ALS HET NIET KASPERSKY ENDPOINT SECURITY FOR BUSINESS IS, IS HET GEEN PLATFORM VOOR ENDPOINTBEVEILIGING

10 VOORDELEN

DIE ALLEEN EEN GEÏNTEGREERD BEVEILIGINGSPLATFORM KAN BIEDEN

KASPERSKY lab

Volgens het rapport van Kaspersky Lab over wereldwijde IT-risico's heeft 94 procent van de bedrijven in de afgelopen 12 maanden te maken gehad met een extern beveiligingsincident[1].

Naarmate de omvang en complexiteit van bedreigingen exponentieel toenemen, groeit bij bedrijven van elke grootte het inzicht in IT-beveilingsrisico's, met name als het gaat om gerichte aanvallen. Ze zien ook dat ze zich kunnen beschermen tegen specifieke bedreigingen in plaats van een willekeurige, brede aanpak te hanteren voor wat algemeen gezien wordt als 'malware'.

Helaas blijven leveranciers van IT-beveiliging juist die willekeurige, brede aanpak aanbieden door nieuwe technologieën in te kopen en dan de vaak niet compatibele codes van deze afzonderlijke technologieën met elkaar te verweven. Dit vergroot de complexiteit en veroorzaakt net zo veel problemen als er worden opgelost.

[1] Global IT Security Risk Report 2014.

De dagen van traditionele endpointbeveiliging (afzonderlijke anti-malware, encryptie, apparaat- en netwerktoegangscontrole) lopen ten einde. Op het gebied van IT-beveiliging, bescherming tegen geavanceerde bedreigingen en gegevensbescherming zijn endpointbeveiligingsplatformen (EPP's), die nauwe integratie van beveiligingstechnologieën beloven, in toenemende mate de trend.

Maar er is een wereld van verschil tussen 'integratie' en een echt platform. Ook de opvattingen over het concept 'integratie' verschillen. Voor veel leveranciers is 'integratie' gewoon een ander woord geworden voor 'compatibel'.

En voor sommige leveranciers betekent 'compatibel' dat ze producten afkomstig van wel 40 overnames met elkaar proberen te verbinden om ze te laten samenwerken met hun eigen codebasis, zonder aan de belangen van hun klanten te denken.

Er zijn veel leveranciers die 'geïntegreerde' oplossingen beloven, maar wie wat dieper graaft, komt er al gauw achter dat er een groot verschil is tussen 'leuk samenwerken' en echte synergie, voortvloeiend uit productstrategieën en productontwikkelingen die gebaseerd zijn op inzicht. Sommige leveranciers worstelen met het integreren van hun bedrijfsovernames, terwijl ze toch beweren dat ze werkelijk geïntegreerde platformen kunnen leveren.

Het opkopen van alles wat de nieuwste hype lijkt te zijn, kan niet dezelfde volledigheid van visie of beveiliging bieden.

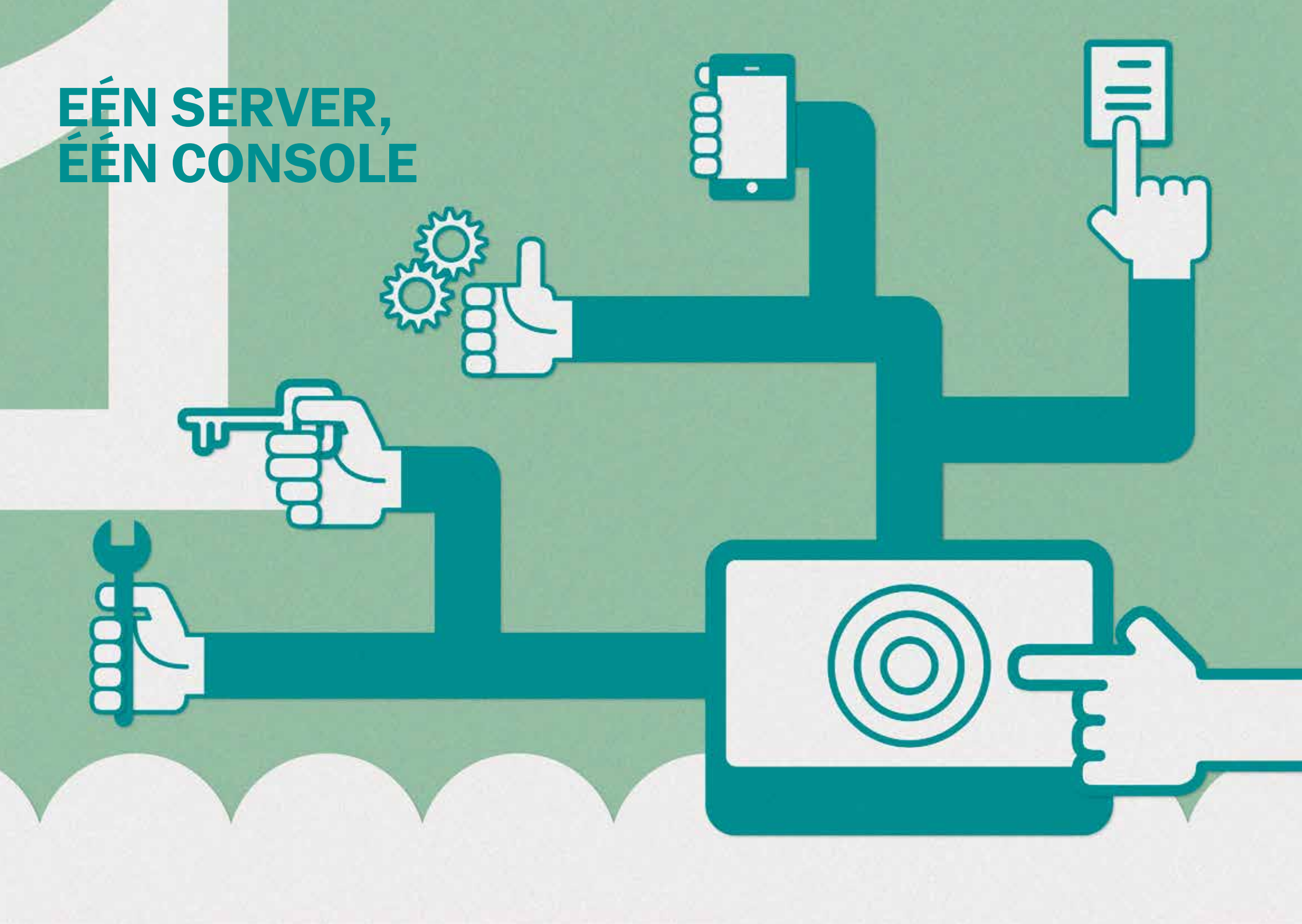
Een werkelijk diep geïntegreerde platformoplossing biedt bepaalde unieke voordelen. Kaspersky Endpoint Security for Business biedt IT-beheerders de volgende, unieke voordelen:

1. Eén server, één console
2. Single Agent Architecture*, eenvoudige installatie
3. Het voordeel van één beleid
4. Het synergie-effect - groter dan de som der delen
5. Centraal beheer van beheerdersrechten - betere controle- en beheerfuncties via één console

6. Uniforme structuur en vertrouwd uiterlijk - voor snellere en eenvoudigere rapportage
7. Beter, diepgaander inzicht in gegevens - geïntegreerde dashboards en rapportfuncties
8. Centraal licentiebeheer - efficiënter, betere controle
9. Eén enkele, intern ontwikkelde codebasis bevordert de integratie
10. Geïntegreerd aanschafmodel - alle benodigde functionaliteit met één aankoop

* Single Agent Architecture per platform (Windows, Linux, Mac).

