Hso | the results company

Van firewall naar zero trust

HSO Security Assessment brengt risico's en aanbevelingen in kaart

Met de komst van Cloud Technologie en mobile computing is het IT-landschap van bedrijven sterk veranderd. Deze nieuwe wereld vraagt om een andere visie op security. Waar bedrijven voorheen hun on-premise omgeving beveiligden met een firewall, oftewel een stevig hek rondom alle systemen, zien we nu de opkomst van de zero trust architecture: een security-aanpak waarbij elk onderdeel van je IT-platform apart beveiligd is.

Tijdens het HSO Security Assessment brengen we de zwakke plekken in je digitale omgeving in kaart en vervolgens zorgen we voor een duidelijk stappenplan hoe je de beveiliging van je hybride of cloud platform kunt optimaliseren.

In deze factsheet lees je meer over deze zero trust aanpak en het security assessment.

Aan de slag?
Ons Cloud & Security team staat voor je klaar.

Contact:
Lucas Köhler
lkohler@hso.com
+31 (0)6 825 79 667

01 Dit zijn de zwakke plekken *in je IT-platform*

De risico's van cybercrime zijn groot. Vrijwel alle bedrijven krijgen er vroeg of laat mee te maken. Je zult niet de eerste organisatie zijn die slachtoffer wordt van een cryptohack, waarbij criminelen je data versleutelen en 'losgeld' eisen voor het vrijgeven ervan. Een ander groot risico is dataverlies, maar ook reputatieschade, bijvoorbeeld in geval van gestolen klantgegevens. Daarom wil je cybercrime ten allen tijde voorkomen. En als het je overkomt, wil je de schade zo snel en zo veel mogelijk kunnen beperken.

We zien dat de meeste hackers binnenkomen via het stelen van logingegevens, via malware in e-mails of via gestolen devices. Daarom focust een complete security-aanpak zich op:

1. Identities, logins en access management
2. Devices, laptops, telefoons en tablets
3. Data
4. Applicaties
5. Infrastructuur
6. Netwerk

02 Waarom een *zero trust security aanpak?*

Een on-premise omgeving wordt meestal beveiligd door een firewall. Oftewel een stevig hek rondom alle systemen. Niet alleen worden cybercriminelen steeds slimmer in het binnendringen van de firewall, het risico hiervan is ook dat als een hacker op de een of andere manier toch binnenkomt, hij al snel toegang heeft tot alle data en applicaties. Een hack wordt ook niet altijd direct ontdekt, met alle gevaren van dien. **De komst van cloud technologie en mobiel werken brengt naast deze risico's nieuwe dreigingen met zich mee.** Steeds meer medewerkers hebben toegang tot applicaties en data buiten de 'traditionele' bedrijfsnetwerkgrenzen om. Daarmee is beveiliging via firewalls en virtuele privénetwerken (VPN) niet meer voldoende.

Om deze uitdagingen het hoofd te bieden ontwikkelde Microsoft de Zero Trust Architecture. De drie principes van Zero Trust zijn:

1. Eis expliciete verificatie
2. Geef medewerkers alleen toegang tot die data en applicaties die ze nodig hebben;
3. Ga er vanuit dat je gehackt wordt.

Bij het inrichten van je security pas je deze principes continu toe. Klinkt het laatste principe nogal verontrustend? Microsoft noemt dit eerder realistisch. En, je kunt je er zo goed mogelijk op voorbereiden, zodat eventuele schade tot een minimum beperkt blijft.

Een Zero-Trust model vereist dat alle onderdelen - identiteit van de gebruiker, het apparaat, het netwerk en de applicaties - continu worden gevalideerd en getest op betrouwbaarheid.

