KASPERSKY ZAKELIJKE PRODUCTEN 2013

SEE IT. CONTROL IT.
PROTECT IT.

KASPERSKY lab

OVER KASPERSKY LAB

Kaspersky Lab is het grootste zelfstandige bedrijf voor beveiligingssoftware ter wereld. Wij bieden uw organisatie de best mogelijke IT-beveiliging door een combinatie van krachtige bescherming tegen malware, flexibele beheertools, Encryptietechnologie en Systems Managementtools. Kaspersky-beveiliging beschermt alles, van het endpoint tot en met uw servers en gateways. Bovendien kunt u dankzij ons unieke geïntegreerde ontwerp al uw fysieke, virtuele en mobiele apparaten beveiligen en beheren vanaf één centrale beheerconsole, ongeacht de omvang van uw infrastructuur. Kaspersky-technologie wordt ook wereldwijd gebruikt in de producten en services van toonaangevende IT-fabrikanten en -uitgevers.

Ga voor meer informatie naar www.kaspersky.nl.

Ga voor het laatste nieuws over bescherming tegen virussen, spyware en spam, en andere problemen en trends op het gebied van IT-beveiliging naar www.securelist.nl.

HET ENIGE ECHT GEÏNTEGREERDE BEVEILIGINGSPLATFORM IN DE BRANCHE

ÉÉN CONSOLE

Kaspersky-producten zijn zodanig ontworpen dat de beheerder via één ‘dashboard’ de gehele beveiligingsomgeving kan bewaken en beheren - van virtuele machines tot fysieke en mobiele apparaten.

ÉÉN PLATFORM

Onze console, beveiligingsmodules en tools komen niet voort uit overnames van andere bedrijven maar zijn intern ontwikkeld door Kaspersky Lab. Dezelfde programmeurs hebben aan de hand van dezelfde codebasis technologieën ontwikkeld die met elkaar communiceren en samenwerken. Dit resulteert in stabiliteit, geïntegreerde beleidsregels, nuttige rapportage en intuïtieve tools.

ÉÉN PRIJS

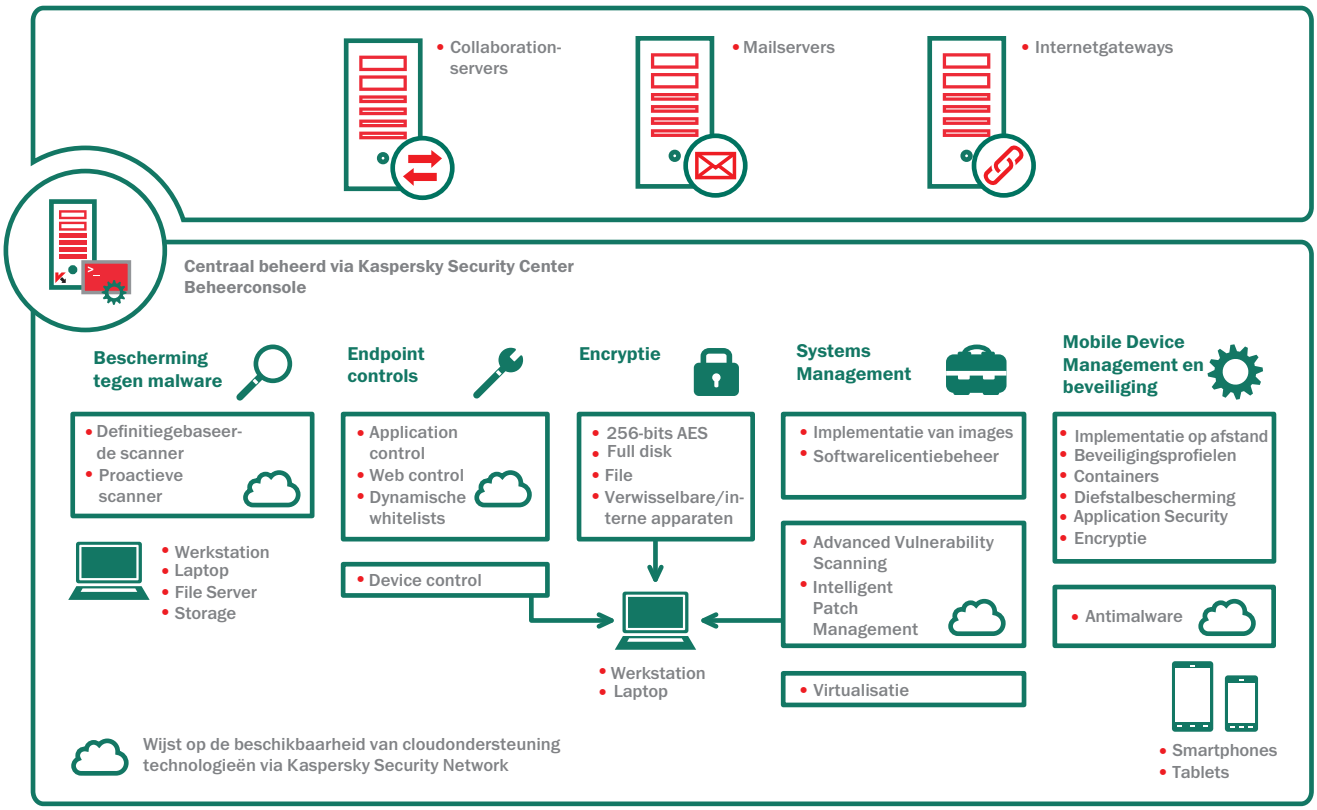
Alle producten en tools van Kaspersky zijn afkomstig van één leverancier en worden geleverd in één oplossing, zodat u niet elke keer opnieuw het budgetterings- en verantwoordingsproces hoeft te doorlopen om uw beveiligingsrisico's op één lijn te brengen met uw bedrijfsdoelstellingen.

DE JUISTE OPLOSSING VOOR U

Kaspersky Security for Business levert de juiste oplossing voor uw organisatie, of u nu uw endpoints wilt beveiligen en beheren (van werkstations tot smartphones en virtuele machines), uw servers en gateways wilt beveiligen of uw volledige beveiligingsomgeving op afstand wilt beheren.

Kaspersky beschikt over een uitgebreide lijst technologieën, van encryptie en beheer van mobiele apparatuur tot Patch Management en licentie-inventarisaties. Deze werken allemaal naadloos samen, terwijl ze worden ondersteund door het cloudgebaseerde Kaspersky Security Network, om onze klanten de beveiliging van wereldklasse te bieden die ze nodig hebben om de steeds slimmere en gevarieerdere cyberdreigingen te bestrijden.

