Bouwen aan een succesvolle **Enterprise Mobility-strategie**

MobileIron®

Deze white paper werd mogelijk gemaakt door de sponsoring van MobileIron.

proximus

Op weg naar **een moderne mobiele onderneming**

Het voorbije decennium is de mobiliteit wereldwijd ongekend snel gegroeid. Sinds de komst van de eerste iPhone in 2007 hebben mobiele toestellen sneller dan eender welke andere technologie in de geschiedenis ingang gevonden. Mobiele IT heeft alles veranderd.

Applicaties zijn niet langer gebonden aan de desktop en gebruikers verwachten dat ze naadloos kunnen switchen tussen desktops, tablets, en smartphones - eender waar en wanneer. Vandaag evolueert de multichannelbenadering naar een omnichannelervaring en wordt ze het nieuwe normaal voor alle consumenten.

De 'Bring Your Own Device'- trend heeft voet aan de grond gekregen in organisaties, omdat bedrijven steeds vaker de voordelen erkennen om hun medewerkers hun persoonlijke mobiele toestellen voor professionele doeleinden te laten gebruiken. Bedrijven gaan de mobiele toer op, met of zonder de uitdrukkelijke instemming - of zelfs het medeweten - van hun bestuursorganen. Vaak wordt de mobiliteitstrend aangestuurd vanuit de organisatie zelf, omdat marketingdepartementen, line of business-managers en early adopters de nood aan een mobiele strategie versnellen.

Het thema van mobiliteit binnen de onderneming gaat verder dan de eigen medewerkers. Steeds vaker maken klanten, maar ook leveranciers, onderaannemers en andere belangrijke stakeholders in uw ecosysteem, gebruik van mobiele toestellen om informatie over uw bedrijf en producten te verzamelen, in contact te komen met verkoop- en managementpersoneel, en om producten en diensten aan te kopen of te leveren.

Een efficiënte bedrijfsvoering vereist van IT-organisaties dat ze tegemoetkomen aan de wensen van hun mobiele gebruikers en tegelijk het gebruik monitoren en beheren om de veiligheid en beveiliging te verzekeren. Bedrijven hebben nieuwe strategieën en technologieën nodig om vol vertrouwen hun mobiele traject af te leggen.

Zoals u zult merken bij het lezen van deze pagina's is enterprise mobility (mobiliteit binnen de onderneming) meer dan gewoon de laatste technologie kopen of e-mail op de gsm van een medewerker installeren. Mobiliteit draait rond het transformeren van uw business om nieuwe productiviteitsbronnen te doen ontstaan. Proximus kan u helpen om een gezonde strategie voor enterprise mobility uit te bouwen en u bijstaan in het veilig transformeren van uw kritieke bedrijfsprocessen met bewezen, toonaangevende enterprise mobility-oplossingen en professionele diensten.

Een allesomvattende benadering van **enterprise mobility**

EMM, het fundament van uw enterprise mobility-strategie.

Als u van plan bent alles op een mobiel platform te beheren, dan is Enterprise Mobility Management (EMM) het vertrekpunt. EMM-oplossingen connecteren mobiele toestellen met workflows van het bedrijf en ondersteunen tegelijk de voortdurende schommelingen qua aantal en types toestellen. Organisaties maken gebruik van EMM-systemen en -diensten voor provisioning, tracking & auditing, support en databescherming. EMM is de navelstreng die mobiele toestellen met hun bedrijfsinfrastructuur verbindt.

Drie essentiële technische functies van EMM helpen IT-afdelingen bij de uitvoering van deze diensten, waarvan sommige overlappen. Organisaties kunnen al deze hulpmiddelen of sommige ervan gebruiken, afhankelijk van hun vereisten.

1 Mobile Device Management (MDM)

Is een onderliggende technologie die op afstand de levenscyclus van mobiele toestellen en hun respectieve platformen beheert. MDM omvat doorgaans de installatie van unieke profielen op mobiele toestellen, zodat organisaties op afstand smartphones en tablets kunnen controleren en versleutelen en ze deze toestellen regels kunnen opleggen. Ze kunnen bijvoorbeeld worden gebruikt om alle apps en data van een toestel te wissen als het verloren of gestolen is[1] . MDM biedt bedrijven ook momentopnames van de voorraad of de levering van toestellen, of van de configuratie van het besturingssysteem, en levert tools om problemen op afstand te bekijken en te controleren.