De security slagkracht van Microsoft

Bij HSO zijn we ervan overtuigd dat on-premise security vrijwel onmogelijk meer het niveau kan halen van cloud-security. Microsoft investeert jaarlijks miljarden in de beveiliging van het Microsoft Cloud platform, en zo'n 3.000 mensen dragen hier iedere dag fulltime aan bij. De kracht van het Microsoft platform zit 'm vooral in de enorme hoeveelheden data, applicaties en informatiestromen waarop continu met behulp van geavanceerde algoritmes gezocht wordt naar afwijkende signalen, datastromen of andere verstoringen. Het niveau van security wordt hierdoor steeds hoger en steeds verder geautomatiseerd, waar je als gebruiker van het Microsoft platform direct van profiteert.

De vier pijlers van *Intelligent Security volgens Microsoft*

Identitymanagement en toegangsbeheer	Threat protection	Information protection	Cloud security
Een universeel platform waarmee je gebruikers (identities) beheert en beveiligt.	Geïntegreerde en geautomatiseerde beveiliging detecteert en stopt cyber-aanvallen.	Bescherming van je bedrijfsgevoelige informatie - waar deze data ook is opgeslagen of wordt verstuurd.	Bescherm je cloudapplicaties.

03 Zo werkt het *HSO Security Assessment*

Stap 1

Bepalen as-is en to-be

Het inventariseren van de ‘as-is’ status van je beveiliging en het bepalen van de eisen en randvoorwaarden van de ‘to-be’ situatie. De eisen en randvoorwaarden stellen we op aan de hand van wet- en regelgeving, standaarden in de markt en bijvoorbeeld verwachtingen van klanten en partners.

Stap 2

Inventarisatie van je huidige IT-landschap

Hoe ziet je huidige IT-landschap eruit, inclusief gebruikers, toestellen, applicaties, netwerk, locaties en data?

Stap 3

Inventarisatie mogelijke bedreigingen

We analyseren de beveiligingsrisico’s en potentiële bedreigingen van je huidige omgeving en brengen deze voor je in kaart.

Stap 4

Assessment report en stappenplan

De laatste stap is een presentatie van het verslag van onze bevindingen, plus een compact stappenplan om te komen tot een zero trust security architectuur.

