

Ontdek hoe het veilig beheren van devices geen dagtaak meer is



In samenwerking met

1001 devices: de nachtmerrie van elke IT-afdeling

Een HP Elitebook, een iPhone en een Lenovo tablet, allemaal voor één medewerker. Als consument kijken we er niet meer van op. De gemiddelde IT'er wordt er echter ongelukkig van. Hoe ga je als IT-afdeling om met de groeiende hoeveelheid devices binnen je bedrijf?

Nog niet eens zo heel lang geleden kreeg iedere medewerker dezelfde desktop en laptop, en werkten ze enkel binnen de kantoormuren met het apparaat. Minder werk voor de IT-afdeling, maar niet optimaal voor de diverse types medewerkers die in een organisatie werken. Met de opkomst van mobiel werken doen steeds meer mobiele devices hun intrede op de werkvloer. Bovendien krijgen bedrijven meer oog voor de individuele behoeften van hun personeel op het gebied van laptops, smartphones en tablets. *One size does not fit all.*

Werknemers nemen hun devices van thuis mee (*Bring Your Own Device*, BYOD) of mogen kiezen uit een lijst opties van het bedrijf (*Choose Your Own Device*, CYOD). Bij sommige organisaties mogen medewerkers zelfs privé gebruik maken van de zakelijke laptops, smartphones of tablets (*Company-issued Personally-enabled*, COPE). Dat vraagt om een nieuwe manier van device management.

» **Lees ook** Kies je voor BYOD, CYOD en COPE?

Devices op basis van persona's

Iedere werknemer heeft eigen wensen als het op mobiele apparaten aankomt. Het is daarom slim om medewerkers te segmenteren en persona's te maken. Je krijgt dan een beter beeld van wie wat nodig heeft. Zo zullen

'De grote verscheidenheid van devices maakt deze taak niet eenvoudig'

'BYOD en CYOD vraagt om een nieuwe manier van device management'

medewerkers die veel onderweg zijn bijvoorbeeld behoefte hebben aan lichte laptops met een goede accu. Managers die veel in conference calls zitten, zijn vooral gebaat bij devices met uitstekend beeld en geluid.

» **Lees ook** Welk type werknemers heb jij?

De taak van een IT-afdeling

Aan de IT-afdeling de schone taak om alle (mobiele) apparatuur en bedrijfsdata efficiënt te beheren en beveiligen. Tegelijkertijd mag de productiviteit van de medewerkers niet in gevaar komen. De grote verscheidenheid van devices maakt deze taak niet eenvoudig. Elk besturingssysteem en merk heeft namelijk een eigen gebruiksaanwijzing.

Vroeger probeerden IT-beheerders de medewerkers dan ook vooral beperkingen op te leggen. Zo waren maar een klein aantal soort apparaten en apps toegestaan. Gelukkig is er vandaag de dag veel meer mogelijk om het beheer van mobiele apparaten te versimpelen, zelfs bij een grote diversiteit aan apparaten en apps. Denk aan oplossingen als Mobile Device Management, Mobile Application Management (MAM), Enterprise Mobility Management (EMM) en Unified Endpoint Management (UEM). Ontdek in deze whitepaper welke oplossing bij jouw organisatie past.

Wist je dat...

... je tot wel 30 procent kosten kunt besparen dankzij devicemanagement? MDM al sinds 1999 bestaat? En dat IT wel wil innoveren, maar tegengewerkt wordt?

» Tot 30% kostenbesparing

Volgens VMware, een aanbieder van Unified Endpoint Management (UEM), kan de manier waarop desktops, laptops en mobiele devices worden beheerd beter. Volgens deze partij kan het je per gebruiker een kostenbesparing van 15 tot 30% opleveren.

» Meer dan 20 jaar oud

Wist je dat Mobile Device Management zoals we het nu kennen al in 1999 ontstond? Met de BlackBerry Enterprise Server (BES) konden gebruikers hun e-mail synchroniseren met de e-mail op hun computer én hun data wissen indien de BlackBerry bijvoorbeeld gestolen werd.

