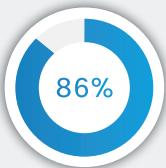




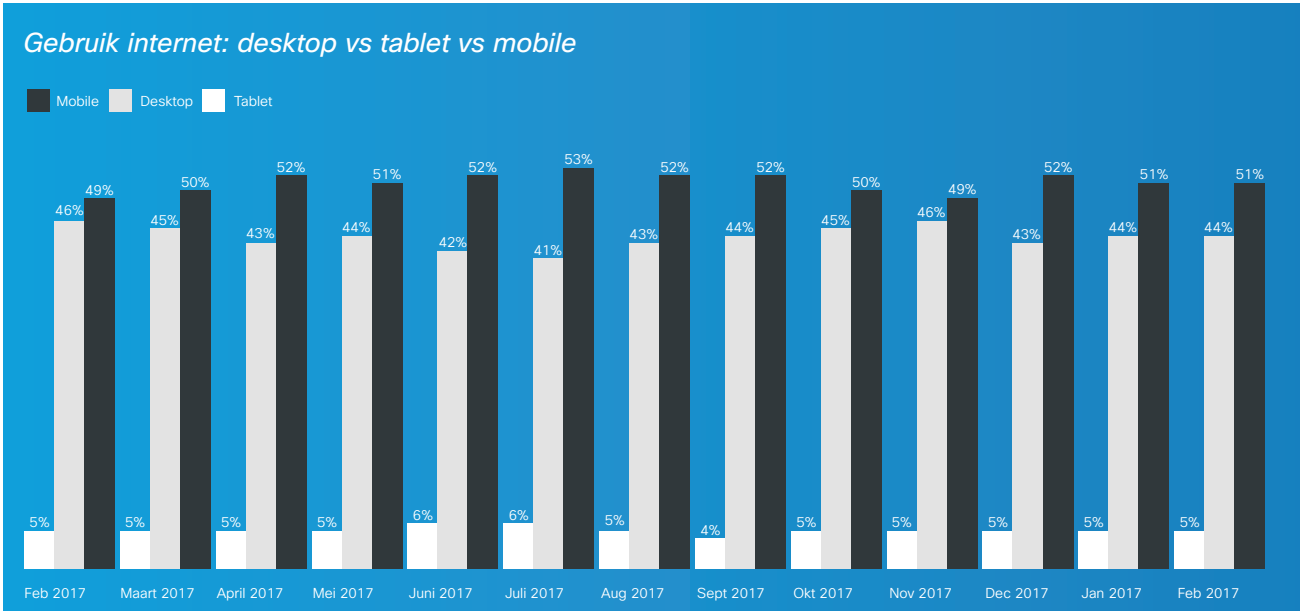
De ideale mobiele apparatuur voor je bedrijf

De mobiele revolutie raast onverminderd door. Wereldwijd is mobiel internet populairder dan internet via de desktop en ook in West-Europa is een duidelijke toename te zien. In het bedrijfsleven betekent het digitaliseringproces dat mobiele apparaten een steeds belangrijkere rol innemen in processen en dat ze een plek krijgen in het IT-beleid. Voor veel bedrijven is het echter lastig om een keuze te maken voor een bepaald merk device, omdat er veel variabelen zijn die meegewogen kunnen worden. Hoe zit het bijvoorbeeld met de beveiliging, het gebruiksgemak, de kosten en de voorkeuren van medewerkers? En waarom zijn deze variabelen van belang voor een goed mobiel ecosysteem in jouw bedrijf?



In 2021 zal 86% van het wereldwijde internetverkeer afkomstig zijn van smartphones