2 Mobile Application Management (MAM)

Dankzij Mobile Application Management-tools (MAM) kunnen organisaties zich toeleggen op het beheer van hun mobiele applicaties in plaats van de hardware. MAM omvat het uitrollen en updaten van mobiele apps, met inbegrip van administratieve pushondersteuning en licentiebeheer van de apps. MAM stelt organisaties ook in staat om beveiligings- en controlepolicy's individueel op deze apps toe te passen en ze selectief - inclusief bijbehorende data - van een specifiek toestel te verwijderen. Zo kan de bedrijfsinformatie worden beschermd zonder dat een toestel volledig moet worden leeggemaakt. MAM biedt ook analysefuncties, waarmee administrators en application owners de gebruikspatronen kunnen begrijpen.

[1] De NMBS heeft voor de periode 2011-2016 in totaal 17.589 gsm's gerapporteerd die werden gevonden in treinen.

3 Mobile Content Management (MCM)

Met Mobile Content Management (MCM) krijgen professionele gebruikers toegang tot content op hun mobiele toestellen. Volgens Gartner[2] heeft MCM drie fundamentele rollen. Een ervan is het opleggen van policy's. Voorbeelden hiervan zijn voorwaardelijke toegang tot bijlagen in e-mail, bestanden die worden gesynchroniseerd met een back-end repository of bestanden die worden gesynchroniseerd met een cloud repository. Een andere rol van MCM is content push, wat betekent dat de MCM-tool regels oplegt voor push-gebaseerde verdeling, vervanging en schrapping van bestanden. Integratie is een andere taak die aan Mobile Content Management wordt toegewezen: naast de basispolicy's voor toegang tot bestanden voegen MCM-tools mobiele compatibiliteit toe voor systemen voor het beheer van rechten van derden, alsook oplossingen voor Enterprise Data Loss Protection (EDLP) en Enterprise Digital Rights Management (EDRM).

[2] Gartner, Magic Quadrant for Enterprise Mobility Management Suites, 6 juni 2017

De almaar grotere footprint van **Enterprise Mobility Management**

Leveranciers gebruiken verschillende benaderingen om de mobiele levenscyclus te beheren en de behoeften van organisaties variëren heel sterk afhankelijk van de sector. De meeste klanten maken gebruik van MDM, MAM en MCM-functies. Andere functies, zoals Mobile Identity and Access Management (MIA), Mobile Information Management (MIM), Mobile Expense Management (MEM) en Containment, om er maar enkele te noemen, worden door een kleiner deel gebruikt.

Unified Endpoint Management (UEM)

Niettemin evolueert EMM verder dan zijn oorspronkelijke toepassingsdomein, dat bestaat uit het beheer van mobiele toestellen, apps en content, omdat client computing versmelt met mobile computing om computing groups van eindgebruikers te vormen. 'De definitie van EMM evolueert: terwijl EMM vroeger vooral draaide rond het beheer van mobiele toestellen en applicaties, behelst het nu meer het mogelijk maken van mobiliteit in de ruimere zin – met uitbreiding naar toestellen met Windows 10 en MacOS-toestellen', aldus David Johnson, hoofdanalist bij Forrester Research[3].

Dit heeft de nood teweeggebracht aan een unieke oplossing, die zowel traditionele toestellen van klanten als mobiele toestellen beheert. Microsoft en Apple hebben MDM API's aan hun platformen toegevoegd om deze convergentie te vergemakkelijken. De grootste uitdaging voor het implementeren van Unified Endpoint Management is dat organisaties doorgaans traditionele vereisten hebben, zoals complexe Win32-applicaties en Windows GPO's, waar EMM-tools op dit ogenblik geen raad mee weten. Momenteel voltrekken zich veranderingen die EMM-tools steeds beter geschikt zullen maken om pc's te beheren. Vooreerst gaat Microsoft verder met het verbeteren van de MDM API's in Windows 10, waardoor de kloof met de GPO's wordt gedicht. Daarnaast bieden EMM-leveranciers bedrijfseigen mogelijkheden om deze lacunes weg te werken in domeinen zoals beveiligingspolicy's, het beheer van scripts en de uitrol van Win32-applicaties.