» Vertraagde implementatie

Nieuwe technologieën zullen de komende jaren flinke impact hebben op onze manier van werken. Het beheer zal dan ook steeds meer een uitdaging worden voor IT. Waarom zijn we hier dan nog niet mee aan de slag? Uit onderzoek van HP blijkt dat IT-managers het seniormanagement als de grote schuldige zien. 25% zegt dat de bedrijfstop dwarsligt bij de implementatie.

» **Lees ook** dit zijn de belangrijkste trends volgens IT-professionals

» AVG-proof

Beveiliging van je data is belangrijker dan ooit. Onder de nieuwe Europese privacywet AVG kan een datalek fikse boetes opleveren. De Autoriteit Persoonsgegevens kan je een boete opleggen van 4% van de jaaromzet of 20 miljoen euro.

» **Lees ook** een jaar na invoering AVG: heb je hier al aan gedacht?

» 4,3 apparaat per werknemer

Marktanalist IDC verwachtte vijf jaar geleden dat bedrijven tegen 2020 gemiddeld 4,3 apparaten per medewerker moeten ondersteunen als de aantallen op de werkvloer zo blijven groeien als ze nu doen. Ze zaten er niet ver naast. Gemiddeld heeft een werknemer twee telefoons (zakelijk en privé) op het werk, een zakelijke laptop en nog een tablet of ander privé device die hij ook zakelijk gebruikt.

Zo versimpel je het beheer

Benieuwd welke opties er allemaal zijn om het beheer te versimpelen? Ontdek de belangrijkste oplossingen. Per oplossing leggen we uit waar het voor dient en waar je op moet letten.

‘MDM draait om het op afstand beheren van alle mobiele devices binnen een bedrijf’

01 Mobile Device Management (MDM)

Grote kans dat je al wel eens gehoord hebt van deze vorm van mobile device beheer. Mobile Device Management (MDM) draait om het op afstand beheren van alle mobiele devices binnen een bedrijf (op kantoor en daarbuiten) vanaf één centraal punt. Daarnaast worden ook alle software, instellingen, gebruikersrechten en het beveiligingsbeleid geregeld. Ook is het mogelijk om bijvoorbeeld bij diefstal van een device de inhoud op afstand te wissen.

Uitdagingen Mobile Device Management (MDM)

Het managen van mobile devices is een goede stap in de juiste richting, maar dan ben je er nog niet. Security draait niet alleen om de apparaten zelf, maar vooral ook om apps en data.

Medewerkers gebruiken steeds vaker hun eigen laptop, tablet of telefoon voor hun werkzaamheden (Bring Your Own Device). Het is dan van cruciaal belang om goede afspraken te maken over het beheer. Wie is bijvoorbeeld verantwoordelijk voor de beveiliging van het apparaat en voor de bedrijfsdata die erop staat?

Daarbij komt ook privacy om de hoek kijken. Als een apparaat gestolen wordt, wil je gegevens en apps kunnen wissen zonder dat de privacy van de gebruiker in gevaar komt. Veel bedrijven bouwen daarom bij alle devices de mogelijkheid in om op afstand apparatuur te vergrendelen of data te wissen. Als een device gestolen wordt of zoek raakt, kan zo een datalek worden voorkomen. Maar bij BYOD mag dat niet zondermeer. Daarover zul je dus vooraf goede afspraken moeten maken.

Een ander nadeel is dat MDM op Android niet goed werkt. Dit komt voornamelijk doordat er zoveel verschillende Android-apparaten en versies zijn. Als je MDM los gebruikt (niet binnen een systeem voor Enterprise Mobility Management, EMM), zijn de implementatiekosten aan de hoge kant.