Bron: Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016–2021 White Paper

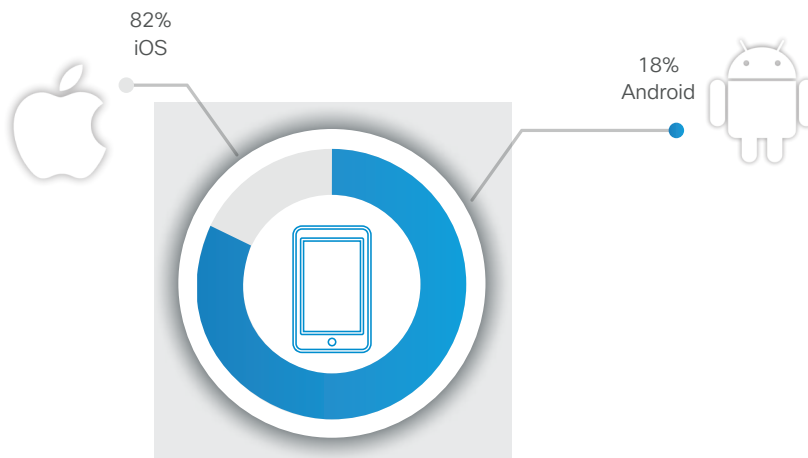


Houd rekening met voorkeuren

Het gros van de managers (85%) is ervan overtuigd dat mobiele apparaten het personeel ondersteunen bij flexibel werken. De systemen en producten moeten dan wel naadloos op elkaar aansluiten, en medewerkers moeten altijd op een veilige en eenvoudige manier toegang hebben tot de benodigde data.

Voor medewerkers is het prettig om devices te gebruiken waar ze bekend mee zijn, zodat ze er snel mee uit de voeten kunnen. En tevreden eindgebruikers leveren kwalitatief beter werk, wat tot een hoger bedrijfsresultaat leidt. Het Amerikaanse bedrijf Egnyte kon op basis van 4 miljard geregistreerde activiteiten achterhalen dat de iPhone verantwoordelijk is voor het grootste gedeelte (82%) van mobiele activiteiten in een zakelijke context.