EÉN SERVER, ÉÉN CONSOLE



1 EÉN SERVER, ÉÉN CONSOLE

Alleen de oplossing van Kaspersky Lab biedt een uniform, volledig geïntegreerd platform voor server- en systeembeheer dat alle aspecten van endpointbeveiliging omvat, van anti-malware en gegevensbescherming tot en met beheer van mobiele apparaten en systemen - Kaspersky Security Center.

Beveiligingsbeleid en rapportage worden beheerd via een enkele console, geïntegreerd met externe bronnen, zoals LDAP-directory's en Microsoft Exchange. Hardware- en software-inventarisatiedatabases en softwarevulnerabilities/-updates zijn ook inbegrepen, wat de integratie- en synergiemogelijkheden verder vergoot omdat verschillende afdelingen kunnen beschikken over dezelfde gegevens. Voortdurend synchroniseren met verschillende servers of datasets is overbodig. Alles wordt direct geïnstalleerd op dezelfde server en beheerd via dezelfde console.

Deze mogelijkheden van diepgaande integratie en synergie bieden duidelijke voordelen boven de oplossingen van concurrenten. Deze systemen, die veelal zijn gebaseerd op gekochte technologie en meerdere, afzonderlijke databases, kunnen eenvoudig niet dezelfde diepte van integratie bieden als het platform van Kaspersky.

De voordelen:

- **Snelle, eenvoudige implementatie:** één beheerserver, console-installatie en configuratieproces zorgt voor volledig geïntegreerde functionaliteit, direct klaar voor gebruik.

- **Dezelfde beheerserverhardware:** geen gedoe met verschillende hardware, verschillende systemen of extra onderdelen voor elke afzonderlijke beheerserver en -console. Kaspersky vereist voor de meeste implementaties slechts ÉÉN server.

- **Dezelfde beheerserversoftware**: gemakkelijk te beheren infrastructuur voor kleine bedrijven die toch kan worden opgeschaald voor grotere implementaties.
  — Voor sommige producten moeten na de eerste implementatie aanvullende pakketten worden geïnstalleerd om soortgelijke functionaliteit te bieden als Kaspersky Lab.
  — Voor nog meer gemak omvat het platform van Kaspersky aanvullende applicaties (zoals de applicaties die vereist zijn voor een Microsoft-omgeving) als onderdeel van het installatieproces en automatische installatie, waarmee tijd en ergernis wordt bespaard. Het werkt gewoon.

SINGLE AGENT ARCHITECTURE*, EENVOUDIGE INSTALLATIE

* Single Agent Architecture per platform (Windows, Linux, Mac).

2 SINGLE AGENT ARCHITECTURE*, EENVOUDIGE INSTALLATIE

Alleen de oplossing van Kaspersky biedt een Endpoint Agent die op basis van diepgaande code-integratie volledige compatibiliteit garandeert tussen alle hardware- en softwareconfiguraties.

Echte endpointbeveiligingsplatformen hebben een gestroomlijnde architectuur, waarbij door het gebruik van een minimumaantal afzonderlijke agenten voor het uitvoeren van taken de complexiteit wordt gereduceerd en de integratie wordt verdiept. Gerelateerde functies, zoals scannen op vulnerabilities, applicatie-updates en patchen, maar ook beschermingsmodules, zoals anti-malware en encryptie, hebben een Single Agent Architecture, wat de prestaties stroomlijnt en beheertaken minimaliseert.

Systemen van concurrenten vereisen vaak meerdere agenten op dezelfde machine voor functies als beheer van patch-applicaties en encryptie. Dit kan leiden tot compatibiliteitsproblemen tussen agents en vereist aanvullende tests.

* Single Agent Architecture per platform (Windows, Linux, Mac).

De voordelen:

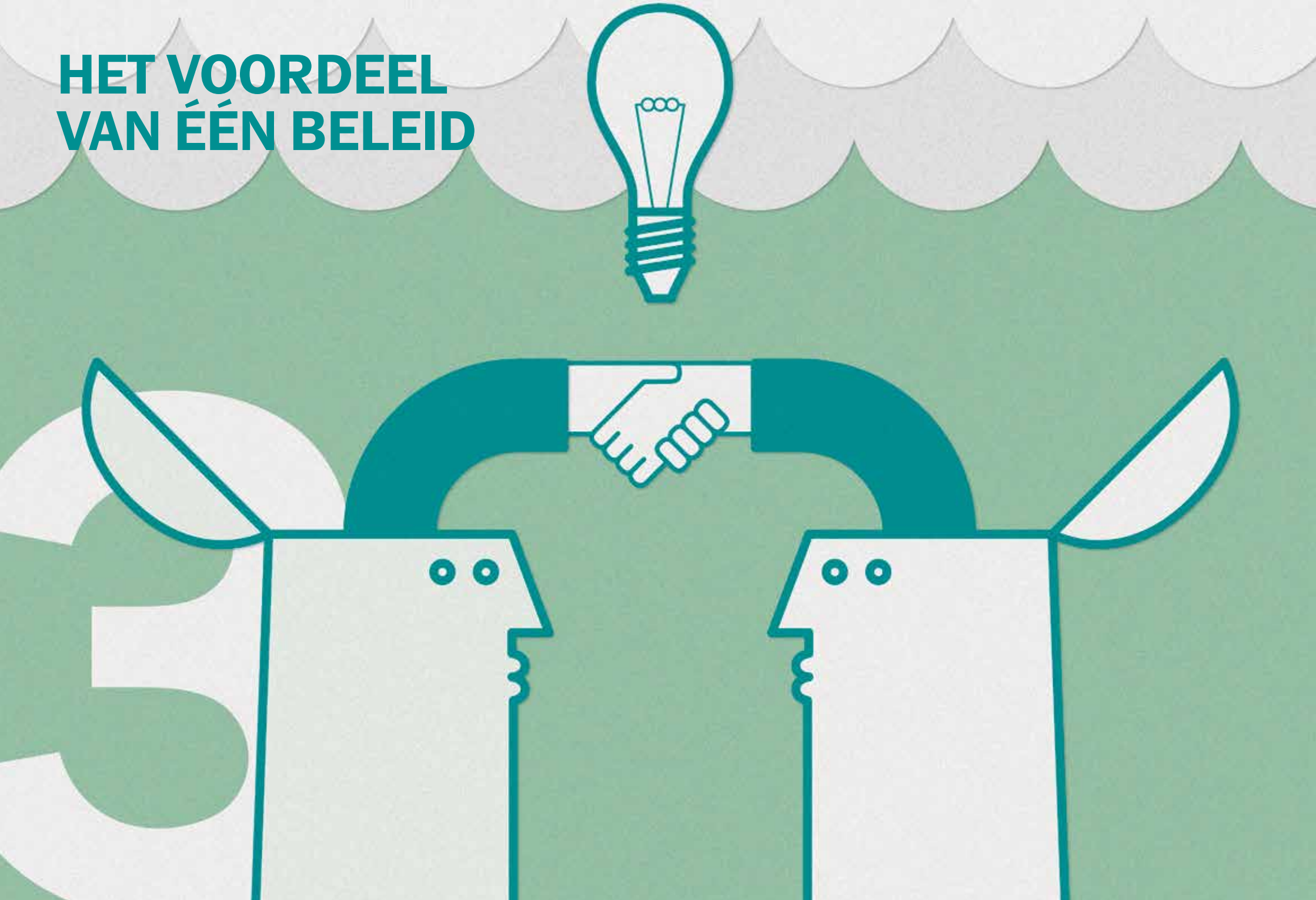
- **Bespaart tijd bij de eerste implementatie en bij updates:** slechts een eenvoudige installatietaak om te beheren, zonder afhankelijkheden en zonder dat het systeem meerdere keren opnieuw moet worden opgestart.