02 Mobile Application Management (MAM)

Applicatiebeheer wordt steeds belangrijker, zeker bij grote organisaties. Mobile Application Management (MAM) richt zich specifiek op het beheer van de software op mobiele devices. Welke apps wil je wel en niet toestaan binnen je bedrijf? Je kunt bijvoorbeeld een Enterprise App Store aanbieden waar medewerkers goedgekeurde

‘Met MAM bied je de gebruiker meer vrijheid met een privé-apparaat’

en ondersteunde apps kunnen downloaden. Een groot voordeel van MAM is dat je de gebruiker meer vrijheid biedt met een privé-apparaat dan met MDM.

Uitdagingen Mobile Application Management (MAM)

Toch krijg je bij Mobile Application Management (MAM) nog steeds te maken met de ingeperkte vrijheid van medewerkers. Dit speelt voornamelijk bij medewerkers die hun eigen device voor hun werk gebruiken. Een oplossing daarvoor is om het device softwarematig te verdelen in een zakelijke en privé-omgeving. Zo voorkom je tegelijkertijd ook dat bedrijfsgegevens weglekken tijdens privégebruik.

03 Mobile Content Management (MCM)

Worden binnen jouw bedrijf veel bestanden met gevoelige informatie gedeeld? Dan heb je te maken met een flink beveiligingsrisico. Als je hier geen richtlijnen voor maakt, is de kans groot dat medewerkers deze documenten rondmailen of gebruikmaken van applicaties als Dropbox, Google Drive en Wetransfer. Dit werkt uiteraard snel, maar de beveiliging van deze diensten is niet altijd optimaal. Mobile Content Management (MCM) maakt het mogelijk om op een veilige (versleutelde) en eenvoudige manier content uit te wisselen.

‘In plaats van losse devices en apps te beheren, werk je bij EMM met gebruikersprofielen’

‘Met MCM kun je op veilige en eenvoudige manier content uitwisselen’

Uitdagingen Mobile Content Management (MCM)

Bij sommige MCM-systemen moet de gebruiker veel extra stappen doorlopen om bij de juiste documenten te komen. Dit zorgt voor ergernis en tijdverlies. In een goed MCM-systeem kan de gebruiker snel bij alle bestanden en is samenwerken geen probleem. Controleer bij het kiezen van een MCM-systeem ook welke besturingssystemen worden ondersteund. Veel bedrijven staan het gebruik van verschillende soorten devices met verschillende soorten besturingssystemen toe. Belangrijk is dat de gebruikerservaring van MCM op al die systemen goed is.

04 Enterprise Mobility Management (EMM)

Mobile Device Management, Mobile Application Management en Mobile Content Management zijn los van elkaar al handig, maar het is slimmer om ze te combineren. Dit kan met Enterprise Mobility Management. In plaats van dat je losse devices en groepen apps beheert, werk je bij EMM met gebruikersprofielen. Hier kun je zien welke devices en apps een medewerker gebruikt, maar ook tot welke documenten iemand toegang moet hebben.
Op zoek naar een geschikt EMM-systeem?

Onderzoeksbureau Gartner heeft drie kenmerken opgesteld van een goede EMM-oplossing.

- De gebruiker moet content op een veilige plek kunnen opslaan binnen het device.
- Er moet content kunnen worden gepusht van de IT-afdeling naar het device.
- De gebruiker moet via een veilige verbinding toegang kunnen krijgen tot een *back-end* waar ze op een veilige manier content vandaan kunnen halen.

5 Unified Endpoint Management (UEM)

Unified Endpoint Management (UEM) gaat nog een stap verder. Het is EMM, maar dan inclusief het beheer van alle apparaten: van de mobiele devices zoals de smartphones, tablets en laptops die je ook met MDM kunt beheren tot aan de desktops en slimme Internet of Things (IoT)-apparaten. Het is de missende schakel tussen MDM en traditionele managementtools. Als IT-beheerder kun je eenvoudig policies inregelen en rechten toewijzen. Die kun je uiteraard ook weer intrekken, zo voorkom je met UEM dat gevoelige gegevens in de verkeerde handen vallen.