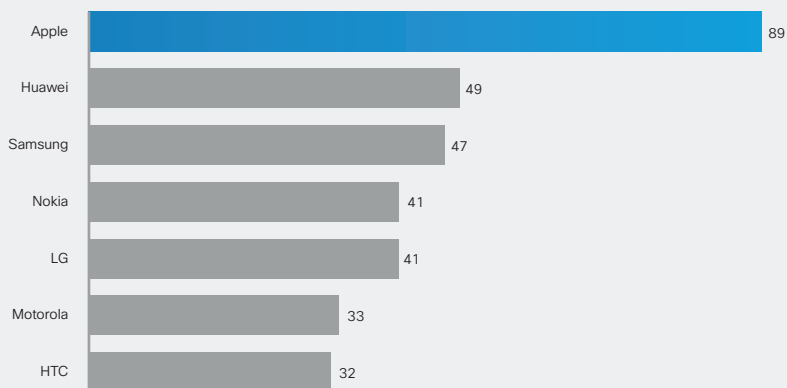
Zakelijk gebruik van iOS versus Android



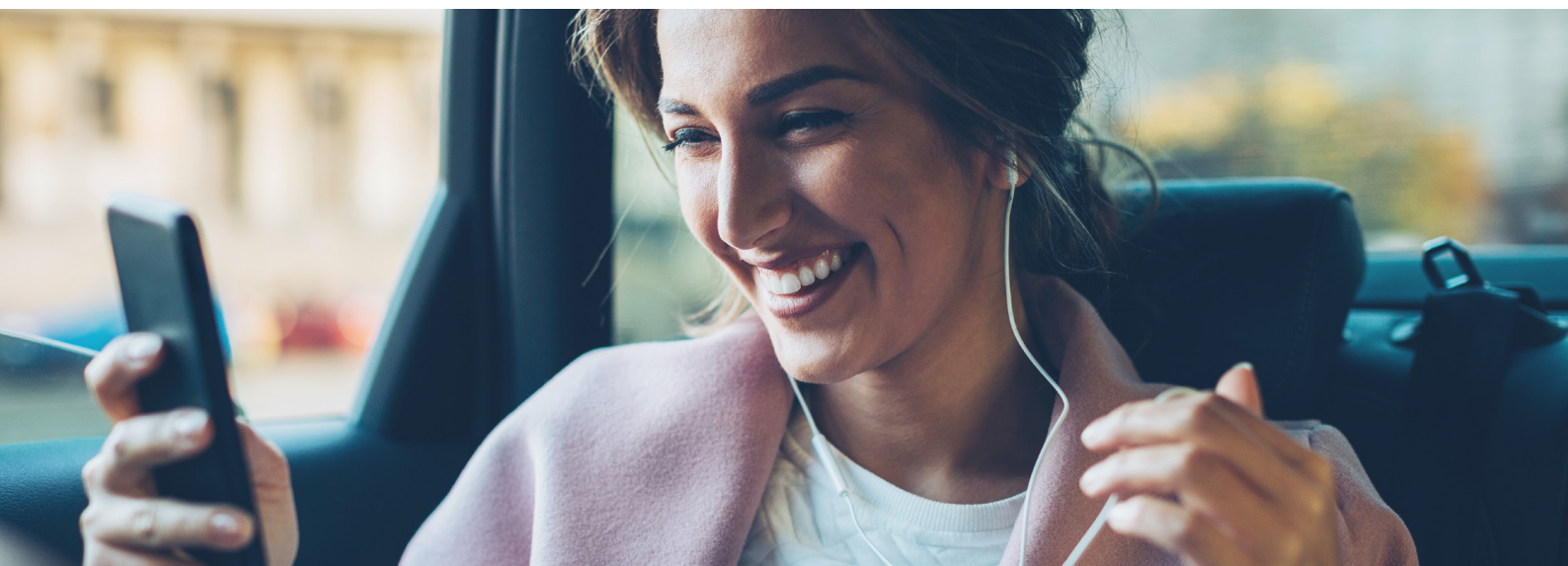
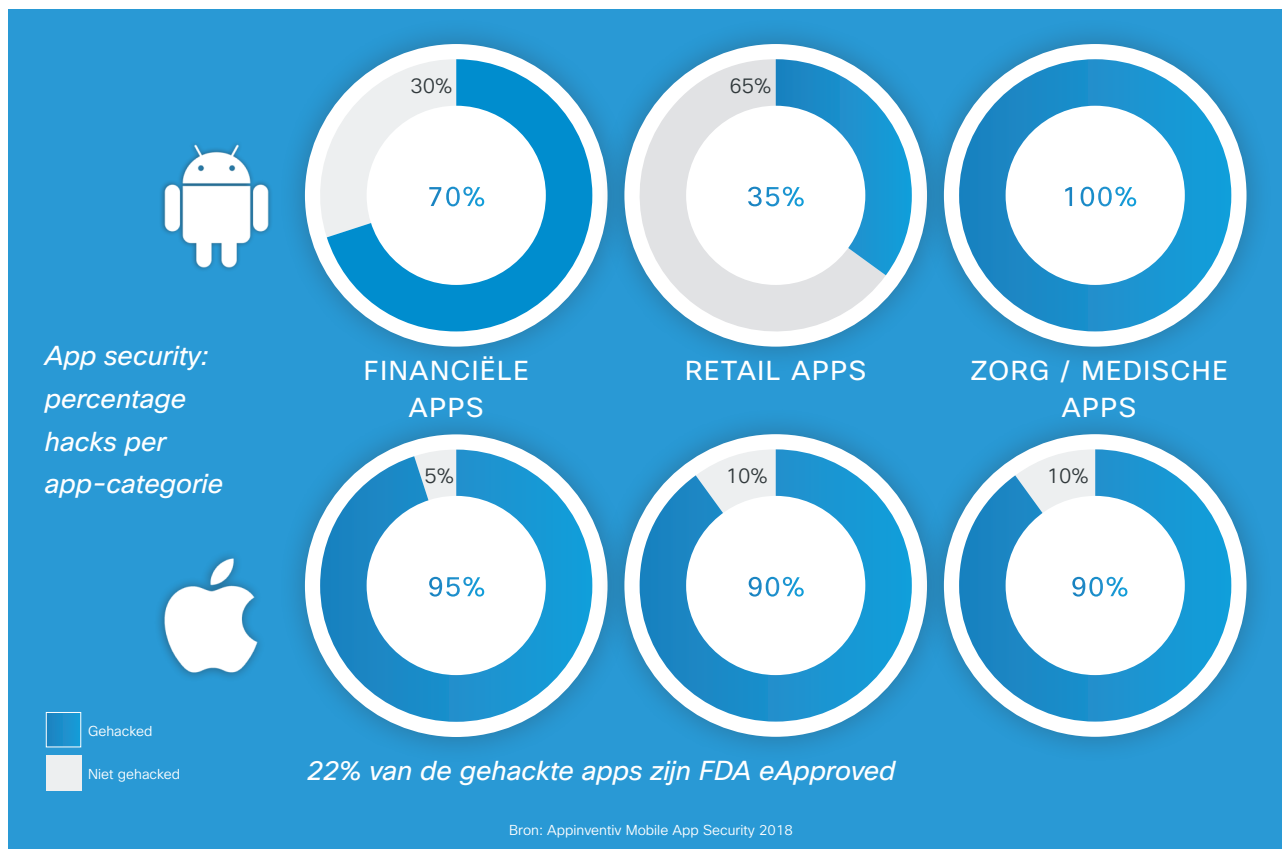