- **Geen gedoe met verschillende systeemvereisten:** het is geen geheim dat groei door overname gepaard gaat met het probleem van softwarecompatibiliteit. Ingekochte functionaliteit kan afzonderlijke, extra ondersteuning noodzakelijk maken, nog afgezien van de ondersteuning voor de daarmee gebundelde software. En daar komt u pas achter als u een implementatie start… Alleen een organische, geïntegreerde ontwikkelingsaanpak kan naadloze compatibiliteit tussen verschillende softwarecomponenten voor beheerde endpointplatformen/-apparaten garanderen. Het betekent ook dat er bij de client minder compatibiliteitstests nodig zijn.

- **Minder impact:** op systeembeheer en beheertaken.

- **Basis voor de ontwikkeling van synergiescenario's:** diepe integratie biedt flexibiliteit en meer functionaliteit. Breid de mogelijkheden uit zonder de systeembronnen zwaarder te belasten.

HET VOORDEEL VAN ÉÉN BELEID



3 HET VOORDEEL VAN ÉÉN BELEID

Complexiteit is de vijand van beveiliging, maar om alle aspecten van gegevensbeveiliging in een organisatie te beheren moeten meerdere, zeer verschillende systemen worden beheerd. Hoe meer u de beheerprocessen kunt vereenvoudigen, hoe groter de transparantie en hoe lager de risico's.

Een echt endpointbeveiligingsplatform voorziet in beheerfuncties voor het detecteren, implementeren en bijwerken van endpoints en het configureren van beleidsinstellingen voor endpoints binnen de hele bedrijfsinfrastructuur. De Single Agent Architecture van Kaspersky Endpoint Security betekent dat beheerders voor een beheerde groep een actief beleid kunnen instellen dat alle vereiste componenten omvat, zonder de noodzaak van herziening van meerdere beleidsregels of correlatie.

'Network Agent' verbindt het endpoint met de beheerserver, waarop systeembeheertaken worden uitgevoerd (zoals software- en hardware-inventarisatie, vulnerabilityscans en patchbeheer), zodat werkelijke flexibiliteit en synergie tussen functies mogelijk is.

De voordelen:

- **Vereenvoudigd beheer van beleid en taken:** dankzij één verzameling van gedeelde parameters en voorinstellingen wordt de implementatie van beheerde groepen, leveringsinstellingen, meldingen en beleid geoptimaliseerd, en worden redundante processen en taken voor de IT-beheerder geëlimineerd.

- **Eenvoudigere controle over implementatie van beleid en taken:** één dashboard en rapportage over de implementatie en uitvoering biedt een uitgebreid, helder overzicht van beleidsstatus en compliance in het gehele netwerk.

- **Gestroomlijnde wijziging van beleid en taken:** aanpassingen worden in één stap uitgevoerd. Automatische beleidstoekenning kan meerdere beveiligingsparameters tegelijk omvatten, van verschillende beveiligingsinstellingen tot applicatie-, apparaat- en webbeheerinstellingen en encryptieregels.

HET SYNERGIE-EFFECT - GROTER DAN DE SOM DER DELEN

4 HET SYNERGIE-EFFECT - GROTER DAN DE SOM DER DELEN

Geïntegreerde endpointbeveiligingsfuncties vormen de basis van Kaspersky's beveiligde platform en zorgen dat zelfs complexe, geavanceerde beveiligingsbeheerscenario's gemakkelijk te implementeren zijn. Werkelijke integratie levert een beveiligingsniveau op dat uitstijgt boven de afzonderlijke delen van elke functie. Voorbeeld:

Om uitgebreide bescherming tegen internetdreigingen te implementeren, naast beleidsgestuurd scannen van webverkeer en gedownloade bestanden, kunnen bedrijven de applicatiebeheerfunctie van Kaspersky gebruiken om het gebruik van slechts één, door IT goedgekeurde browser af te dwingen. Deze browser kan vervolgens verder worden beveiligd door automatische patching van vulnerabilities met hoge prioriteit af te dwingen en bescherming tegen zero-day-aanvallen toe te voegen door middel van Automatic Exploit Prevention. Op deze manier vormen de geïntegreerde functies van Kaspersky een beschermingslaag tegen zeer grote infectiehaarden; dat is wat we het synergie-effect noemen.