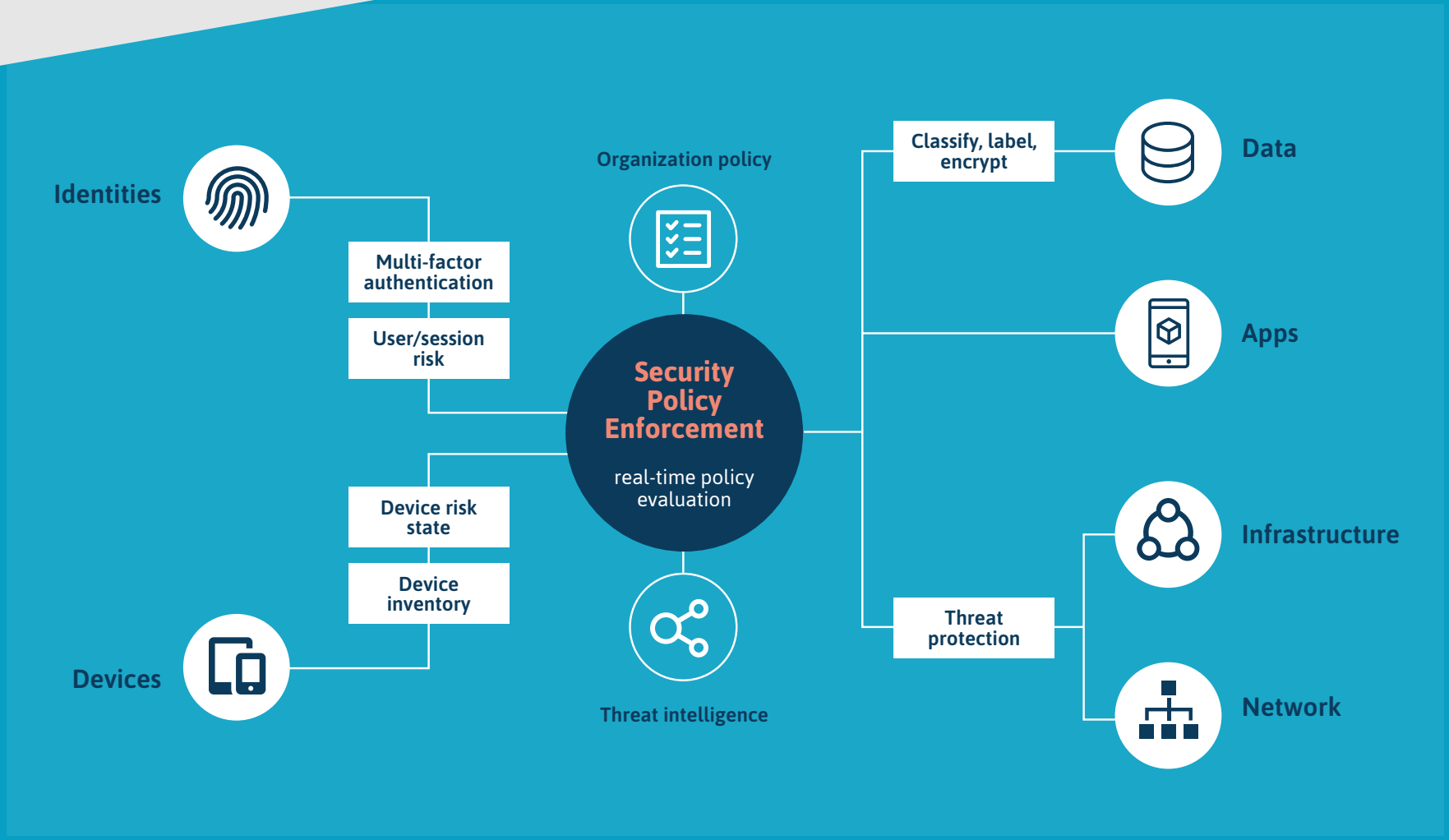
Doorlooptijd

Voor het Security Assessment is in de regel een doorlooptijd van 3-4 weken voldoende.

Wat vragen we van jou?

Voor stap 1, het zetten van de kaders en doelstellingen, en stap 4, de presentatie vragen we beschikbaarheid van het management en het IT-team. Verder vragen we inzet van het IT-team bij stap 2 en 3, waarbij we samen het huidige platform en de mogelijke zwakke plekken en risico’s in kaart brengen.