De iPhone-gebruikers zijn het meest lovend over hun device; Apple heeft van alle merken de hoogste Net Promotor Score. Gebruikers bevelen Apple het vaakst aan bij vrienden, collega's of familieleden.

*Aanbevelen van het merk
aan een vriend, collega of
familielid (NPS-score)*



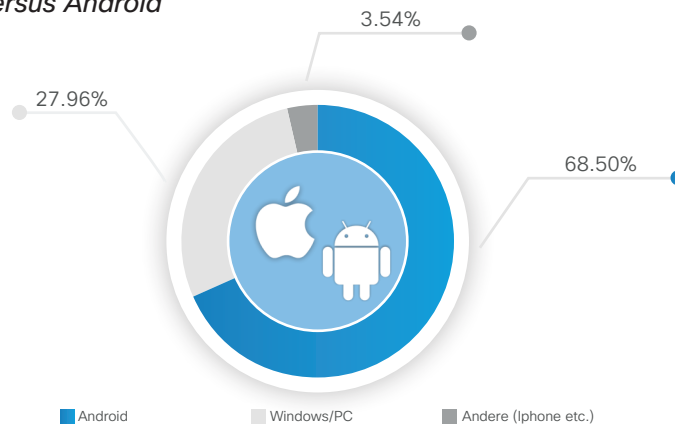
Bron: NPS Benchmarks - npsbenchmarks.com