Kortom, wij hebben het eerste – geheel nieuw ontwikkelde – beveiligingsplatform in de branche geleverd, waarmee IT-beheerders eenvoudig hun gehele omgeving kunnen zien, beheren en beschermen.

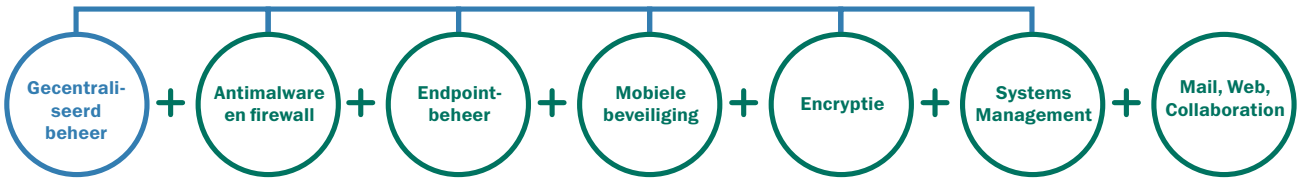


KASPERSKY SECURITY FOR BUSINESS

Onze technologieën en hoe ze met elkaar samenwerken voor u

	Core	Select	Advanced	Total	Beheerd door Security Center	Beschikbaar als Targeted Solution
Antimalware	•	•	•	•	•	
Firewall	•	•	•	•	•	
Application Control		•	•	•	•	
Device Control		•	•	•	•	
Web Control		•	•	•	•	
File Servers		•	•	•	•	•
Mobile Endpoint Agent		•	•	•	•	•
Mobile Device Management		•	•	•	•	•
Encryptie Technologie			•	•	•	
OS-imagebeheer			•	•	•	•
Licentiebeheer			•	•	•	•
Vulnerability Management			•	•	•	•
Patch Management			•	•	•	•
Network Admission Control			•	•	•	•
Collaboration				•		•
Mailservers				•		•
Internetgateways				•		•
Virtualisatie					•	•
Storage					•	•

KASPERSKY ENDPOINT SECURITY FOR BUSINESS



CORE

Deze oplossing is gebaseerd op de bekroonde en krachtige antimalwaretechnologie voor niet-servers van Kaspersky en een beschermende firewall, waaraan we onze intuïtieve beheerconsole Kaspersky Security Center hebben toegevoegd. Dit is de oplossing voor klanten die alleen anti-malware nodig hebben.

SELECT

Voortbouwend op het niveau CORE hebben we **File Server Security, Application Whitelisting en Control, Device Control en Web Control** toegevoegd aan de bescherming. U ontvangt tevens een **oplossing voor Mobiele beveiliging** die uit een **agent voor endpointbeveiliging** en **Mobile Device Management (MDM)** bestaat. Als u ook mobiele medewerkers wilt beschermen en een IT-beleid moet uitvoeren, is SELECT waarschijnlijk het juiste productniveau voor u.

ADVANCED

Op het niveau ADVANCED heeft Kaspersky **gegevensbescherming** toegevoegd in de vorm van **encryptie** van afzonderlijke bestanden of gehele schijven. In een ander nieuw aanbod, **Kaspersky Systems Management**, wordt beveiliging gecombineerd met IT-efficiëntie. Met deze uitgebreide functionaliteit ontvangen beheerders essentiële tools om het volgende te doen:

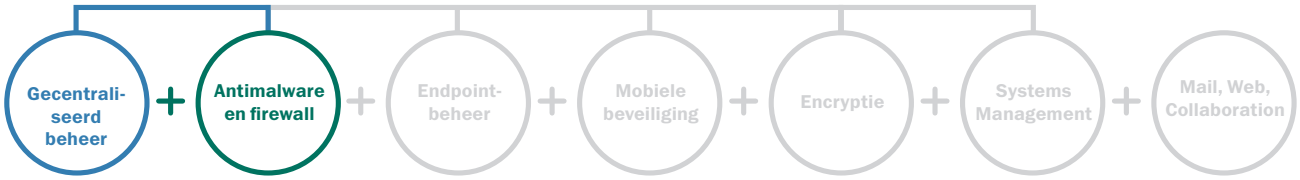
- Images maken en systemen implementeren met de module voor het beheren van images.
- De afhandeling van hardware- en softwarerisico's prioriteren met een krachtige combinatie van geavanceerde scans naar vulnerabilities en intelligent Patch Management.
- Het licentiegebruik en de compliance controleren met beheer van softwarelicenties.
- Met Network Admission Control een toegangsbeleid voor gegevens en de infrastructuur instellen voor gebruikers en gasten.
- Op afstand updates en nieuwe software voor gebruikers implementeren en installeren via de centrale console.

TOTAL

Ons ultieme product, Kaspersky Total Security for Business, combineert alle drie voorgaande niveaus en beschermt uw omgeving nog beter dankzij extra beveiliging voor de mail, web- en collaborationserver. Dit is de perfecte oplossing voor organisaties met uitgebreide beveiligingsvereisten, die de beste bescherming voor elk netwerk verlangen.

