

# Lookout

“Beveiliging voor de mobiele generatie.”



De hoeveelheid bedrijfsgevoelige gegevens, alsmede hun toegankelijkheid, op mobiele devices is de laatste tijd enorm gestegen. Deze data maakt apparaten erg waardevol en daarmee een doelwit voor hackers. Sinds 1 januari 2016 is de Wet Bescherming Persoonsgegevens aangescherpt en ligt de verantwoordelijkheid, voor verlies van bedrijfsgevoelige gegevens, bij de ICT-manager en directie. Goede beveiliging van mobiele devices is daarom erg belangrijk.

Lookout beschermt mobiele apparaten tegen cyberaanvallen van buitenaf. Hierbij werkt Lookout vanuit de Cloud, waardoor het aanschaffen van hardware of onderhoudscontracten overbodig is.

## ✓ Gegevens uit 's werelds grootste mobiele database

Meer data betekent accuratere beveiliging. Lookout maakt gebruik van meer dan 100 miljoen mobiele sensors die de database voorzien van informatie.

## ✓ Gericht op mobiele beveiliging

Als sinds 2007 richt Lookout zich uitsluitend op de beveiliging van mobiele apparaten. Hierdoor weten ze meer over het wereldwijde mobiele ecosysteem en bedreigingen dan wie ook.

## ✓ 'Machine Intelligence'

Lookout maakt gebruik van zogenoemde machine intelligentie om bedreigingen te signaleren. Deze manier van werken voorziet in een grote hoeveelheid data zodat potentiële aanvallen snel gesignaleerd kunnen worden.

## Mobile Endpoint Security

Lookout beschikt over data via miljoenen mobiele apparaten wereldwijd en scant dagelijks tientallen duizenden apps op bedreigingen. Doormiddel van de beveiliging van Lookout worden apps op mogelijke data lekken gecontroleerd en ontvangen zowel de gebruiker als beheerder notificaties wanneer zich, mogelijk, een bedreiging voordoet. Lookout kan daarnaast gekoppeld worden met onder andere Airwatch, MobileIron en Microsoft om geautomatiseerd acties uit te laten voeren bij bedreigingen. De beheer console werkt vanuit de Cloud en is hierdoor te benaderen waar u ook bent. Op deze manier regelt u de beveiliging van uw apparaten makkelijk en snel.

## App Security

Met Lookout App Security scant u apps op de aanwezigheid van malware. Veiligheidsrisico's worden daarbij gecontroleerd voordat medewerkers of klanten de applicatie in gebruik nemen. Lookout geeft u een gedetailleerd inzicht in de risico's bij het gebruik van een app en markeert deze als onbetrouwbaar indien nodig. Hiermee beveiligt u gebruikers tegen bedreigingen van buitenaf.

# Lookout

“Beveiliging voor de mobiele generatie.”



## App Risk Control

In de verschillende App Stores worden applicaties van allerlei partijen aangeboden. Helaas zitten hier vaak ook goedgekeurde apps tussen welke toegangsrechten hebben die niet voldoen aan interne beleidsregels van een organisatie. Zo hebben gratis applicaties vaak ongewenst toegang tot bijvoorbeeld notities, de camera, foto's, contacten of zelfs de microfoon. Het kan daarbij voorkomen dat er gegevens van mobiele apparaten gehaald worden, en dit op externe servers wordt opgeslagen. Deze informatie wordt vervolgens gedeeld met reclame bureau's of gebruikt voor andere doeleinden. App Risk Control geeft u inzicht in de rechten die alle geïnstalleerde applicaties, op de apparaten van uw organisatie, hebben. Hier kunt u vervolgens actie op ondernemen door een app te weren of de toegang te weigeren.

## Threat Intelligence

Cyber criminaliteit wordt steeds geavanceerder. Lookout Threat Intelligence biedt 's werelds grootste zoek database met mobiele bedreigingen. Doormiddel van analyses trackt u deze wereldwijd en krijgt u 'real time' inzicht in cyberaanvallen en hun exacte locatie. Hiermee beveiligt u gevoelige netwerken en devices.

## Vragen?

Mail ons: [info@ecaretcs.nl](mailto:info@ecaretcs.nl)

of bel ons: +31 (0)88 488 0080

“Lookout zorgt voor beveiliging van een mobiele wereld die steeds meer met elkaar in verbinding is.”