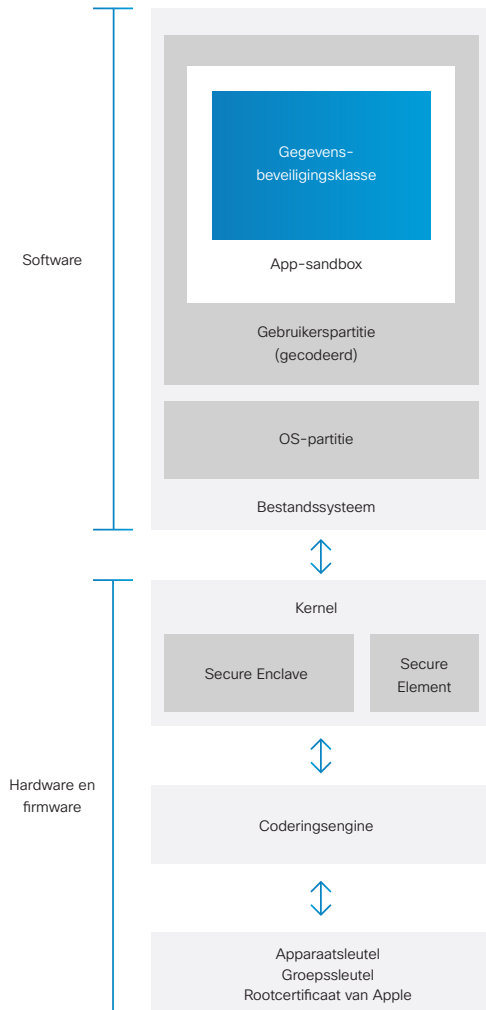
Ken de security-verschillen

Voor zakelijke devices is er keuze uit twee besturingssystemen: Android en iOS van Apple. Nu worden in organisaties nog regelmatig beide systemen gebruikt. Omdat het efficiënter is om over slechts één uniform besturingssysteem te beschikken (onder andere vanwege eenvoudiger beheer en snellere implementatie) is het belangrijk om hier een keuze in te maken. Bij de keuze voor een zakelijk device is het goed om de verschillen tussen deze besturingssystemen te kennen. En aangezien veiligheid bij organisaties bovenaan de prioriteitenlijst staat, door de toename van malware-aanvallen en cybercrime, is dat voor veel bedrijven het belangrijkste onderdeel van het beslissingsproces. Dat Android – omwille van diens open karakter en brede installed base – aanzienlijk gevoeliger is voor cybercrime dan iOS, blijkt uit onderstaande onderzoekscijfers.

Cybercrime: iOS versus Android



Schematisch overzicht van de beveiligings-architectuur van iOS



Beveiligingsmethoden

Uiteraard hebben beide ontwikkelaars een vorm van security aangebracht op hun systemen. Maar de manier waarop verschilt.

Apple heeft altijd hoog ingezet op het gebied van beveiliging. Dit is merkbaar in het ontwerp en de functionaliteit van de producten. Regelmatige software-updates, versleuteltechnieken en Mobile Device Management-opties maken iOS-devices veilig en controleerbaar voor zowel (zakelijke) gebruikers als IT-beheerders. De strenge kwaliteitscontroles binnen het Apple-ecosysteem zorgen ervoor dat gebruikers altijd goed beveiligd zijn.

Android heeft ervoor gekozen om voor hun zakelijke gebruikers een extra beschermingslaag toe te voegen in de software, de 'Android for Work'-feature. Met deze techniek kunnen medewerkers hun zakelijke gegevens en apps scheiden van privé-zaken door een werkprofiel aan te maken. De zakelijke content binnen het profiel kan men op afstand beheren en verwijderen, zonder dat persoonlijke gegevens worden aangetast. Daarnaast is het op schijfniveau encrypted, zodat gegevens alleen met een wachtwoord te achterhalen zijn.

Apple-devices bevatten, door gestandaardiseerde software-updates, in veel meer gevallen dan Android-toestellen de laatste (en dus veiligste) versie van het operating systeem.

91% Apple-devices bevat laatste versie besturingssysteem

21% Android-devices bevat laatste versie besturingssysteem



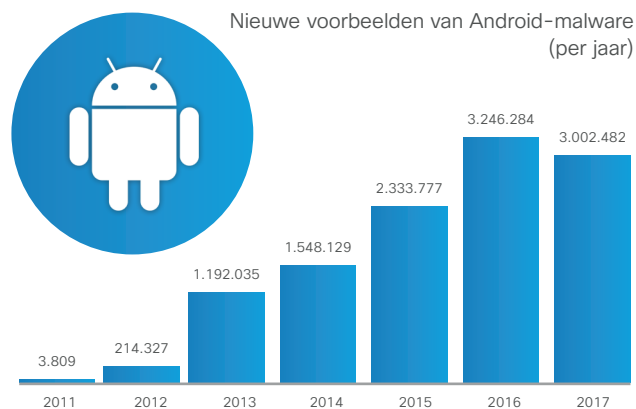
Open versus gesloten ecosysteem

Een belangrijk verschil tussen iOS en Android is dat het één een open en het ander een gesloten ecosysteem is. Beide partijen hebben dit heel bewust gekozen, waarbij Apple de volledige controle wil hebben en de makers van Android de focus leggen op het 'eigen' kunnen maken van het besturingssysteem. Je 'eigen touch' mee kunnen geven aan devices is iets waar veel smartphone-leveranciers gebruik van maken. Ze hoeven niet zelf een systeem te ontwikkelen en onderhouden. Ook voor de gebruikers biedt het open besturingssysteem voordelen: men heeft bijvoorbeeld veel mogelijkheden om bestanden uit te wisselen, zonder dat daar specifieke software voor nodig is. En ze kunnen eenvoudig alle beschikbare en gewenste apps op hun device installeren. Het open ecosysteem maakt Android persoonlijker en dynamischer dan iOS, maar ook kwetsbaarder voor dreigingen als malware en dataverlies.