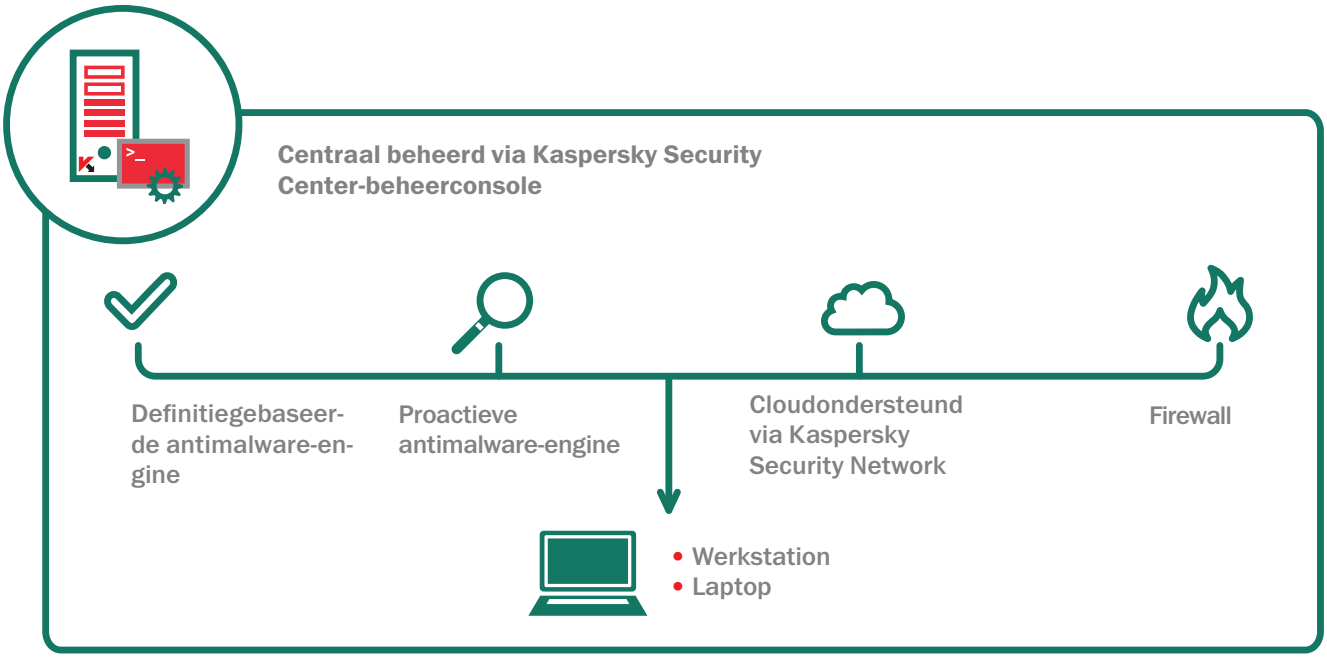
KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Core



Bekroonde antimalware met gecentraliseerde implementatie, beheerfuncties en rapportage.

Een gelaagd beveiligingsmodel begint met superieure bescherming tegen malware. Omdat Kaspersky sinds lang vermaard is om zijn capaciteiten bij het detecteren en verwijderen van schadelijke software, bestaat er geen beter fundament. Het niveau 'Core' van Kaspersky Endpoint Security for Business wordt centraal beheerd via het Kaspersky Security Center en wordt ondersteund door het cloudgebaseerde Kaspersky Security Network.



Kaspersky Endpoint Security for Business Core. Krachtige anti-malwarebescherming met realtime beveiliging via de cloud.

BELANGRIJKSTE FUNCTIES:

KRACHTIGE ANTI-MALWAREBESCHERMING VOOR ENDPOINTS
De scanengine van Kaspersky werkt op meerdere niveaus van het besturingssysteem, zodat malware volledig wordt geëlimineerd.

CLOUDONDERSTEUNING
Met het cloudgebaseerde Kaspersky Security Network worden gebruikers in realtime beschermd tegen nieuwe risico's.

GECENTRALISEERD BEHEER
Beheerders kunnen via dezelfde console centraal bestaande antivirussoftware verwijderen. Kaspersky configureren en implementeren en rapporten genereren.

ENDPOINT ANTI-MALWARE FUNCTIES:

REGELMATIGE UPDATES EN DEFINITIEGEBASEERDE BESCHERMING
Beproefde traditionele definitiegebaseerde methode voor het detecteren van malwarerisico's.

GEDRAGSANALYSE DOOR SYSTEM WATCHER
Kaspersky Security Network (KSN) treedt veel sneller dan traditionele beschermingsmethoden op tegen mogelijke risico's. De responstijd van KSN is soms slechts 0,02 seconden!

HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS) MET PERSONAL FIREWALL
De firewall kan sneller worden geconfigureerd dankzij vooraf gedefinieerde regels voor honderden veelgebruikte applicaties.

BREDE PLATFORMONDERSTEUNING
Kaspersky biedt endpointbeveiliging voor Windows®, Macintosh® en Linux®, wat het makkelijker maakt voor beheerders die heterogene netwerken moeten ondersteunen.

FUNCTIES VAN KASPERSKY SECURITY CENTER:

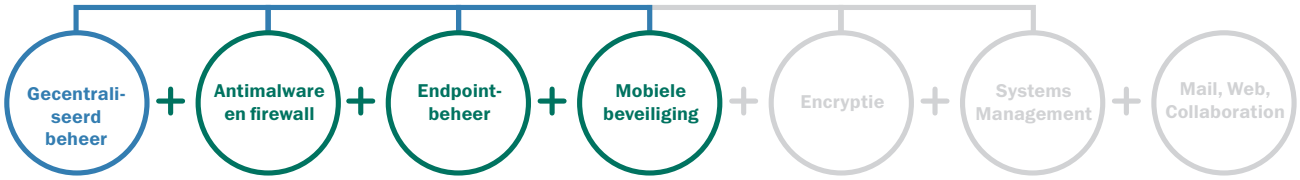
ÉÉN CENTRALE CONSOLE
Om al uw door Kaspersky beschermde endpoints op afstand te beheren.

INTUÏTIEVE GEBRUIKERSINTERFACE
Met duidelijke, bruikbare informatie in een overzichtelijk dashboard kunnen beheerders de beschermingsstatus in realtime controleren, beleidsregels instellen, systemen beheren en rapporten genereren.

WEBINTERFACE
Een toegankelijke interface voor externe bewaking van de beveiligingsstatus en rapportage van belangrijke gebeurtenissen.