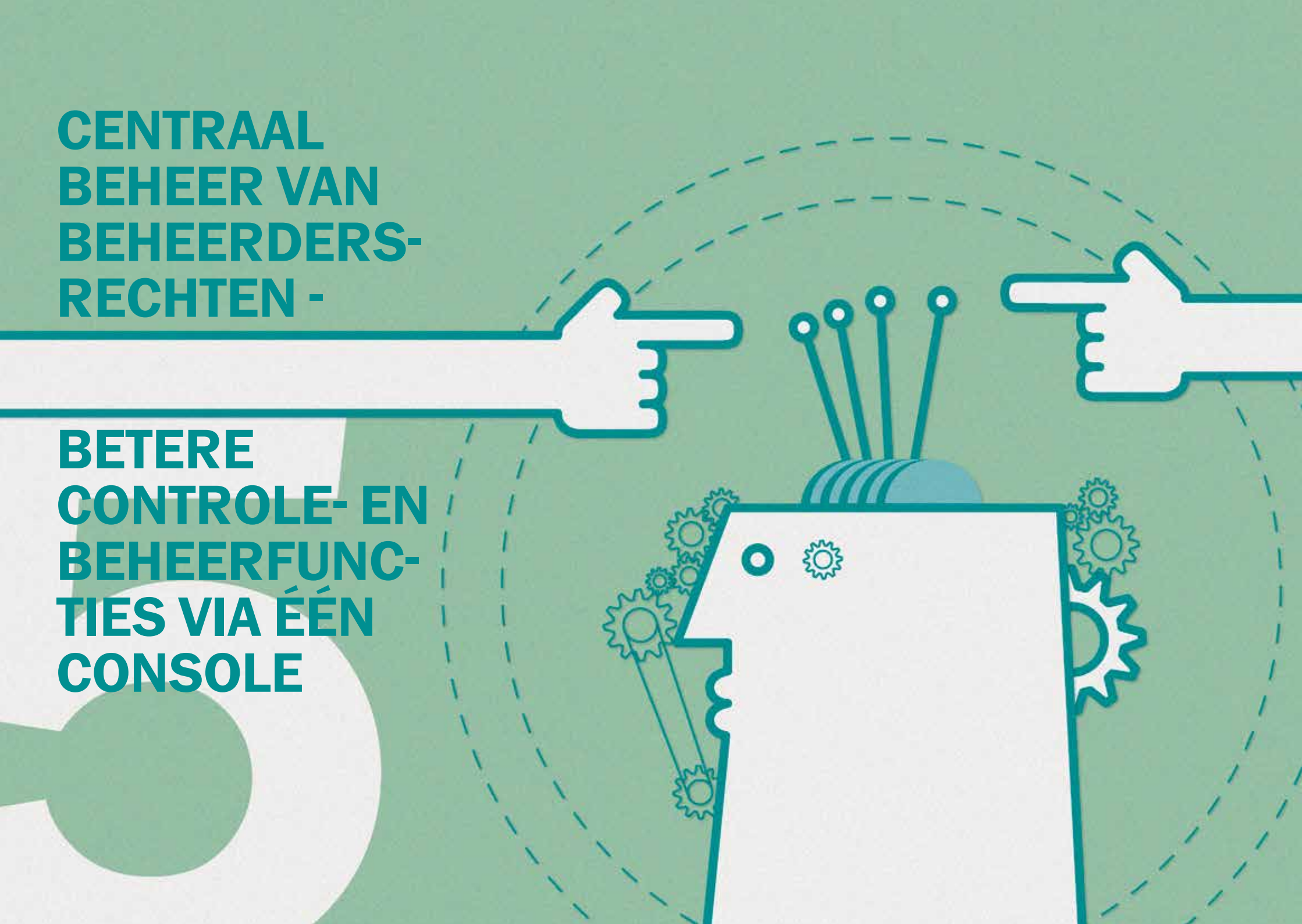
De voordelen:

- **Uitwisseling van procedures voor beveiligingsbeheer en informatie die wordt verzameld via verschillende functies, bijvoorbeeld:**
  - — verzamelde informatie over verwisselbare apparaten wordt gebruikt voor apparaatbeheer en encryptie;
  - — informatie over applicaties wordt gebruikt voor applicatiebeheer en encryptieregels;
  - — Mobile Device Management (MDM) geïntegreerd met gegevensbeveiliging op apparaten;
  - — beslissingen omtrent patchbeheer kunnen worden gebaseerd op vulnerabilitybeoordeling.

Het synergie-effect is niet beperkt tot de hierboven beschreven scenario's. Kaspersky's diepe code-integratie garandeert volledige, gemakkelijk te realiseren compatibiliteit en synergie tussen hardware- en softwareconfiguraties. Kortom, het platform van Kaspersky biedt een betere beveiliging dan de afzonderlijke delen van elke functie.

CENTRAAL BEHEER VAN BEHEERDERS-RECHTEN -

BETERE CONTROLE- EN BEHEERFUNC-TIES VIA ÉÉN CONSOLE



5 CENTRAAL BEHEER VAN BEHEERDERSRECHTEN - BETERE CONTROLE- EN BEHEERFUNCTIES VIA ÉÉN CONSOLE

Onderbezetting van IT-afdelingen is bij veel kleine en middelgrote ondernemingen een veelvoorkomend probleem. Economische inkrimping en toenemende IT-complexiteit betekenen dat IT-beheerders meer taken moeten uitvoeren in minder tijd.

Het Endpoint Protection Platform van Kaspersky biedt centrale beheertools voor dagelijkse beveiligingstaken om deze problemen het hoofd te bieden. Diepe integratie zorgt dat toegangsrechten en logboeken vanaf één console kunnen worden beheerd. Eén log voor de registratie van alle handelingen in tegenstelling tot producten van concurrenten, die vaak gegevens van afzonderlijke consoles en servers moeten ophalen.

Door geïntegreerd rechtenbeheer en registratie is effectievere beheersing mogelijk en wordt beter inzicht verkregen in de handelingen van medewerkers voor een effectiever machtigingenbeheer. Het resultaat: betere beveiliging en grip op IT-activiteiten en -beheer. Vanaf één console.

De voordelen:

- **Eenvoudig machtigingen definiëren en beheren**: in een doorsnee MKB-bedrijf, waar alles neerkomt op de IT-medewerker, zou het gemakkelijk moeten zijn om alle aan beveiliging gerelateerde taken uit te voeren, zoals het instellen van machtigingen voor lezen/wijzigen, toegangsrechten, enzovoort.

- **Snelle reactietijd bij incidenten en geïntegreerd event log:** IT-beheerders zijn ook maar mensen; soms worden er fouten gemaakt en als het gaat om een beveiligingsincident is een snelle reactie essentieel. Functionaliteit om toegangsrechten snel te kunnen wijzigen of blokkeren is van vitaal belang, net als de mogelijkheid die veranderingen bij te houden. Met afzonderlijke oplossingen moeten bij complexe incidenten soms meerdere analyseprocessen worden gecreëerd. Kaspersky neemt de complexiteit weg, met informatie over alle wijzigingen in endpointbeveiliging, beleidsregels en beheeractiviteiten in één logbestand, weer te geven vanuit één beheerconsole.

UNIFORME STRUCTUUR EN VERTROUWD UITERLIJK - VOOR SNELLERE EN EENVOUDIGERE RAPPORTAGE

6 UNIFORME STRUCTUUR EN VERTROUWD UITERLIJK - VOOR SNELLERE EN EENVOUDIGERE RAPPORTAGE

Beheerders in tijdnood grijpen elke kans aan om tijdwinst te behalen of een taak te vereenvoudigen. Endpointbeveiligingsplatformen met uniforme, geïntegreerde functies en een vertrouwde interface maken rapportage, analyse en incidentbeheer eenvoudiger. Het Kaspersky Security Center genereert rapporten met een uniforme structuur en vertrouwd aanzien.