Vanwege het gesloten ecosysteembeleid is iOS alleen verkrijgbaar op Apple-apparaten. Dit zorgt ervoor dat de keuze in devices relatief beperkt is. Gebruikers zijn door het gesloten ecosysteem ook gebonden aan Apple's strenge veiligheidseisen. Ze kunnen uitsluitend door Apple goedgekeurde apps downloaden en bestanden uitwisselen met andere Apple-toepassingen. Met de opensourceprogrammeertaal 'Swift' kunnen wel zelf apps gemaakt worden, maar alleen als ze aan strenge eisen voldoen worden ze toegevoegd aan apparaten. Dit beperkt enerzijds de vrijheid van de gebruikers, maar heeft anderzijds het voordeel dat het risico op malware veel minder is.

Android-gebruikers lopen het grootste risico om getroffen te worden door malware; het gros van de cybercriminelen richt zich namelijk op dat besturingssysteem.

Jaarlijks aantal nieuwe malware op Android



Bron: G DATA Malware Analysis 2018

Extra aandachtspunten voor juiste keuze

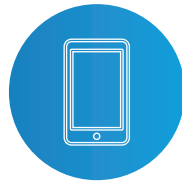
De meeste zakelijke applicaties

Met een iPhone beschik je over ruim 250.000 zakelijke apps – alle volledig getoetst en veilig bevonden. Dit zijn er meer dan op ieder ander mobiel platform. Al deze applicaties zijn bedoeld om werken en samenwerken op een eenvoudige en gewenste manier mogelijk te maken. Dit is een groot pluspunt op de werkvloer en voor mensen die op locatie werken. Mobiel (samen)werken wordt eindelijk écht ondersteund.

Device Enrollment Program

Een tweede voordeel van Apple is dat het IT-afdelingen van organisaties gemakkelijk maakt om snel op grote schaal meerdere devices tegelijkertijd uit te rollen, zelfs zonder het fysieke product in handen te hebben gehad. Het grootschalig implementeren en beheren van Apple-devices verloopt eenvoudig. Elke iPhone, iPad en Mac wordt automatisch geconfigureerd, waardoor de IT-afdeling niet alle devices één voor één af hoeft te gaan. De medewerker hoeft het apparaat slechts uit te pakken en aan te zetten. Het is dan al geïnstalleerd en geconfigureerd. IT kan bovendien op basis van





Mobile Device Management

Het blijft natuurlijk niet alleen bij het uitrollen van apparatuur. Apple heeft ook het beheer van zijn mobiele devices goed op orde. Met Mobile Device Management (MDM) heeft de systeembeheerder de beschikking over een all-in beheeromgeving waarmee die de controle heeft over tot welke voorzieningen elk device toegang heeft. Dat betekent bij iOS ook het op afstand installeren of verwijderen van apps op iPhones en iPads.

Met MDM op Apple-apparatuur krijg je deze zes basisfunctionaliteiten:

Uitrol van configuraties

Hiermee krijgen alle mobiele apparaten een standaardconfiguratie, inclusief de juiste apps en instellingen.

Management

Upgrades ('over the air' dus via het draadloze netwerk), lokaliseren van apparaten, locken en unlocken, synchronisatie.

Beveiliging

Apparatuur is altijd op de juiste manier beveiligd, onder meer doordat altijd verbinding wordt gemaakt via een VPN. Beveiliging checkt welke apps zijn geïnstalleerd.

Monitoren

Houdt verbruiksgegevens in de gaten, waaronder de opslag op het apparaat, dataverbruik, netwerkgegevens.

Verwijdering

Mobiele apparatuur kan op afstand worden gewist.

Ondersteuning

Via MDM kan ondersteuning worden geboden aan de gebruiker.