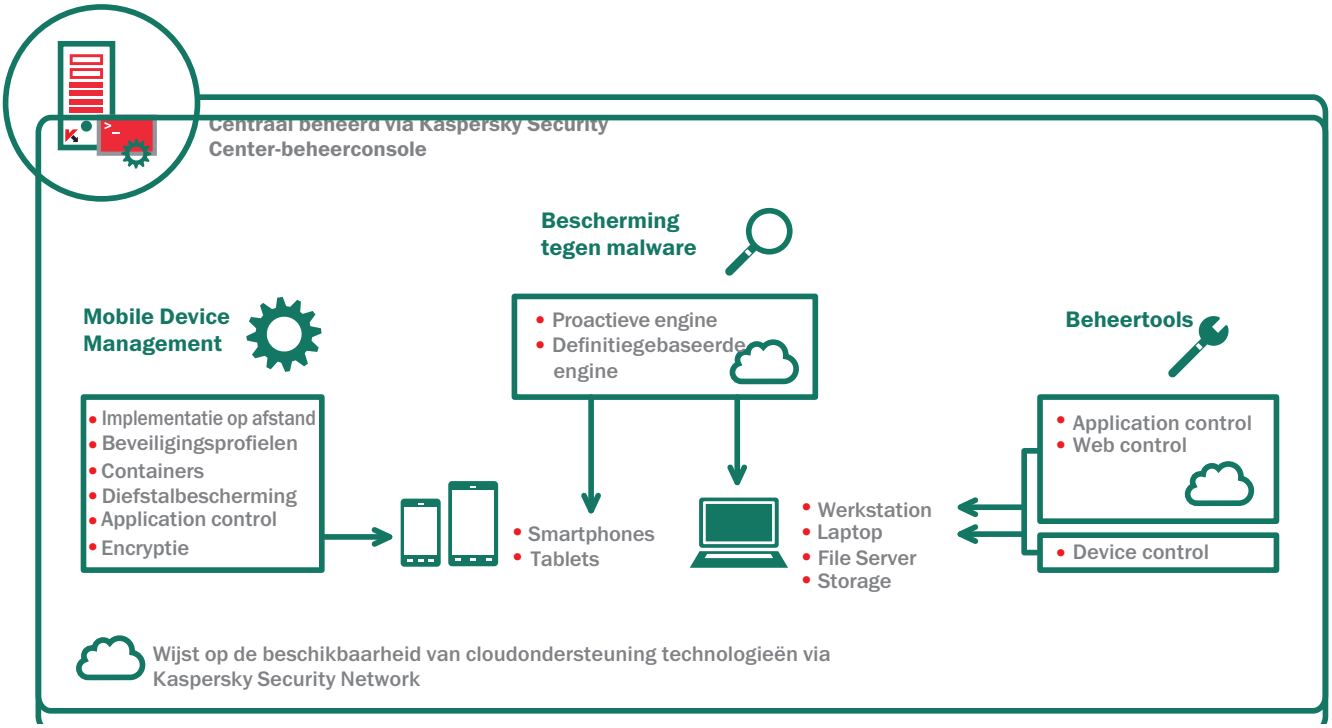
SCHAALBARE ONDERSTEUNING
Hoe groot uw infrastructuur ook wordt, Kaspersky Security Center biedt alle implementatie- en beheerfuncties, flexibele beleidsopties en robuuste rapportagevoorzieningen om aan uw toenemende behoeften te voldoen.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Select



Tools voor het ondersteunen van mobiele medewerkers zorgen ervoor dat het IT-beveiligingsbeleid wordt nageleefd en malware wordt geblokkeerd.

Het niveau 'Select' van Kaspersky omvat de implementatie en bescherming van mobiele apparaten via Mobile Device Management (MDM) en mobiele antimalware. Beheertools voor endpoints (web, apparaat en applicatie) helpen uw organisatie bij het uitvoeren van uw-IT beleid en zorgen ervoor dat de essentiële elementen van uw IT-omgeving veilig blijven.



Kaspersky Endpoint Security for Business - Select. Met Control tools en mobiele beveiliging.

BELANGRIJKSTE FUNCTIES:

KRACHTIGE ANTI-MALWAREBESCHERMING VOOR ENDPOINTS
De scanengine van Kaspersky die het beste in zijn klasse is, werkt op meerdere niveaus van het besturingssysteem, zodat malware volledig wordt geëlimineerd. Het cloudgebaseerde Kaspersky Security Network (KSN) beschermt gebruikers in realtime tegen nieuwe risico's.

FLEXIBELE, NAUWKEURIGE BEHEERTOOLS
Een cloudgebaseerde, gecategoriseerde database met veilige en onveilige applicaties en websites helpt de beheerder bij het instellen en uitvoeren van beleidsregels voor webbrowsers en andere applicaties, terwijl nauwkeurige instellingen garanderen dat alleen specifieke apparaten kunnen worden aangesloten op systemen in het netwerk.

EFFICIËNTE MOBIELE IMPLEMENTATIE EN BEVEILIGING VOOR SMARTPHONES EN TABLETS
Agentgebaseerde mobiele beveiliging is beschikbaar voor Android™-, BlackBerry®-, Symbian- en Windows® Mobile-apparaten. Beleidsregels en software voor mobiele apparaten kunnen veilig Over The Air (OTA) op deze apparaten en iOS-apparaten worden geïmplementeerd via Kaspersky MDM.

NIEUW OP DIT NIVEAU:

ENDPOINTBEHEER:

APPLICATION CONTROL
Hiermee kunnen IT-beheerders beleidsregels instellen om applicaties (of applicatiecategorieën) toe te staan, te blokkeren of te reguleren.

DEVICE CONTROL
Hiermee kunnen gebruikers een gegevensbeleid instellen, plannen en uitvoeren voor opslagapparatuur en andere randapparaten die zijn verbonden via USB of een andere interface.

WEB CONTROL
Hiermee worden specifieke endpointgebaseerde browsercontroles voor gebruikers ingesteld, ongeacht het feit of deze zich op of buiten het bedrijfsnetwerk bevinden.

DYNAMISCHE WHITELISTS
Realtime informatie van Kaspersky Security Network over de reputatie van bestanden garandeert dat uw goedgekeurde applicaties vrij van malware zijn, en maximaliseert de productiviteit van uw gebruikers.

KASPERSKY SECURITY FOR MOBILE:

INNOVATIEVE ANTIMALWARETECHNOLOGIEËN
Gecombineerde, definitiegebaseerde, proactieve en cloudondersteunde detectie resulteert in realtime bescherming. Een veilige browser en antispam verhogen de beveiliging.

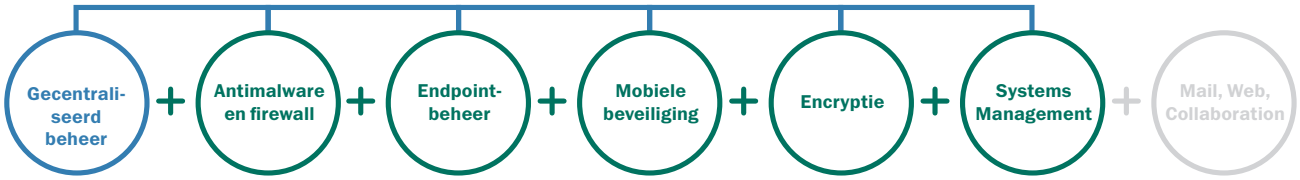
IMPLEMENTATIE MET OTA-PROVISIONING (OVER THE AIR)
De mogelijkheid om applicaties vooraf te configureren en centraal te implementeren via sms, e-mail en de pc.