> "EMM breidt uit naar Unified Endpoint Management - dat EMM-functies combineert met pc's en laptops van klanten, zowel uit het oogpunt van bedrijfstoestellen als van BYOD. EMM-platformen breiden ook uit naar niet-traditionele geconnecteerde eindpunten, zoals wearables, digital signage, kiosken, en andere IoT-gerelateerde scenario's"[4].
>
> **Phil Hochmuth**, Enterprise Mobility Research Program Director bij IDC

Er moet echter worden opgemerkt, dat niet alle IoT-objecten binnen het toepassingsdomein van de EMM-tools zullen vallen. Sommige toestellen zullen rechtstreeks door de fabrikanten worden beheerd of bedrijfsspecifieke beheerstools hebben. En voor heel wat toestellen zal er helemaal geen beheer nodig zijn. Hoe dan ook is het duidelijk dat de diversiteit en het aantal toestellen zullen blijven groeien, en dat IT-organisaties voorbereid moeten zijn.

[3] Matt Kapko, What is EMM? Enterprise Mobility Management explained, Computerworld, 9 oktober 2017
[4] Phil Hochmuth, IDC MarketScape: Worldwide Enterprise Mobility Management Software 2017 Vendor Assessment, augustus 2017

Uw business beschermen **tegen mobiele bedreigingen**

Het opleggen van policy's zal niet voor eeuwig en altijd volstaan als antwoord op mobiele beveiligingsproblemen. Tegen 2019 zal mobiele malware goed zijn voor een derde van de totale malware die in standaardtests wordt gerapporteerd, een forse toename t.o.v. de 7,5% vandaag, volgens Dionisio Zumerle, Research Director voor mobiele beveiliging bij Gartner[5].

Mobile Threat Protection (MTP)

Afhankelijk van de sector, de toepasselijke regelgeving, de gevoeligheid van de gegevens, specifieke gebruiksgevallen en de risicocultuur, moeten organisaties ernstig overwegen om, geleidelijk maar wel zonder dralen, Mobile Threat Protection-oplossingen in te voeren. Sterk gereguleerde instellingen, zoals financiële instellingen, en gevoelige organisaties, zoals gezondheidszorginstellingen, zouden er goed aan doen om beter vroeg dan laat voor MTP-oplossingen te kiezen.

Hoewel de markt voor de bescherming tegen mobiele bedreigingen aan belang wint, is er nog altijd heel wat verwarring en onzekerheid bij eindgebruikers i.v.m. welke risico's MTP onder controle kan houden en hoe dringend of nuttig MTP kan zijn. Uiteraard is het gebruik van detectie van mobiele bedreigingen en de bescherming ertegen geen klein bier: om doeltreffend te zijn, moet de technologie bedreigingen op het niveau van de gebruikers, applicaties, toestellen (iOS, evenals Android-toestellen en -tablets) kunnen aanpakken.

MTP-oplossingen moeten niet alleen in staat zijn om afwijkend gedrag te detecteren door verwachte of aanvaardbare gedragspatronen te traceren, ze zouden ook mobiele toestellen moeten kunnen inspecteren op zwakke plekken in de configuratie, die de deur kunnen openen voor malware. MTP-systemen zouden in staat moeten zijn om netwerkverkeer te monitoren, verdachte connecties te verbreken en applicaties te scannen om te identificeren welke ervan bedrijfsdata in gevaar zouden kunnen brengen.

En bovenal moeten IT-organisaties bijzondere aandacht hebben voor het selecteren van een MTP-oplossing die optimaal met hun EMM-tools integreert.

Mobiele malware is in 2016 op jaarbasis met meer dan

100%

toegenomen, wat neerkomt op ca.

7.5%

van alle malware

(bron: AV-TEST T Security Report 2015/16)

[5] Gartner, *Market Guide for Mobile Threat Defense Solutions*, 22 augustus 2017

Proximus Enterprise Mobility Management

Bij Proximus beschouwen we EMM als het centrale integratiepunt voor mobiele policy's. Omdat het de hoeksteen is voor het beheer van mobiele middelen op ondernemingsniveau, is **Proximus EMM** het uitgelezen platform om **policy's voor andere diensten en tools samen te voegen.**

Dankzij haar ruime mogelijkheden om te integreren met infrastructuurcomponenten van derden biedt onze EMM-oplossing een gemeenschappelijke, platformoverschrijdende basis om **toestelpolicy's** op te stellen, te controleren, te valideren, te handhaven en te actualiseren **voor een ruim aanbod van tools en diensten**, zoals gateways, proxy's, VPN's, netwerktoegangscontroles en -certificaten, applicatiecertificaten, content- en rechtenbeheersystemen, identiteits- en toegangsbeheer, versiecontrole en -back-ups, systeemupdates, of het initialiseren en wissen van toestellen.