Snel van start met AutoPilot
Krijgen jouw medewerkers nieuwe devices? Nu worden de nieuwe laptops meestal eerst op kantoor bezorgd en ingesteld door de IT-afdeling. Vervolgens komen alle medewerkers naar kantoor om hun laptop op te halen. Dat kan makkelijker. Windows AutoPilot stelt gebruikers in staat de installatie van een nieuw Windows 10-apparaat zelf te doen. Zonder begeleiding van de IT-afdeling dus. Daardoor kan de eindgebruiker (de medewerker) het apparaat direct van de leverancier thuis ontvangen. En de IT-afdeling? Die hoeft enkel de nieuwe devices op afstand te (laten) registreren.

» **Lees ook** alles wat je moet weten over Windows Autopilot

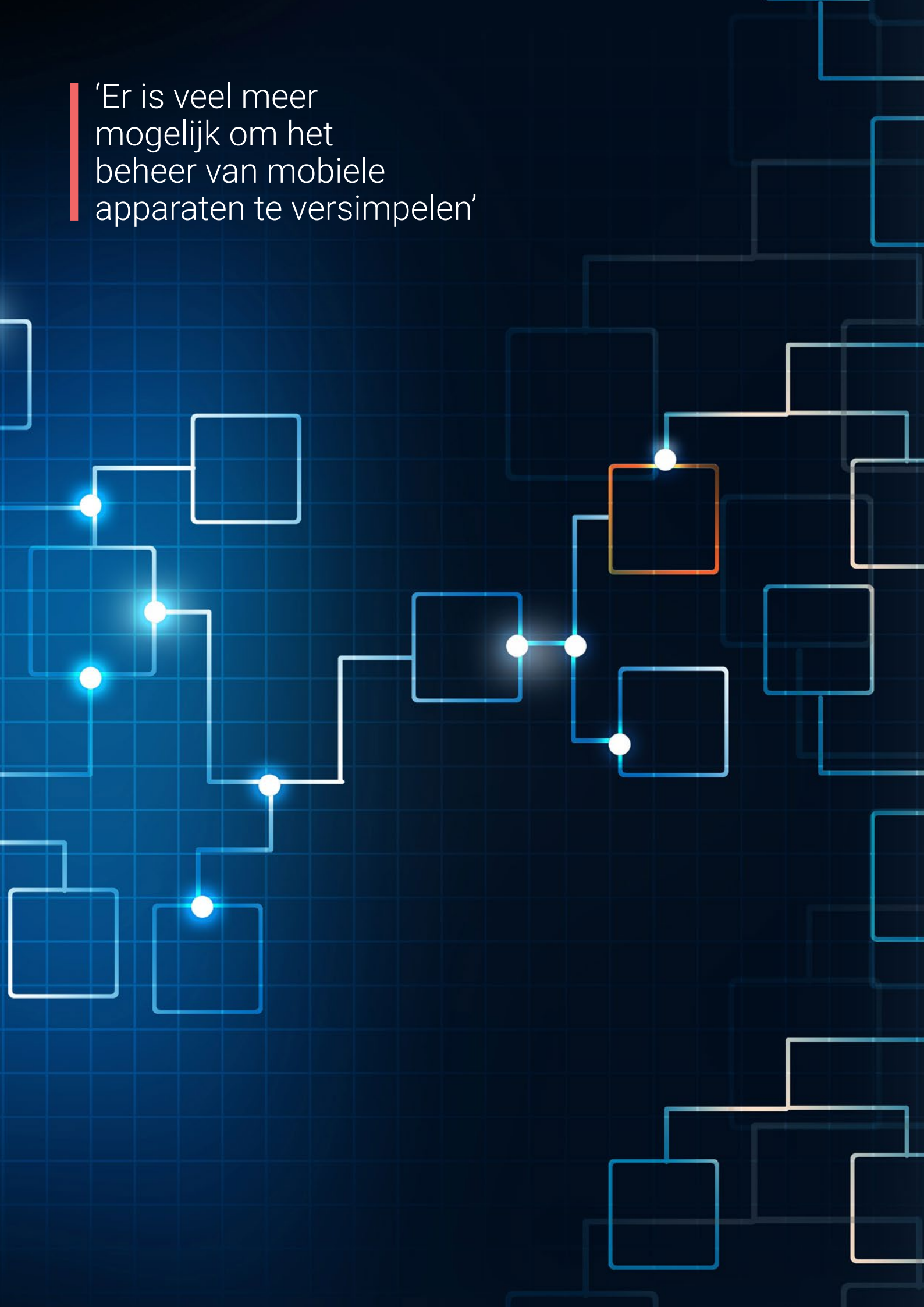
‘UEM gaat nog een stap verder: hiermee beheer je ook desktops en slimme Internet of Things (IoT)-apparaten’