EXTERNE TOOLS TEGEN DIEFSTAL
De functies SIM-Watch, Remote Lock, Wipe en Find voorkomen allemaal ongeoorloofde toegang tot bedrijfsgegevens wanneer een apparaat zoekraakt of wordt gestolen.

APPLICATION CONTROL VOOR MOBIELE APPARATEN
Bewaakt applicaties die op een mobiel apparaat zijn geïnstalleerd volgens een vooraf gedefinieerd groepsbeleid. Is voorzien van een groep voor "Mandatory Applications".

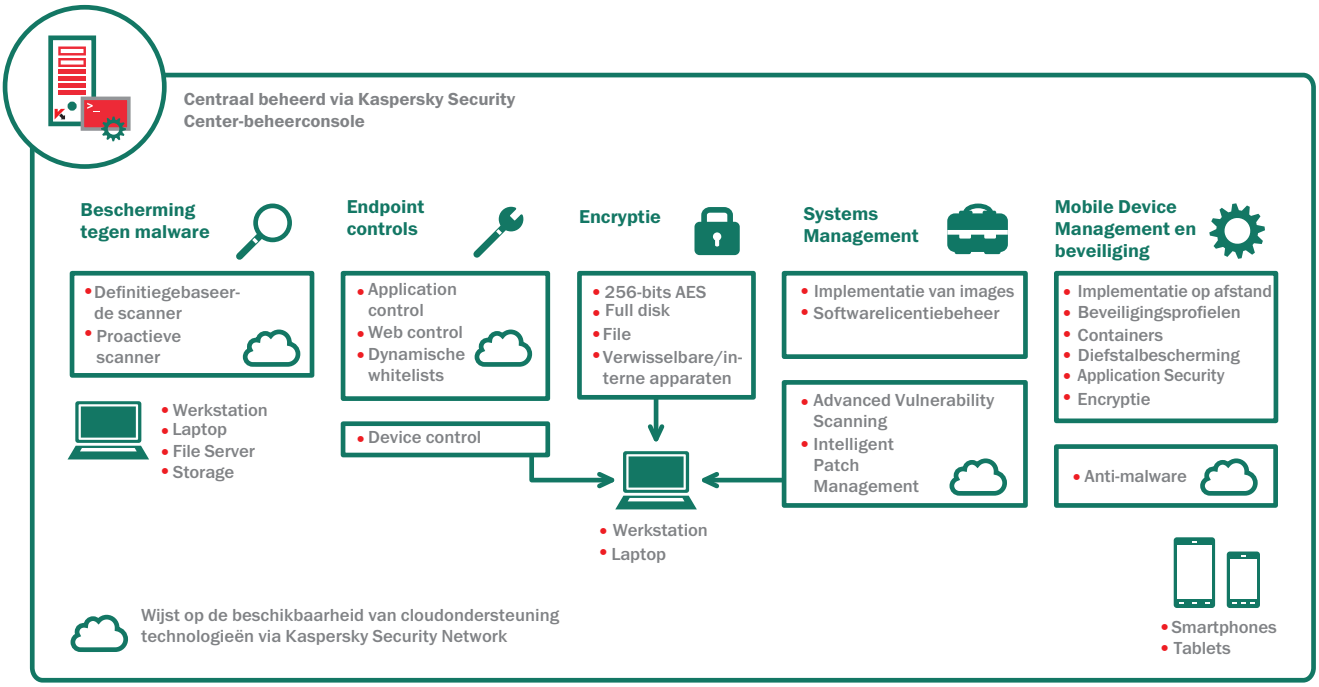
SUPPORT VOOR APPARATEN VAN WERKNEMERS
Bedrijfsgegevens en applicaties worden geïsoleerd in gecodeerde containers die transparant zijn voor de gebruiker. Deze gegevens kunnen afzonderlijk worden gewist.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS
Advanced



Uitgebreide security- en IT-functionaliteiten.

Het niveau Advanced van Kaspersky biedt de beschermings- en beheeroplossing die uw organisatie nodig heeft om het IT-beleid uit te voeren, gebruikers te beschermen tegen malware en gegevensverlies, en de IT-efficiëntie te verhogen.



Kaspersky Endpoint Security for Business - Advanced. Met Encryptietechnologie en beveiligingsSystems Management.

BELANGRIJKSTE FUNCTIES:

KRACHTIGE ENCRYPTIETECHNOLOGIE
AES 256-bits Encryptie op full disk- en folder voorkomt dat gegevens verloren gaan of gestolen worden. Bovendien kunt u hiermee veilig gegevens delen via verwisselbare apparaten, e-mail, het netwerk of internet, en dat allemaal met volledige transparantie voor de gebruiker.

SYSTEEMCONFIGURATIE EN PATCH MANAGEMENT
De functie voor het maken en implementeren van images van besturingssystemen, de functie voor het scannen op beveiligingslekken, geautomatiseerd Patch Management, Network Admission Control, inventarisaties en licentiebeheer vormen samen een volledig geïntegreerde toolkit die kan worden beheerd via één gebruiksvriendelijke centrale console.

MOBIELE IMPLEMENTATIE EN BEVEILIGING VOOR SMARTPHONES EN TABLETS
Agentgebaseerde beveiliging van mobiele mobile endpoints en apparaat- en softwarebeleidsbeheer op afstand via Kaspersky MDM.

KRACHTIGE ANTI-MALWAREBESCHERMING VOOR ENDPOINTS EN FLEXIBELE BEHEERFUNCTIES
De allerbeste cloudondersteunde antimalware- en granulaire applicaties, web- en Device Controltools van Kaspersky.

NIEUW OP DIT NIVEAU:

ENCRYPTIE EN GEGEVENSBESCHERMING:

UITGEBREIDE ENCRYPTIE
Kies tussen full disk encryptie en afzonderlijke bestanden op basis van AES (Advanced Encryption Standard) met 256-bits encryptie om kritieke bedrijfsgegevens te beschermen in geval van diefstal of verlies.

VEILIG GEGEVENS DELEN
Maak eenvoudig gecodeerde en zelfuitpakkende pakketten om de veiligheid te garanderen van gegevens die worden gedeeld via verwisselbare apparaten, e-mail, netwerken of het web.