Als uniek punt inzake policy's en verantwoordelijkheid biedt Proximus EMM de mogelijkheid om werknemerinflatie te vermijden, doordat een massa add-on utilities beslag leggen op lokale resources, wat de taak van het coördineren van policy's voor de systeembeheerders bemoeilijkt.

Proximus EMM omvat een bijkomende functionaliteit die voorwaardelijke toegang biedt tot cloud archieven (MI Access). In tegenstelling tot traditionele beveiligingsbenaderingen correleert onze oplossing de identiteit van de gebruiker met unieke informatiefeeds, zoals toestand van het toestel en status van de apps. Proximus EMM verzekert dat de bedrijfsgegevens binnen de vastgelegde IT-grenzen blijven, zodat ze niet kunnen worden opgeslagen op niet-beveiligde toestellen, geen verbinding kunnen maken met niet-beheerde apps, of geen informatie kunnen uitwisselen met niet-goedgekeurde clouddiensten.

Dankzij onze EMM-oplossing maken organisaties gebruik van een op normen gebaseerde benadering die gelijk welke clouddienst kan beveiligen, waaronder Office 365, zonder dat bedrijfsspecifieke integraties nodig zijn.

1 MDM-component

De **MDM**-component van onze oplossing omvat de basis van gelijk welke EMM-oplossing, doordat hij **IT in staat stelt om medewerkers te helpen productief te zijn op hun geprefereerde mobiele toestellen en desktops, mobiele toestellen en desktops** te beveiligen en te beheren voor verschillende besturingssystemen (waaronder Android, iOS, macOS en Windows 10), bedrijfs-e-mail te beveiligen, toestellen automatisch te configureren, en op certificaten gebaseerde beveiliging te leveren. MDM stelt administrators in staat om op selectieve wijze bedrijfsgegevens van mobiele toestellen en desktops te wissen, zonder impact op de persoonlijke gegevens.

2 MAM-capabilities

Dankzij de **MAM**-functies **kan IT een etalage van bedrijfsapps opbouwen** en onderhouden, applicaties op gelijk welk toestel beveiligen, eindgebruikers op het toestel authenticeren, en bedrijfs- en persoonlijke apps op mobiele toestellen en desktops scheiden.

3 MCM-module

De **MCM**-module stelt IT in staat om **bedrijfsgegevens op mobiele toestellen en desktops te beveiligen**, zonder de eindgebruikerservaring in het gedrang te brengen. Gebruikers kunnen op een intuïtieve manier documenten raadplegen, ze van commentaar voorzien en ze delen vanuit e-mail, SharePoint, en andere systemen voor het beheer van bedrijfsconten, alsook bedrijfs- en persoonlijke clouddiensten.

Proximus EMM: al de stakeholders van uw onderneming hebben er baat bij

Voordelen voor de onderneming: beveiliging en conformiteit

- Helpt uw onderneming in overeenstemming te zijn met de Algemene Verordening Gegevensbescherming van de EU (AVG).
- Zorgt ervoor dat er geen kritieke informatie in verkeerde handen terechtkomt wanneer een toestel gestolen wordt of verloren raakt.
- Belet dat, al dan niet opzettelijk, data worden gelekt aan derden.
- Uw werknemers krijgen enkel toegang tot de data waarvoor ze toestemming hebben.

Voordelen voor de IT-medewerkers: controle en gebruiksgemak

- Eenvoudig, veilig beheer van de vloot van toestellen
- Efficiënte uitrol van vooraf geconfigureerde mobiele toestellen
- Biedt een overzicht van alle mobiele toestellen in uw onderneming, waar ze zich bevinden en wie ze gebruikt.
- Laat toe om gebruikers en mobiele toestellen in bulk te registreren en er policy's aan toe te wijzen, zonder dit toestel per toestel, gebruiker per gebruiker te moeten doen.