UEM werkt alleen met Windows 10, hierdoor is apparaatbeheer in de cloud mogelijk. De IT-afdeling kan alle instellingen op een device op afstand configureren. Denk aan de VPN, het verplichten van wachtwoorden en encryptie, maar ook het bepalen welke apps geïnstalleerd mogen worden. Daarnaast kun je updates en patches pushen. Gebruikers kunnen via de beveiligde cloudomgeving bij alle bestanden en apps. Het maakt hiervoor niet uit welk device wordt gebruikt. Daarnaast kan een apparaat op afstand worden gevonden en gewist.

Uitdagingen Unified Endpoint Management (UEM)

Helaas zijn er ook een aantal nadelen aan UEM. Deze beheervorm is een stuk ingewikkelder dan de voorgenoemde oplossingen. Het configureren en updaten van de BIOS en firmware van componenten gaat bijvoorbeeld nog erg lastig. Ook het feit dat UEM alleen met Windows 10 werkt, kan voor problemen zorgen.

‘Er is veel meer mogelijk om het beheer van mobiele apparaten te versimpelen’



Vind de oplossing die bij je past

Er zijn diverse device managementoplossingen. Maar welke past bij jouw organisatie? Gebruik dit stappenplan om daarachter te komen.

Stap 1 Breng je huidige situatie in kaart

Hoe beheer je de mobile devices binnen je bedrijf op dit moment? Maak je bijvoorbeeld al gebruik van Mobile Device Management (MDM)? Dan is het slim om uit te breiden met Mobile Application Management (MAM).

Heb je nog niets geregeld? Dan kun je beter kiezen voor Enterprise Mobility Management (EMM) of Unified Endpoint Management (UEM). Deze combineren de MDM, MAM en MCM in één pakket. Deze pakketten zijn vaak goedkoper. Wil je graag ook het beheer van je laptops en desktops in één dashboard hebben? Dan kies je voor UEM. Houd er wel rekening mee dat deze oplossing behoorlijk ingewikkeld kan zijn. Laat je hierover dus goed voorlichten.

Stap 2 Onderzoek het deelgedrag van je medewerkers

Worden binnen je organisatie veel gevoelige documenten gedeeld? Dan is het slim om te kijken naar een Mobile Content Management (MCM)-oplossing. Is dit op jouw bedrijf nu (en in de toekomst) niet van toepassing? Dan heb je deze oplossing niet nodig.

Stap 3 Kies een aanbieder

Per soort oplossing zijn er veel verschillende aanbieders. Heb je deskundig advies nodig bij het kiezen van een beheeroplossing? Neem dan contact op met HP of een IT-partner voor persoonlijke tips.

Contact opnemen met HP of een IT-partner kan via:
ikwilmobielwerken.nl/meer-informatie

Colofon
Dit is een uitgave van MT MediaGroep BV in opdracht van HP.

Redactie
Pauline Veenstra, redactie Management Team

Februari 2020