ONDERSTEUNING VOOR VERWISSELBARE APPARATEN
Uw beveiliging wordt verhoogd met beleidsregels waarmee gegevens op verwisselbare apparaten verplicht worden gecodeerd.

TRANSPARANTIE VOOR EINDGEBRUIKERS
De Encryptieoplossing van Kaspersky werkt naadloos en onzichtbaar voor gebruikers en heeft geen nadelige gevolgen voor de productiviteit. Ook zijn er geen gevolgen voor applicatiesinstellingen of updates.

SYSTEEMCONFIGURATIE EN PATCH MANAGEMENT:

PATCH MANAGEMENT
Geavanceerde diepgaande scans naar vulnerabilities in combinatie met geautomatiseerde distributie van patches.

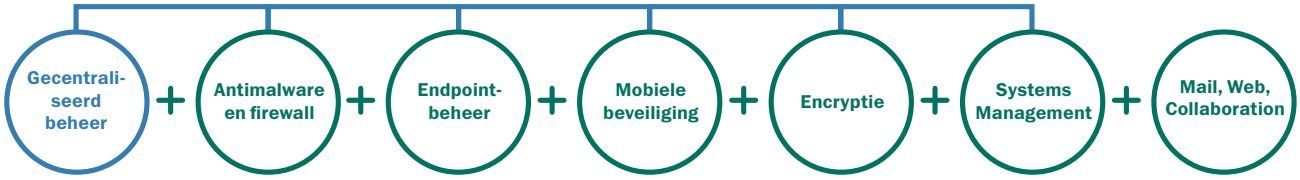
OPERATING SYSTEM EN APPLICATION IMAGE DEPLOYMENT
U kunt eenvoudig systeemimages maken, opslaan en implementeren vanaf een centrale locatie. Perfect voor een migratie naar Microsoft® Windows® 8.

SOFTWARE OP AFSTAND IMPLEMENTEREN
U kunt software op afstand implementeren op clientsystemen, zelfs in externe vestigingen.

NETWORK ADMISSION CONTROL (NAC)
Met Network Admission Control (NAC) kunt u een beleid voor 'gasten' in het netwerk definiëren. Gastapparaten (waaronder mobiele apparaten) worden automatisch herkend en naar een bedrijfsportal doorgestuurd waar deze met behulp van het juiste identificatiewachtwoord gebruik kunnen maken van de informatiebronnen die u hebt goedgekeurd.

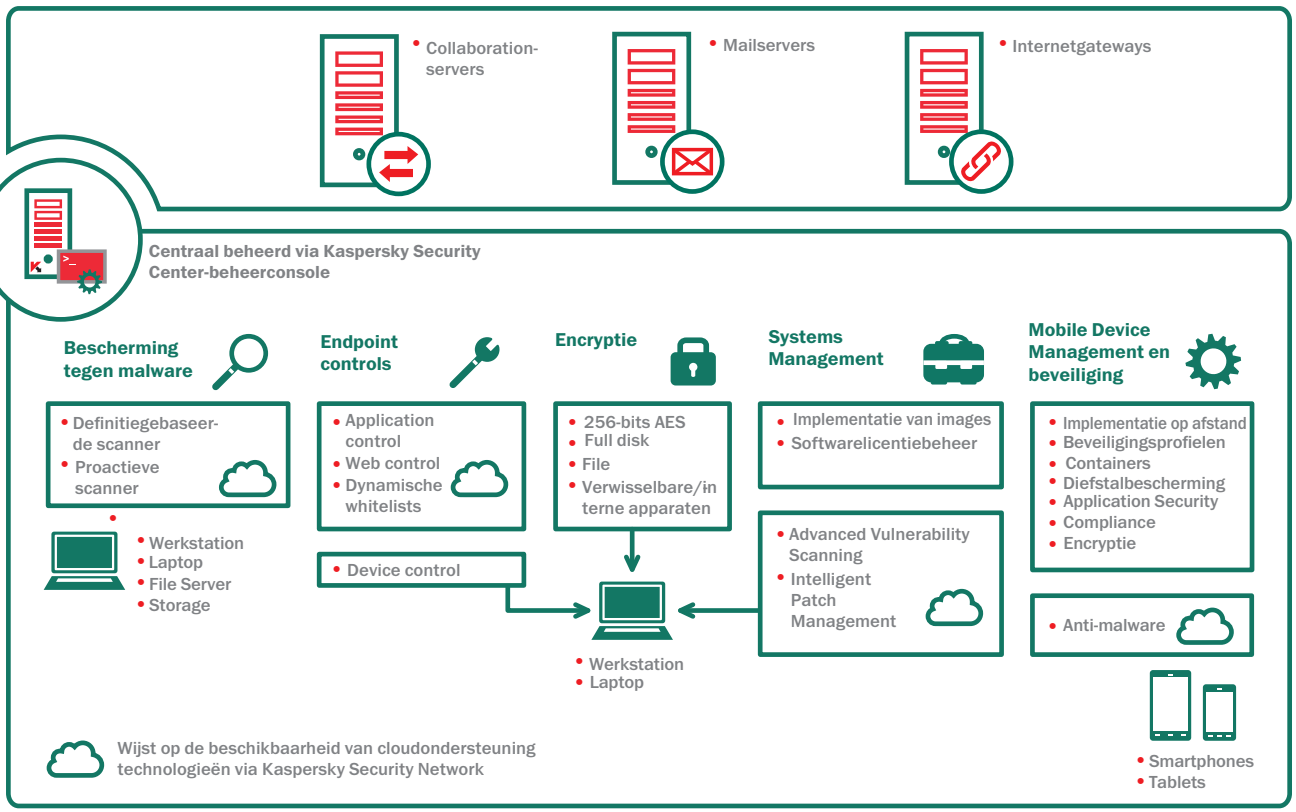
HARDWARE-, SOFTWARE- EN LICENTIEBEHEER
Met hardware- en software-inventarisatierapporten kunt u controle houden over softwarelicentieverplichtingen. U kunt kosten besparen door softwarerechten centraal te beheren.

KASPERSKY TOTAL SECURITY FOR BUSINESS



End-to-end-bescherming tegen malware, Encryptie, uitgebreide tools voor IT-efficiëntie en de uitvoering van beleid.