Voordelen voor de medewerkers: juist evenwicht tussen beveiliging, gebruikerservaring en productiviteit

- Laat uw medewerkers toe om op gelijk welke locatie op een veilige manier te werken.

Proximus Unified Endpoint Management

Terwijl EMM al voor de meest voorkomende gebruiksscenario's voor pc-beheer een oplossing biedt, waren er tot hiertoe een aantal hiaten in het EMM-model die verhinderden dat IT weg zou evolueren van de traditionele tools voor pc-beheer.

Proximus UEM verzoent de mobiele wereld en de desktopwereld. Het breidt de EMM-functies uit en biedt IT-teams een vereenvoudigde manier om de **beveiliging en het beheer voor Windows 10 te moderniseren**, zonder de fijnmazige policy's en acties die ze de voorbije twintig jaar hebben opgebouwd, op te offeren.

Onze UEM-oplossing stelt IT-teams in staat om makkelijker af te stappen van een duur en verwarrend model met twee snelheden, waarbij pc's worden beheerd door traditionele tools en mobiele toestellen door moderne tools. Scripts die gebruikmaken van GPO's kunnen nu bestaan naast EMM-profielen, zonder de nood aan traditionele pc-beheerstools. Alle commando's kunnen nu gebruikmaken van het EMM-protocol om informatie naar het toestel te sturen, ongeacht of het een script is, dan wel een EMM API. Dit betekent dat IT-departementen kunnen focussen op het verhogen van de organisatorische productiviteit, met meer efficiëntie en wendbaarheid, en tegen lagere kosten - dit alles zonder de veiligheid van het toestel in het gedrang te brengen voor gebruikers die in een modern bedrijf vaak onderweg zijn.

Voordelen

Proximus UEM stelt IT-teams in staat om:

- Dankzij EMM volledige controle over pc's te hebben
- Pc's op afstand draadloos te beheren
- De noodzaak te verminderen om desktops te 'imagen'
- Gebruik te maken van op GPO gebaseerde commando's met PowerShell-scripts die door EMM worden geïmplementeerd
- Registry makkelijk te bewerken en te beheren
- Niet-MSI wrapped Win32-apps probleemloos uit te rollen
- De zichtbaarheid van het bestandssysteem te vergroten

Proximus UEM ontsluit mogelijkheden op het vlak van pc-beheer, die voorheen niet mogelijk waren met EMM, zoals:

- Randapparatuur definiëren
- Snelkoppelingen op het bureaublad maken
- Nagaan welke hardware met het toestel is verbonden
- Zicht hebben op de software op het toestel
- Begrijpen welke bestanden in een map zijn opgeslagen
- Meer zicht hebben op het register
- Wijzigingen aan het register aanbrengen
- Nutteloze of ongewenste software van het toestel verwijderen, ook wanneer het een systeemapp is

Proximus Mobile Threat Protection

Terwijl EMM-oplossingen instaan voor het beheer en het opleggen van policy's, zijn ze niet bedoeld om specifiek de beveiligingsstatus van een mobiel toestel te behandelen, omdat ze geen informatie over bedreigingen bieden of malware detecteren.

Toch zijn mobiele bedreigingen in opmars, en neemt de hoeveelheid malware in app stores toe. De inzet is groter dan ooit:

> Het Ponemon Institute[6] raamt de gemiddelde kosten van een inbreuk op de bedrijfsgegevens op 18.000 EUR per dag.

Proximus MTP maakt gebruik van detectie van kwaadwillige apps om bekende en onbekende bedreigingen op te sporen door middel van de emulatie van bedreigingen, geavanceerde analyse van statische code, de reputatie van apps en machinaal leren. Zijn dynamische reactie op bedreigingen belet dat gecompromitteerde toestellen toegang krijgen tot het netwerk van uw organisatie, terwijl uw organisatie aanpasbare policycontroles kan instellen.

Proximus MTP biedt IT- en Security-teams de mogelijkheid om:

- Geavanceerde app-analyses uit te voeren om bekende en onbekende bedreigingen te detecteren
- Netwerkactiviteit op verdacht of kwaadwillig gedrag te monitoren
- Kwetsbaarheden op het niveau van het toestel (OS) te evalueren om het aanvalsoppervlak te verkleinen
- Sms-phishingaanvallen die bedoeld zijn om inloggegevens van bedrijven te stelen, te detecteren en te blokkeren

Proximus MTP zal de performantie van de toestellen of de levensduur van de batterij nooit negatief beïnvloeden, omdat de risicoanalyse grotendeels in de cloud wordt uitgevoerd. De app op het toestel draait feilloos op de achtergrond tot een kwaadwillige activiteit wordt gedetecteerd, en de gebruiker wordt verwittigd om actie te ondernemen.