De werkdag van een IT-beheerder bestaat vaak uit een veelvoud van routinematige, doch cruciale taken, die stuk voor stuk moeten worden bewaakt en vastgelegd. In een omgeving waar gebruik wordt gemaakt van meerdere oplossingen zijn uiteenlopende dashboards actief die verschillende rapporten genereren in verschillende indelingen, van PDF en HTML tot e-mails. En wie heeft nog de tijd dit allemaal door te nemen én te zorgen dat alles werkt zoals het moet?

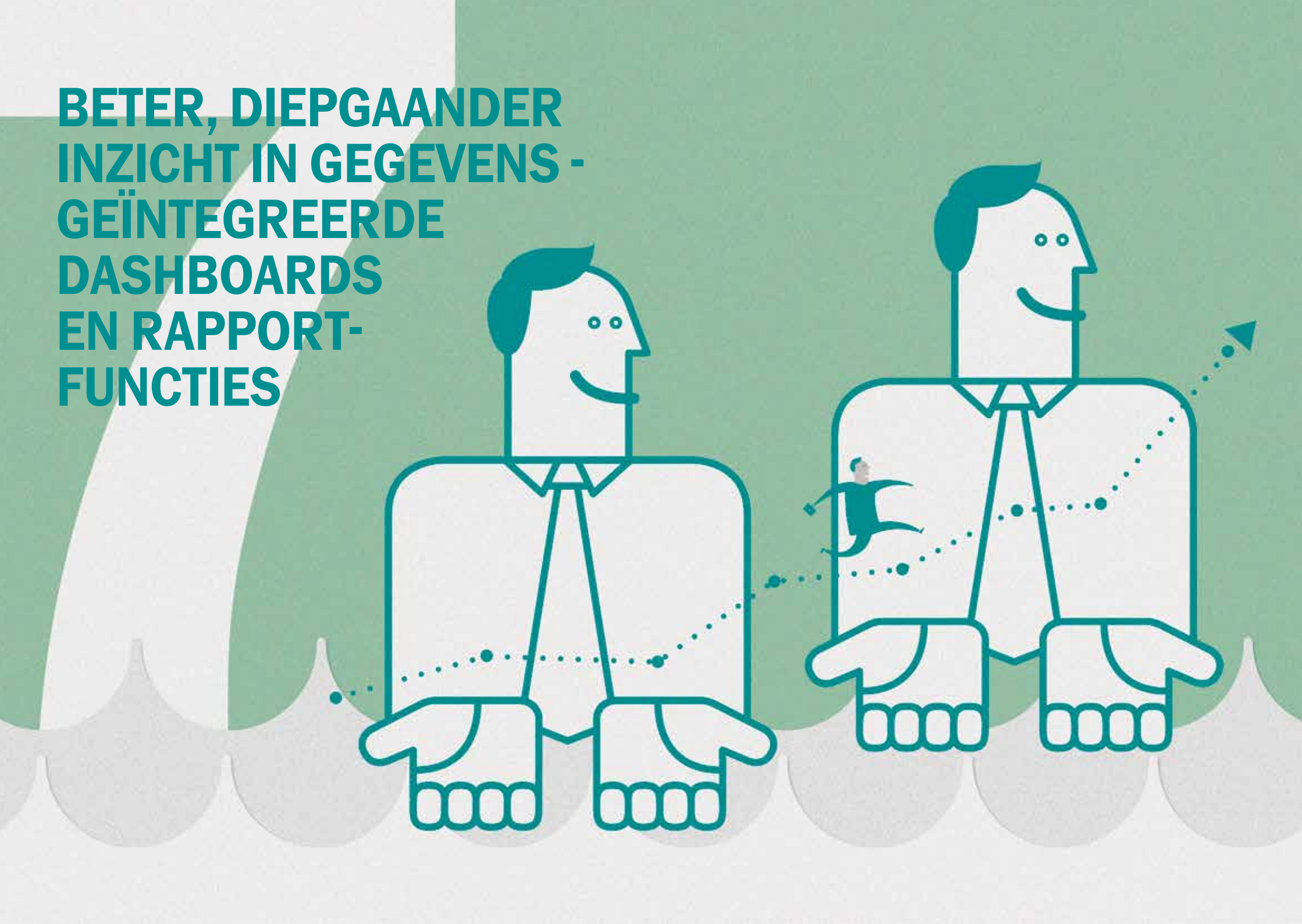
In zo'n omgeving kan zelfs de kleinste verbetering van bruikbaarheid of efficiëntie al tijdwinst opleveren en de werkdruk (en stress) van overbelaste IT-beveiligingsbeheerders verlichten. Uniforme rapporten met een vertrouwd aanzien maken analyse en beoordeling makkelijker, verbeteren het incidentbeheer en ondersteunen een proactieve benadering van IT-beveiliging.

De voordelen:

- **Eenvoudigere, snellere rapportanalyse:** in alle rapportsjablonen wordt dezelfde terminologie en structuur gehanteerd. ‘Computer, pc, node, machine’ - allemaal synoniemen voor hetzelfde beheerde endpoint. Producten en leveranciers gebruiken deze termen door elkaar; hoe groter de hoeveelheid producten waarmee wordt gewerkt, hoe verwarrender dit kan zijn. Wat nu als elk veiligheidscomponent van uw samengestelde oplossingsomgeving met een soortgelijk terminologieprobleem zou kampen? En stel dat elke parameter van elk van deze componenten een vergelijkbare, maar toch net andere naam had? In zo'n complexe omgeving wordt het onderzoeken van bedreigingen of andere incidenten een stuk ingewikkelder dan zou moeten. Zelfs voor beheerders die het systeem door en door kennen. Dat beheerders de complexiteit accepteren is tot daar aan toe, maar wat als u te maken krijgt met externe partijen, zoals auditors of toezichthouders…? Met een onsamenhangend overzicht van uw infrastructuur geeft u niet bepaald het gewenste visitekaartje af.

- **Vereenvoudigd incidentbeheer:** het eenvoudig herkennen van gelijksoortige incidenten in verschillende IT-infrastructuurnodes, zoals malware of overtredingen van beleid.

BETER, DIEPGAANDER INZICHT IN GEGEVENS - GEÏNTEGREERDE DASHBOARDS EN RAPPORT-FUNCTIES



7 BETER, DIEPGAANDER INZICHT IN GEGEVENS - GEÏNTEGREERDE DASHBOARDS EN RAPPORTFUNCTIES

Een ideaal Endpoint Protection Platform benadert dashboards en rapportage op holistische wijze. Werkelijke integratie gaat dieper dan het uiterlijk van de interface - het klikken op een willekeurig tabblad ‘endpointeigenschappen’ van een beheerconsole zou een overzicht van alle veiligheidsaspecten van de beheerde client moeten geven, inclusief het beleid dat van toepassing is, statusupdates en incidenten.