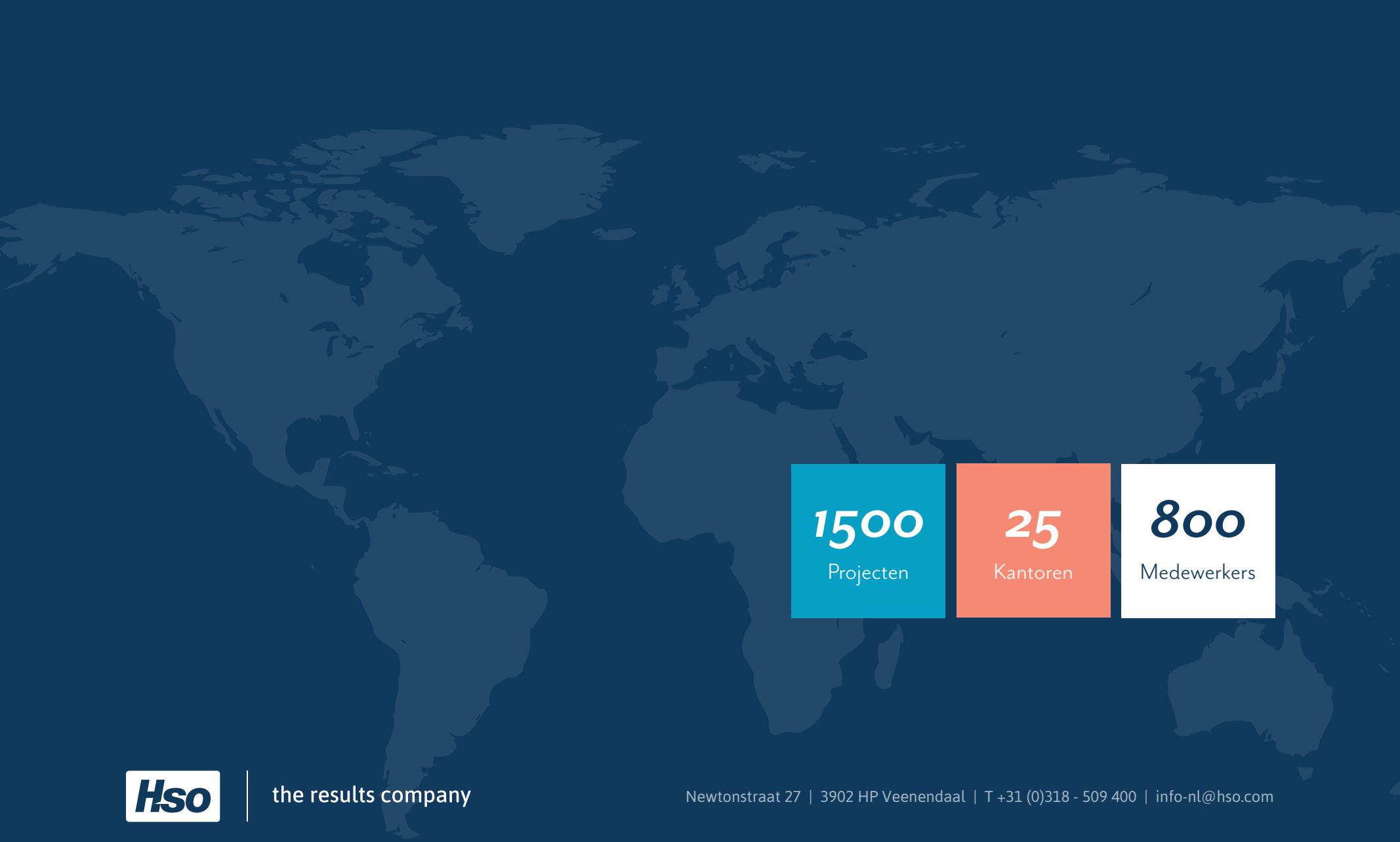
Zero Trust Architecture



Interesse in het HSO Security Assessment?

Wil jij de beveiliging van je hybride of cloud platform naar een hoger niveau brengen? Onze experts staan voor je klaar. Neem gerust contact met ons op!

Contact:
Lucas Köhler
lkohler@hso.com
+31 (0)6 825 79 667



Hso | the results company

Newtonstraat 27 | 3902 HP Veenendaal | T +31 (0)318 - 509 400 | info-nl@hso.com

Sinds 1989 is HSO actief als Microsoft Solution Integrator en uitgegroeid tot een succesvol ICT-bedrijf met meer dan 800 medewerkers en vestigingen in Europa, Noord-Amerika en Azië. HSO ondersteunt lokale en internationale bedrijven in de retail, groothandel, industrie en (technische) dienstverlening om met digitale technologie het verschil te maken. Het fundament hiervoor is Microsoft Dynamics 365: een compleet platform van CRM, ERP, Office 365 en BI-software. HSO verzorgt de implementatie, optimalisatie en het 24/7 beheer van deze cloud oplossingen. HSO behoort tot de Microsoft Dynamics Inner Circle en is in het trotse bezit van het predicaat 'Meest klantgerichte partner van Microsoft'. Meer informatie over HSO is te vinden op http://www.hso.com/nl of volg HSO op Twitter via @HSO_NL.