[6] Ponemon Institute, *2016 Cost of Cyber Crime Study & the Risk of Business Innovation*, oktober 2016

Integratie met EMM

Door naadloos te integreren met Proximus EMM – en ook met de meeste EMM-oplossingen op de markt – biedt Proximus MTP een uitgebreid platform, dat een kritieke beveiligingslaag toevoegt aan de Enterprise Mobility Management-oplossingen. Onze MTP-oplossing kan worden gebruikt om op een dynamische manier toegangsprivileges te wijzigen om risiconiveaus weer te geven, waarbij statische beheerspolicy's worden omgezet in actieve bescherming van toestellen.

Hoeveel toestellen u ook in uw mobiele vloot hebt, de integratie van Proximus MTP met uw EMM-platform gaat snel en makkelijk. De uitrol en het beheer kunnen automatisch via uw EMM gebeuren, wat de toepassing versnelt en de totale operationele kosten vermindert. Onze oplossing schaalt op met uw EMM, waardoor geregistreerde mobiele toestellen naadloos worden beschermd. Daardoor kunt u zeker zijn dat u de nodige beveiligingslagen hebt om uw mobiele toestellen te beheren en te beschermen, zelfs in een uiterst dynamische omgeving.

Voordelen

- In alle vertrouwen eender welk mobiel toestel met iOS of Android in het netwerk van uw organisatie uitrollen
- Gevoelige informatie op mobiele toestellen beschermen tegen spionage
- De zichtbaarheid van en bescherming tegen de nieuwste mobiele bedreigingen verbeteren, met mobiele beveiliging die makkelijk met uw bestaande mobiliteits- en beveiligingsinfrastructuur integreert (MDM, MAM, NAC, SIEM, enz.)
- De beveiligingsmaatregelen van Microsoft Exchange en container/wrapper-oplossingen verbeteren
- Een snelle reactie mogelijk maken op platformoverschrijdende APT-aanvallen (Advanced Persistent Threat)
- Onderaannemers veilig toegang geven tot bedrijfsgegevens vanaf niet-beheerde toestellen
- De gebruikerservaring en privacy vrijwaren, en de bescherming toevoegen die organisatorische of regelgevingsmachtigingen vereisen

Waarom **Proximus** kiezen?

Gelet op het feit dat het gebruik van **smartphones naar verwachting zal stijgen van 1,47 miljard toestellen in 2016 tot meer dan 1,7 miljard in 2021**[7], spreekt het vanzelf dat organisaties een globale manier moeten vinden om een groot scala van toestellen van werknemers snel in de onderneming binnen te brengen en te beveiligen.

Dankzij de combinatie van toonaangevende technologieleveranciers - waaronder **MobileIron en Check Point Software Technologies** - en het uitgebreide professionele dienstenaanbod van Proximus kunnen organisaties aanspraak maken op de voordelen van mobiele oplossingen van een uitstekende kwaliteit.

Er is geen 'one-size-fits-all' benadering voor Enterprise Mobility Management, en heel wat ondernemingen stuiten op moeilijkheden op hun weg naar mobiliteit. Proximus kan u helpen alle mogelijke mobiele scenario's onder ogen te zien, plannen te maken voor de uitdagingen, een solide strategie uit te bouwen, de juiste technologieën te gebruiken, de gepaste policy's in te voeren, en de best practices aan te wenden om uw mobiele initiatief tot een succes te maken.

De behoeften kunnen sterk uiteenlopen volgens de grootte van de onderneming en het type van activiteit of volgens de voorwaarden van de regelgeving, en de EMM-vereisten veranderen naarmate de mobiele platformen evolueren. Om tred te houden met deze veranderingen kunt u een beroep doen op onze Proximus-experts om het veranderende landschap van de mobiele toestellen en de implicaties voor het beheer van de mobiliteit te begrijpen.