Idealiter maken dashboards en rapporten ook het instellen van een onderzoek eenvoudiger en het endpoint zichtbaarder - wanneer informatie door integratie kan worden verzameld vanuit meerdere componenten is dit een stuk eenvoudiger.

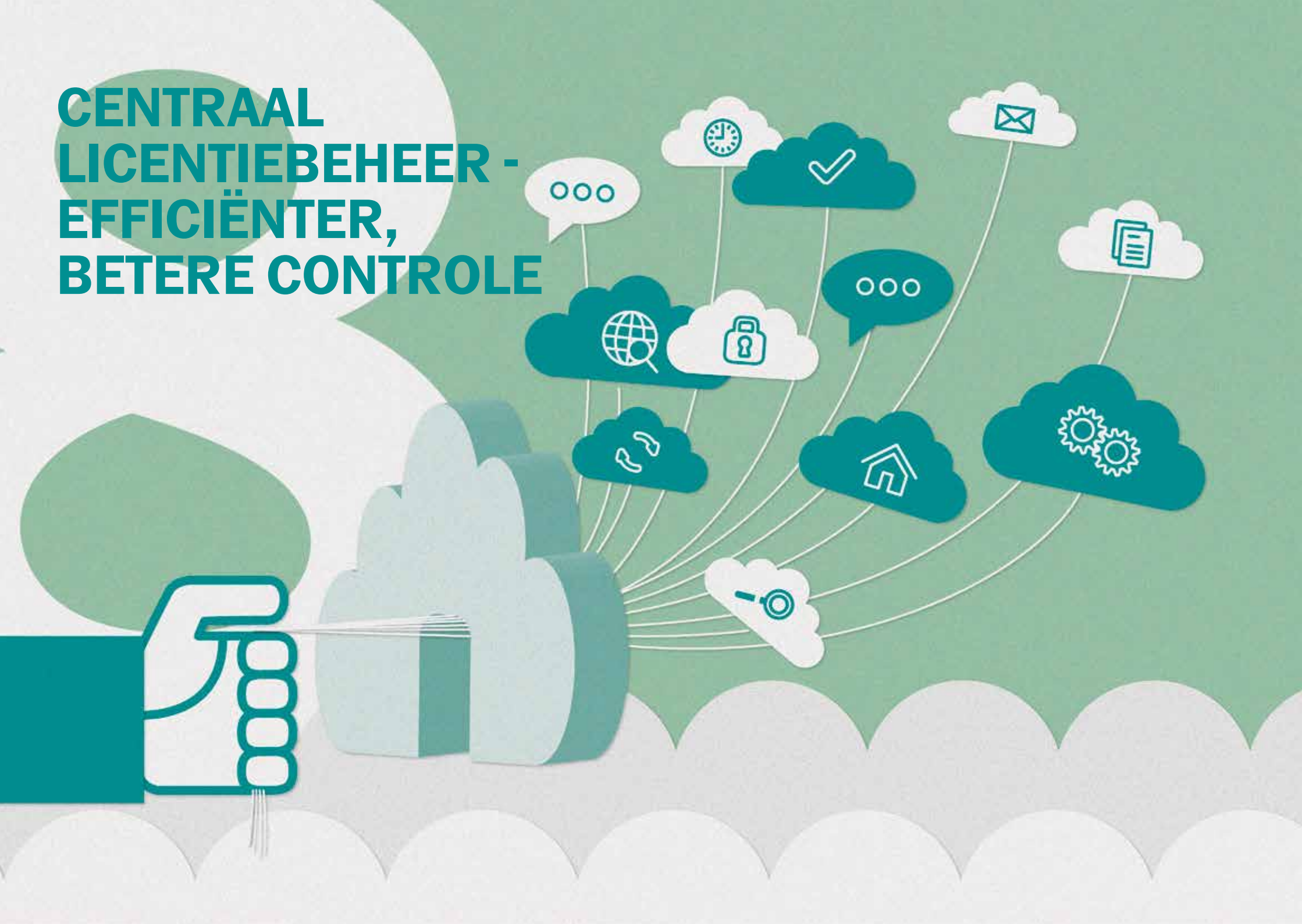
De voordelen:

- **Eén dashboard voor alle componenten van endpointbeveiliging:** een dashboard waarop u niet de hele ochtend een dampend kopje koffie ziet, dat de belangrijkste informatie bevat over de status van beheerde endpoints, de uitvoering van implementatietaken en licentiebeheer, en waarop alle belangrijke beveiligingsgebeurtenissen en -incidenten te zien zijn.

- **Gestroomlijnde diepgaande gegevensverzameling en -analyse**: gedetailleerd zoeken in onderling afhankelijke rapporten om gegevens voor verschillende doeleinden te verzamelen en te analyseren, waaronder endpointbeheer, vulnerabilitybeoordeling en patching, inventarisatie van hardware en applicaties, en gemaakte gebruikersaccounts. Goede zichtbaarheid van de beschermingsstatus en incidenten, waaronder malwaredetectie en de status van gegevensencryptie. Dit maakt veiligheidsanalyse en -onderzoek een gestroomlijnd en eenvoudig proces.

- **Kant-en-klare managementrapportage**: managementrapportage behoort tot de kerntaken van een IT-beveiligingsbeheerder. Het opstellen van gedetailleerde rapporten vanuit meerdere consoles en datasets is een tijdrovende en frustrerende klus. Daarom biedt het Endpoint Security Platform van Kaspersky functionaliteit voor kant-en-klare managementrapportage. Het handmatig aanpassen van rapporten gegenereerd met tools van derden behoort nu tot het verleden. U houdt meer tijd over voor andere projecten.

CENTRAAL LICENTIEBEHEER - EFFICIËNTER, BETERE CONTROLE



8

CENTRAAL LICENTIEBEHEER - EFFICIËNTER, BETERE CONTROLE

Het licentiebeheer voor alle beveiligingsoplossingen binnen het hele zakelijke netwerk was nog nooit zo eenvoudig. Bij Kaspersky Labs worden alle - en wij bedoelen echt ALLE - functies geactiveerd met één licentie: endpointbeveiliging, gegevensbescherming, beheer van mobiele apparaten en systeembeheer.

Deze ene licentie kan eenvoudig worden gedistribueerd binnen de zakelijke endpointinfrastructuur, ongeacht status of locatie, dus zowel naar fysieke als virtuele machines en op zowel vaste als mobiele netwerken. Met de functionaliteit van Kaspersky voor geïntegreerd licentiebeheer kunt u de licenties waarvoor u betaalt effectiever inzetten en houdt u beter grip op de validiteit ervan.