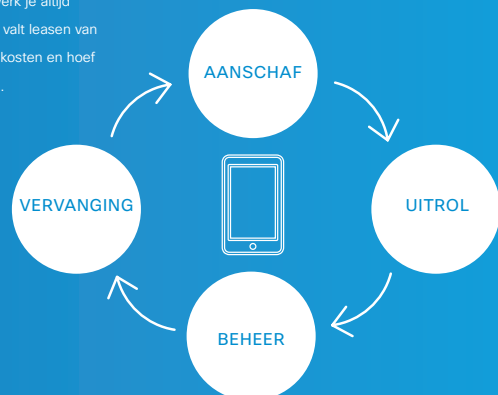
MDM en Device Enrollment Program werken bij Apple nauw samen. Apparatuur wordt al voordat ze in gebruik worden genomen aangemeld bij het DEP. Zo kunnen instellingen en configuraties vooraf worden opgegeven door de beheerder.



Financiële voordelen: hoge restwaarde

De in eerste instantie duur lijkende Apple-devices blijken verrassend voordelig te zijn. Apple-producten zijn weliswaar duurder in aanschaf, maar die investering wordt snel terugverdiend door tijdsbesparing op de uitrol van devices en applicaties, de langere levensduur en besparing op operationele (beheer)kosten. Windows-computers worden bijvoorbeeld vaak in drie jaar volledig afgeschreven, terwijl een Mac na drie jaar gemiddeld nog een restwaarde van 35 procent heeft. Dat ontdekte ook IBM. Het bedrijf bespaarde door het inzetten van Mac's meer geld dan het van tevoren had gedacht: elke Mac leverde de organisatie over een periode van vier jaar een besparing van \$ 535 op.

Dankzij de hogere restwaarde van Apple-apparatuur wordt de cirkel gesloten. Gebruik van de nieuwste apparatuur wordt goedkoper en zo werk je altijd met de nieuwste devices. Bovendien valt leasen van Apple producten onder operationele kosten en hoef je geen investeringen ineens te doen.



Werken met de nieuwste apparatuur

De medewerkers van nu en morgen zijn gewend aan de beste en nieuwste apparatuur. Het is voor werkgevers in deze krappe arbeidsmarkt daarom belangrijk om keuze te bieden in apparaten. Als medewerkers hun eigen devices kunnen kiezen, is maar liefst 78% van de millennials en 68% van de rest van de werknemers effectiever in hun werk. Ook is 37% creatiever en is 35% trotser op het bedrijf waar ze werken. Dit blijkt uit onderzoek van ManpowerGroup, Fortune en HR Drive.

Vooraf millennials blijken daarbij een grote voorkeur te hebben om te werken op Apple-apparaten. Dit geldt zowel voor computers als voor telefoons en tablets. Tussen pc en MacOS kiest maar liefst 72% voor MacOS en bij tablets kiest 75% voor een iPad.

Het is niet altijd eenvoudig om ervoor te zorgen dat je je medewerkers de nieuwste apparatuur biedt. Vaak zijn de investeringen hoog en moet je er daarnaast voor zorgen dat je alle informatie van de oude apparatuur weer afhaalt voordat je ze inlevert. Met Apple Financial Services wordt dit opgelost en kun je Apple-apparatuur eenvoudig en betaalbaar leasen. En dankzij de hoge restwaarde van Apple devices wordt het mogelijk om tegen lagere kosten je apparaten te vervangen aan het eind van de leaseperiode. Zo werk je altijd met de nieuwste apparatuur. En houd je je medewerkers tevreden.

Nu overstappen!

Vanaf 14 januari 2020 stopt Microsoft met de ondersteuning van Windows 7. De meeste pc's uit die tijd zijn niet geschikt voor een update. Dit is dus hét moment om over te stappen op een Apple device!



Meer informatie

Wil je meer informatie over het aanschaffen en gebruiken van Apple-apparaten, zoals MacBook, iPhone en iPad? Ga naar www.veiligmobielwerken.nl/contact

Bronnen:

- StatCounter GlobalStats February 2017 – February 2018
- Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2016-2021 White Paper
- www.apple.com/business/products-platform
- Skycure Mobile Threat Intelligence Report – Q1 2017
- Enterprise Insights by Egnyte
- Strategy Analytics – Enterprise Mobility Predictions 2017
- Nokia Threat Intelligence Lab
- NPS Benchmarks – npsbenchmarks.com
- G DATA Malware Analysis 2018
- Appinventiv Mobile App Security 2018