Proximus levert de Enterprise Mobile Management-oplossingen die organisaties nodig hebben om hun klanten beter te bedienen in de digitale wereld van vandaag, samen met de bijbehorende technische consultancydiensten en managed services. Een ander doel van Proximus is om end-to-enddiensten te leveren die worden omkaderd door duidelijke SLA's.

Onze Enterprise Mobile Management-oplossingen stellen u in staat om:

- Verlies van kritieke data te vermijden dankzij robuuste EMM- en MTP-oplossingen
- Complexiteit te beperken en kosten te drukken
- Uw databeheer en uw dagelijkse activiteiten te vereenvoudigen
- Uw IT-voetafdruk te verkleinen dankzij een uiterst efficiënt gebruik van resources
- Te begrijpen hoe risico's kunnen worden beperkt, de return on investment te analyseren om toekomstige investeringen te rechtvaardigen
- De huidige status van uw bedrijfswerking te beoordelen en een roadmap te ontwikkelen om toekomstige initiatieven te ondersteunen
- Service Level Agreements te verbeteren en de efficiëntie van uw organisatie op te drijven

Omdat we permanent aan de verbetering van onze managementsystemen werken, worden ze gecontroleerd en geauditeerd. Daarnaast monitoren en analyseren we onze resultaten en de feedback die we krijgen van klanten, medewerkers en andere stakeholders om zo onze doelstellingen en targets op het vlak van kwaliteit, beveiliging, veiligheid en milieu te bepalen.

[7] IDC, *Worldwide Quarterly Mobile Phone Tracker*, 29 augustus 2017

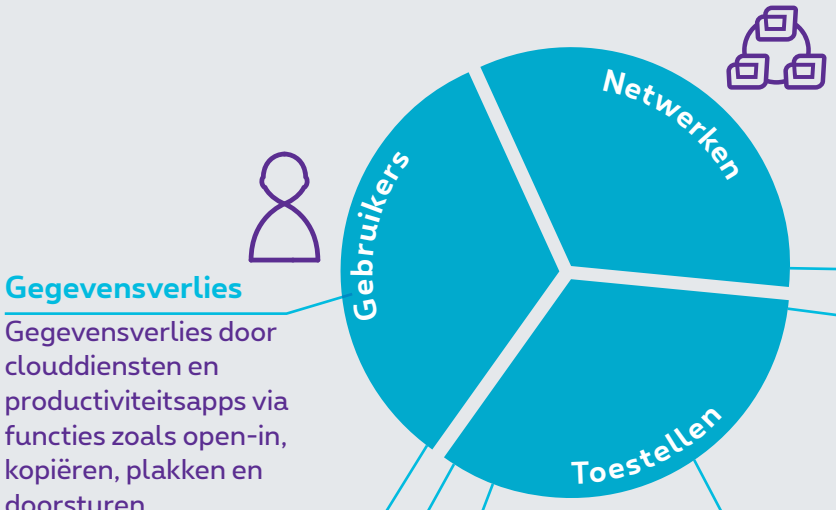
Infografieken en figuren

Mobile threat vectors

Een van de grootste mobiele uitdagingen die IT moet opnemen is het beveiligen van data en apps - inclusief apps van derden - op alle mobiele toestellen, zonder dat dit een impact heeft op de native gebruikerservaring. Vóór het mobiele tijdperk waren de belangrijkste beveiligingsrisico's malware en virussen, door de kwetsbaarheid van openbestandssystemen en een niet-beschermde kernel. Vandaag hebben mobiele besturingssystemen een gesandboxt bestandssysteem en een beschermde kernel, zodat traditionele beveiligingsbedreigingen minder aan de orde zijn. Mobiele technologieën hebben evenwel af te rekenen met drie andere types van bedreigingen: op basis van de gebruiker, het toestel en het netwerk.

Bedreigingsvectoren op mobiele toestellen verschillen van die op pc

Mobiele besturingssystemen met SandBox-technologie zijn veilig. Bedreigingen zoals malware worden verminderd door het OS design. Om gegevensverlies op mobiele toestellen te voorkomen moet men zich richten op verschillende risicovectoren.