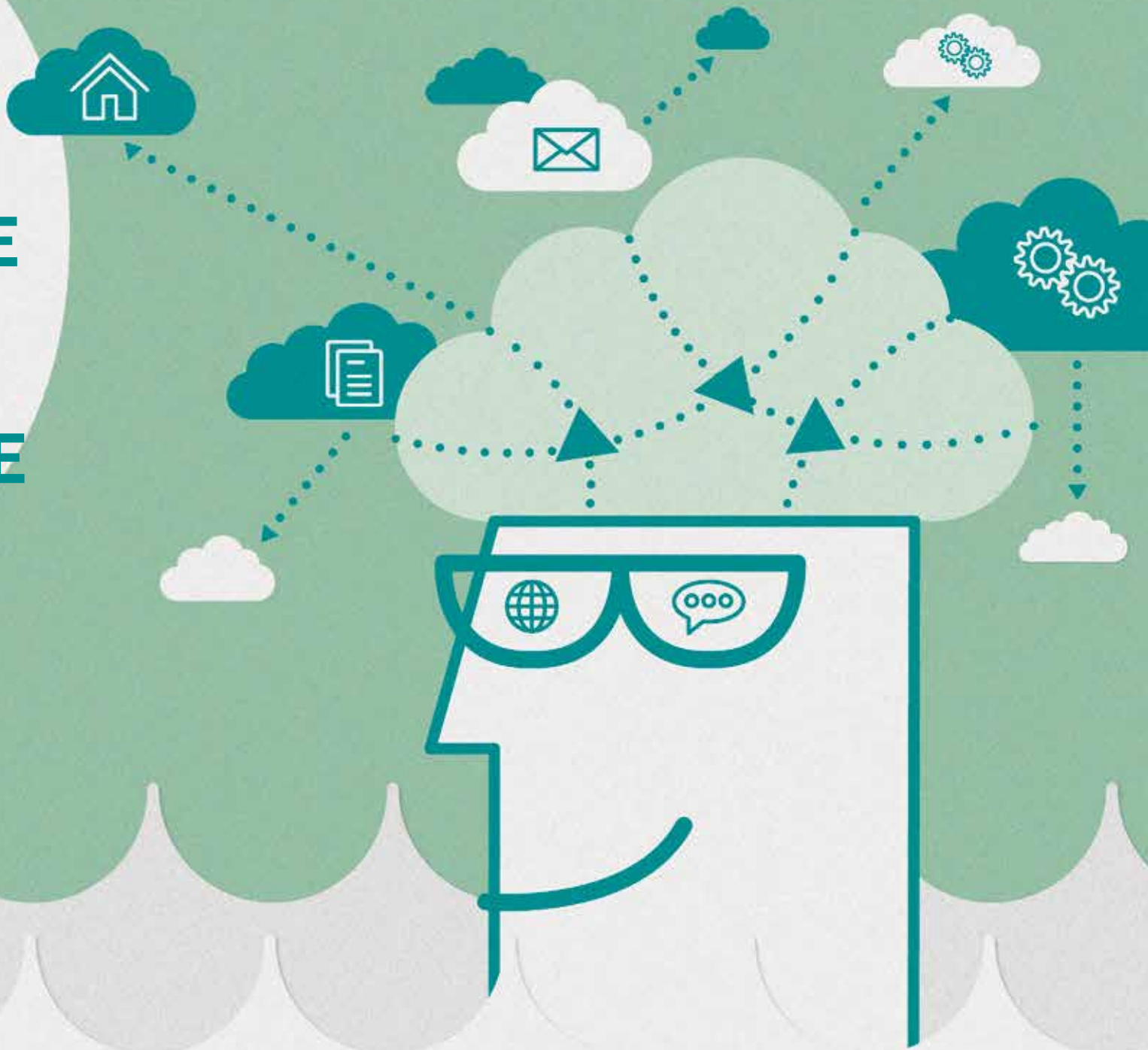
De voordelen:

- **Eén dashboard voor licentiecontrole**: u hebt geen andere tools voor licentiecontrole nodig om de status te controleren en beheren.

- **Efficiënt licentiegebruik:** reduceert de kosten door flexibele distributie in een veranderende IT-omgeving. Denk hierbij aan de migratie van traditionele pc's en notebooks naar mobiele apparaten met dezelfde functionaliteit.

- **Eenvoudige upgrade van uw beveiligingsoplossing**: met het endpointbeveiligingsplatform van Kaspersky kunt u de beveiligingsfuncties aanpassen aan uw behoeften. Begin met endpointbeveiliging en activeer functies zoals encryptie of systeembeheer eenvoudig door een nieuwe licentie toe te voegen.

EÉN ENKELE, INTERN ONTWIKKELDE CODEBASIS BEVORDERT DE INTEGRATIE



9 EÉN ENKELE, INTERN ONTWIKKELDE CODEBASIS BEVORDERT DE INTEGRATIE

De enkele codebasis van Kaspersky, die intern is ontwikkeld en wordt onderhouden, vormt de kern van ons geïntegreerde Endpoint Protection Platform.

Waar andere leveranciers de strategie hanteren om via overnames hun productaanbod te vergroten in het snel veranderende landschap van bedreigingen, onderscheidt Kaspersky zich door als enige alles intern te ontwikkelen en te onderhouden. Hierdoor wordt, in tegenstelling tot bij andere leveranciers, diepgaande integratie op codebasis ondersteund en kunnen wij de talloze voordelen bieden die in dit document worden beschreven.

De voordelen:

- Eén beheerserver en -console;
- Eén endpointclientarchitectuur;
- Eén set beleidsregels en geïntegreerde taken;
- Synergievoordelen door geïntegreerde functionaliteit;
- Geïntegreerde dashboards en rapportage.

De uniforme codebasis en ontwikkelingsprocessen maken snellere updates en patching mogelijk - gebruikers van Kaspersky hoeven slechts één applicatie te updaten en niet de doorgaans twee of meer applicaties (en bijbehorende componenten) tellende producten van veel concurrenten.

GEÏNTEGREERD AANSCHAFMODEL - ALLE BENODIGDE FUNCTIONALITEIT MET ÉÉN AANKOOP

10

10 GEÏNTEGREERD AANSCHAFMODEL - ALLE BENODIGDE FUNCTIONALITEIT MET ÉÉN AANKOOP

Met één bestelling hebt u al uw beveiligingsbehoeften gedekt; activeer alle benodigde functies via één licentie.

De voordelen:

- **Voorzien in verschillende behoeften via één pakket:** gebruikers van Kaspersky kunnen verschillende niveaus en verschillende soorten geïntegreerde functionaliteit aanschaffen die in verschillende behoeften van klanten voorzien. En dat met slechts één licentiepakket. Dit is uniek.

TOT SLOT...

Met Kaspersky Lab krijgen gebruikers een echt Endpoint Protection Platform, van begin tot eind ontwikkeld op basis van dezelfde codebasis en R&D. Onze geïntegreerde technologieën voor anti-malware en softwarevulnerabilities worden intern ontwikkeld door onze speciale onderzoeksgroep. Deze groep analyseert voortdurend hoe moderne bedreigingen systemen proberen binnen te dringen om hier effectieve bescherming voor te ontwikkelen.