Kaspersky Total Security for Business biedt het meest complete beschermings- en beheerplatform dat momenteel in de branche beschikbaar is. Total Security for Business beveiligt elke laag van uw netwerk en bevat krachtige configuratietools om ervoor te zorgen dat uw gebruikers productief blijven en worden beschermd tegen malware, ongeacht het apparaat dat ze gebruiken of hun locatie.



BELANGRIJKSTE FUNCTIES:

Alle functies van de voorgaande drie niveaus plus:

BESCHERMING VAN MAILSERVER
Antimalware- en antispambescherming voor e-mailverkeer voor alle populaire e-mailsystemen

BEVEILIGING VOOR INTERNETGATEWAYS
Garandeert veilige internettoegang in de gehele organisatie door automatisch schadelijke en potentieel gevaarlijke programma's in HTTP(S)-/ FTP-/SMTP- en POP3-verkeer te verwijderen.

COLLABORATION SECURITY
Kaspersky beschermt uw SharePoint®-servers tegen malware, terwijl de functionaliteit voor content- en bestandsfiltering voorkomt dat ongewenste gegevens worden opgeslagen.

NIEUW OP DIT NIVEAU:

E-MAILSERVERS:

BEVEILIGING VAN E-MAILVERKEER
E-mail beschermen op de nieuwste versies van grote e-mail- en collaborationplatformen: Microsoft Exchange-, IBM Lotus Domino- en Linux-e-mailservers.

KSN-INTEGRATIE VOOR ANTI-SPAM
Zorgt voor een hogere detectieratio voor spam dankzij de integratie met de cloudgebaseerde dreigingsidentificatie-engine (KSN) van Kaspersky Lab.

VERMINDERDE TRAFFIC LOAD
Intelligente spamfilters met cloudondersteuning zorgen voor een aanzienlijk lagere belasting door verkeer.

OPTIMALISATIE VAN SYSTEEMBRONNEN
De nieuwe anti-virusengine, een gelijkmatige verdeling van de belasting voor serverbronnen en scanuitsluitingen zorgen samen voor een lagere belasting van uw systeem.

INTERNETGATEWAYS:

UITSTEKENDE PRESTATIES
Een krachtige anti-virusengine, optimale intelligente scantechnologie en een gelijkmatige verdeling van de belasting verhogen de prestaties en beperken de hoeveelheid resources die nodig is om op virussen te scannen.

MULTI-PLATFORM SUPPORT
Kaspersky Security for Internet Gateway ondersteunt de populairste gateways op Windows- en Linux-platformen.

COLLABORATION

ANTI-MALWAREBARRIÈRE VOOR SHAREPOINT-FARMS
Maakt gebruik van innovatieve detectietechnologie die is ontworpen om malware te identificeren en uploads of downloads in realtime te voorkomen.

CONTENTFILTERS
Hiermee worden ongewenste externe uploads voorkomen, wordt intern communicatiebeleid afgedwongen en wordt de opslag van ongewenste bestanden geblokkeerd op basis van het bestandstype of de tekstinhoud.

KASPERSKY SECURITY FOR MOBILE

Complete mobiele beveiliging met Mobile Device Management (MDM) en Endpoint Security for Mobile Devices.

Met Kaspersky MDM kunt u probleemloos en eenvoudig mobiele apparaten beveiligen terwijl Kaspersky Endpoint Security for Mobile Devices u beschermt tegen de actuele gevaren, zelfs op eigen apparaten van medewerkers.

UITGEBREIDE FUNCTIES VAN KASPERSKY SECURITY FOR MOBILE:

FUNCTIES VOOR IT-EFFICIËNTIE:

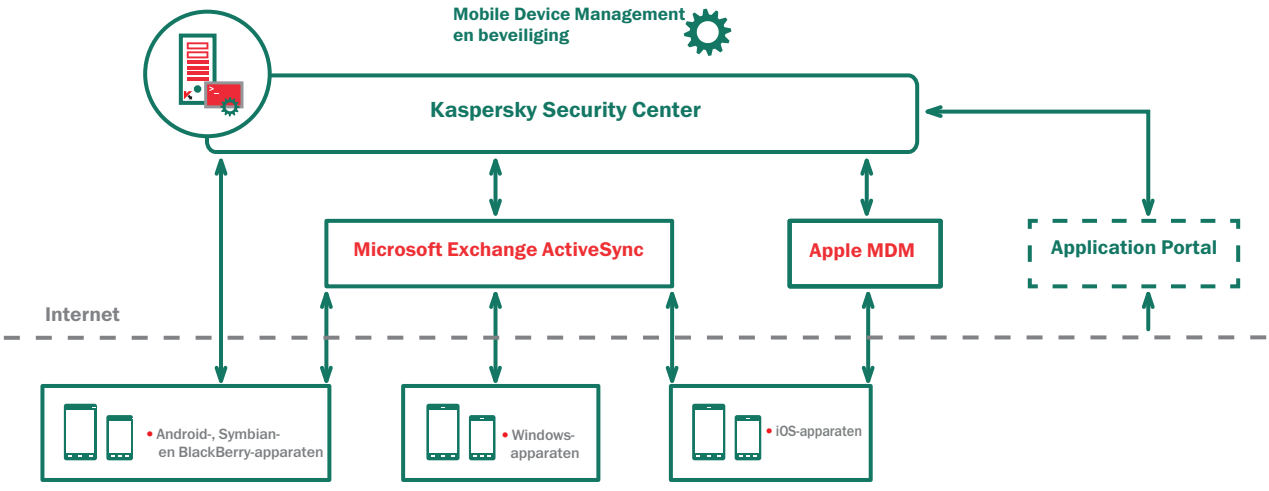
EENVOUDIGE CONFIGURATIE VIA ÉÉN CONSOLE
In tegenstelling tot andere oplossingen kunnen beheerders met Kaspersky Lab via één console de beveiliging van mobiele apparaten, fysieke endpoints, virtuele systemen, encryptie en beleidsregels beheren.

EIGEN APPLICATION PORTAL
Beheerders kunnen een bedrijfsportal met koppelingen naar goedgekeurde applicaties publiceren. Het is mogelijk in te stellen dat alleen deze applicaties kunnen worden gebruikt.

OTA-PROVISIONING (OVER THE AIR)
U kunt telefoons op afstand beveiligen door een e-mailbericht of sms met een koppeling naar de bedrijfsportal te verzenden. Daar kunnen gebruikers vervolgens het profiel en de goedgekeurde applicaties downloaden. Er wordt pas toegang tot gegevens verleend wanneer de gebruiker de configuratie heeft geaccepteerd.