Gegevensverlies

Gegevensverlies door clouddiensten en productiviteitsapps via functies zoals open-in, kopiëren, plakken en doorsturen

Manipulatie van toestellen

De zwakke plekken in het OS worden misbruikt voor jailbreaking, rooting, het omzeilen van de beveiliging en het installeren van kwaadwillige apps vanuit een niet-toegelaten app-store

Always On-connectiviteit

Mobiele toestellen zijn vaker online en hebben toegang tot gevoelige data via een niet-beveiligde verbinding. Daardoor stijgt het risico op gegevensverlies via "wifi-sniffing", onbetrouwbare access points en "Man in the Middle"-aanvallen

Kwaadwillige of risicovolle apps

Verzamelen en delen van gegevens, zoals persoonlijke identificatie en locatie, met publiciteitssystemen van derden en analysesystemen

De aard van het toestel

Door de aard van het toestel zelf kan het makkelijker gestolen worden of zoek raken

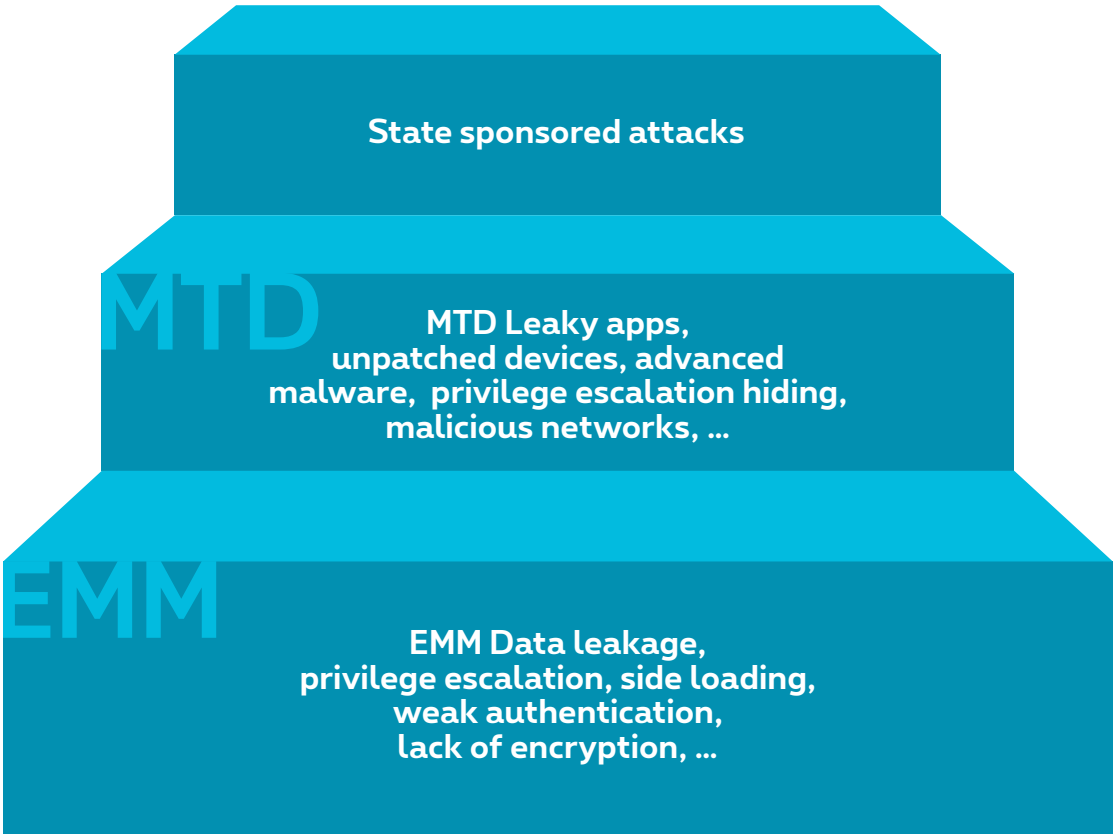
Bron: MobileIron

Infografieken en figuren

In maart 2017 werden voor het eerst meer gelijktijdige Android- dan Windows-internetverbindingen opgetekend

Bron: StatCounter, Android overtakes Windows for first time, 3 April 2017

Mobiele beveiligingsbedreigingen aangepakt door EMM en MTD



Bron: Gartner, *Market Guide for mobile threat defense solutions*, 22 august 2017

Meer info

Proximus is uw trusted cloud advisor voor het beheer van beveiligde data die altijd beschikbaar zijn. Surf naar **www.proximus.be** of neem contact op met uw accountmanager.