De eigen applicatiewhitelist- en vulnerabilityonderzoeksgroep van Kaspersky Lab beheert ons ecosysteem van partners en leveranciers, voorziet in het voortdurend bijwerken van een database met legitieme software en biedt de meest actuele informatie over beschikbare patches.

De integratie van endpointbeveiliging en technologie voor client-/systeembeheer wordt steeds populairder. Kaspersky Lab, met een volledig eigen codebasis en intern ontwikkelingsproces, is uniek gepositioneerd om in te spelen op de overduidelijke synergievoordelen die bestaan tussen beveiligingsfuncties en functies die traditioneel worden gezien als componenten van systeembeheer.

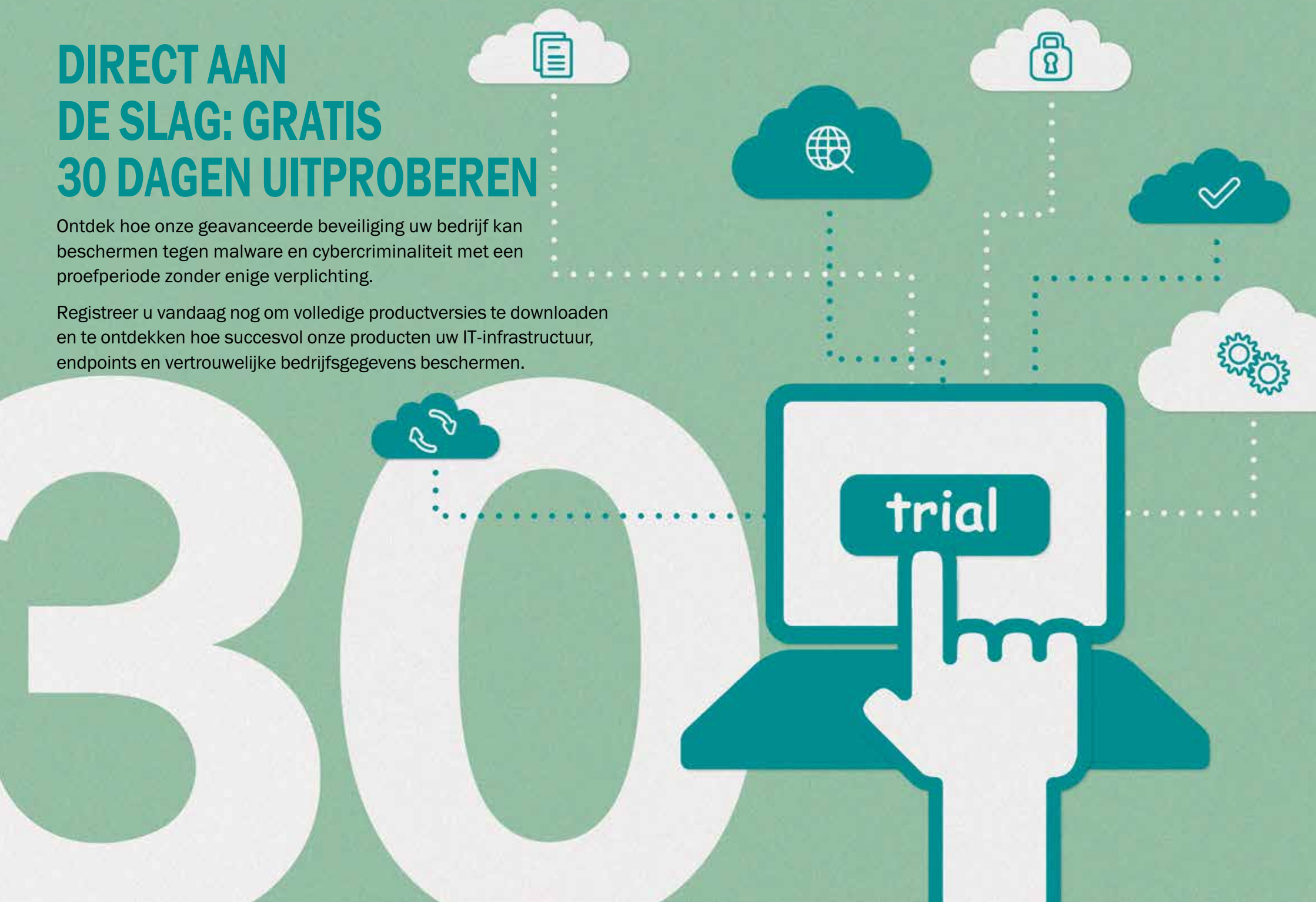
Integratie door Kaspersky Lab maakt een echt endpointbeveiligingsplatform mogelijk. Bescherming is optimaal, niet optioneel.

Meer informatie vindt u op **www.kaspersky.nl/business**

DIRECT AAN DE SLAG: GRATIS 30 DAGEN UITPROBEREN

Ontdek hoe onze geavanceerde beveiliging uw bedrijf kan beschermen tegen malware en cybercriminaliteit met een proefperiode zonder enige verplichting.

Registreer u vandaag nog om volledige productversies te downloaden en te ontdekken hoe succesvol onze producten uw IT-infrastructuur, endpoints en vertrouwelijke bedrijfsgegevens beschermen.



OVER KASPERSKY LAB

Kaspersky Lab is 's werelds grootste particuliere leverancier van beveiligingsoplossingen voor endpoints. Het bedrijf staat in de top 4 van wereldwijde leveranciers van beveiligingsoplossingen voor endpointgebruikers*. In zijn meer dan 17-jarige geschiedenis is Kaspersky Lab altijd innovatief op het gebied van IT-beveiliging gebleven en Kaspersky Lab levert effectieve digitale beveiligingsoplossingen voor grote ondernemingen, het MKB en consumenten. Kaspersky Lab, waarvan de holding is geregistreerd in het Verenigd Koninkrijk, is momenteel actief in bijna 200 landen en regio's over de hele wereld en levert wereldwijd beveiliging aan meer dan 300 miljoen gebruikers.
Meer informatie vindt u op **www.kaspersky.nl**.

* Het bedrijf staat op de vierde plaats in de IDC-rating Worldwide Endpoint Security Revenue by Vendor, 2012. De rating werd gepubliceerd in het IDC-rapport "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC #242618, augustus 2013). In het rapport worden softwareleveranciers gerangschikt op basis van de verkoopomzet voor endpointbeveiligingsoplossingen in 2012.

PRAAT MEE

#securebiz

Bekijk ons op YouTube


Bekijk ons op Slideshare


Like ons op Facebook


Lees ons blog


Volg ons op Twitter

Meld u aan op LinkedIn

KASPERSKY lab