VEILIGE CONFIGURATIE
Bescherm de integriteit van hardware en software door gekraakte apparaten ('rooting' en 'jailbreaking') te detecteren. Andere beschikbare beveiligingsinstellingen zijn onder meer 'camera uitschakelen' en 'wachtwoord afdwingen'.

COMPLIANCE EN BELEID UITVOEREN
Met Application Control kunt u het gebruik van applicaties op het apparaat bewaken en beheren. Daarbij beschikt u bijvoorbeeld over de functies 'Default Deny' en 'Default Allow'.



BEVEILIGINGSRISICO'S BEHEREN:

ENCRYPTIE
Mobiele gegevens worden beschermd met transparante Encryptie op full disk- en fileniveau, die ook kan worden gebruikt voor een container.

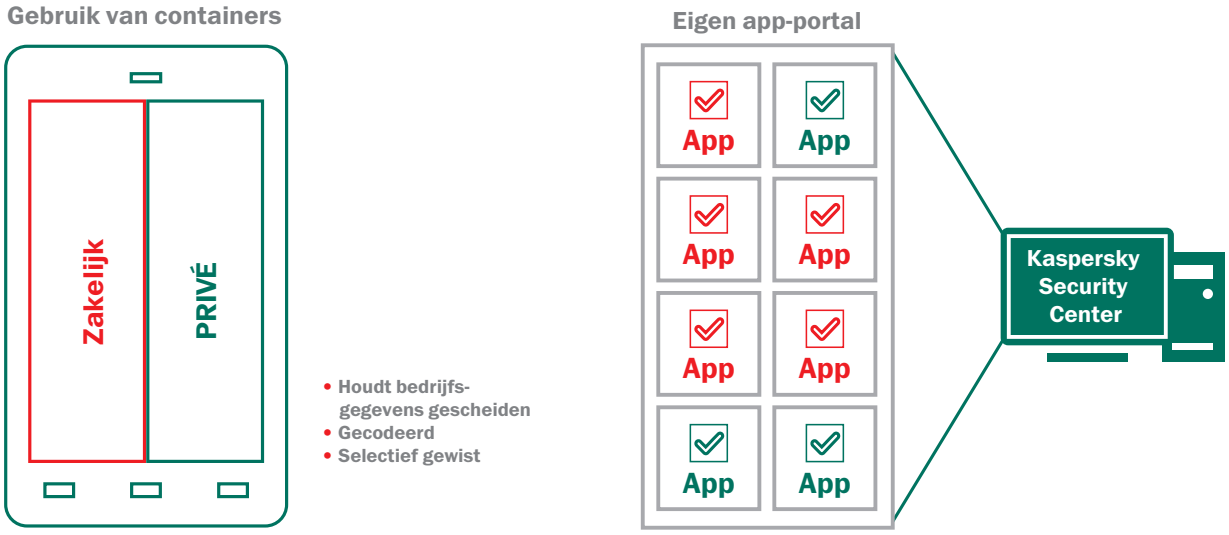
DIEFSTALBESCHERMING
Beheerders kunnen op afstand een apparaat volledig of gedeeltelijk wissen, de locatie van een zoekgeraakt apparaat achterhalen met de functie 'GPS Find' en een melding ontvangen als een simkaart wordt verwijderd of verwisseld.

MOBIELE ANTIMALWARE
De antimalware-engine van Kaspersky Lab biedt meerdere detectielagen, waaronder cloudondersteunde beveiliging, in combinatie met een veilige browser en krachtige antispamfunctionaliteit om apparaten te beschermen tegen schadelijke software.

INTEGRITEIT VAN BEDRIJFS- EN PRIVÉGEGEVENS:

CONTAINERS
Speciaal voor scenario's waarbij apparaten eigendom van de medewerker zijn, kunnen bedrijfsgegevens en applicaties in geïsoleerde 'containers' worden geplaatst. Dit biedt maximale beveiliging voor bedrijfsgegevens en optimale integriteit voor privécontent.

REMOTE DATA BEVEILIGINGSTOOLS
Als een apparaat zoekraakt, kan dit op afstand worden vergrendeld. Bedrijfsgegevens in een 'container' op het apparaat kunnen op afstand worden beveiligd, gecodeerd, beheerd en gewist, onafhankelijk van persoonlijke gegevens op het apparaat.



PERFECT VOOR BYOD-INITIATIEVEN (BRING YOUR OWN DEVICE)

Veel werknemers gebruiken hun eigen apparaten zowel voor privétaken als zakelijke taken. Sommige organisaties moedigen medewerkers zelfs aan om zelf een smartphone of tablet te kiezen bij een handelaar, waarna de IT-afdeling toegang tot e-mail en bedrijfsgegevens instelt op het apparaat van de medewerker.

Hoewel er kosten- en productiviteitsvoordelen bestaan, kan BYOD ook tot beveiligingsrisico's voor uw organisatie leiden. Als bedrijfsgegevens niet goed worden beveiligd en tussen privégegevens terechtkomen, kunnen deze eenvoudig worden misbruikt. Vaak worden de betrokken apparaten ook gebruikt door gezinsleden die zich niet om applicatiesbeveiliging bekommeren. Sommige apparaten zijn zelfs gekraakt zodat beheerderstoegang mogelijk is.

Kaspersky Security for Mobile biedt een antwoord op deze problemen doordat u smartphones en tablets kunt beveiligen en implementeren via de console die u ook voor de netwerkbeveiliging gebruikt. Dit biedt IT-beheerders de zekerheid dat apparaten van gebruikers over de juiste instellingen beschikken en kunnen worden beschermd als ze zoekraken, worden gestolen of worden misbruikt door de gebruiker.

KASPERSKY SYSTEMS MANAGEMENT

Kaspersky Systems Management biedt een uitgebreide reeks IT-productiviteitstools die in dezelfde code zijn geschreven en worden beheerd vanaf één console. Het resultaat is een platform dat de eenvoud en automatisering biedt die u verlangt, en de beveiliging en controle die u nodig hebt.

DE VERSCHEIDENHEID AAN IT-TOOLS LEIDT TOT COMPLEXITEIT, EN COMPLEXITEIT IS HET PIJNPUNT VAN IT-BEVEILIGING.

Voorkom dubbel werk
Zorg ervoor dat u niet meerdere systemen hoeft in te stellen voor nieuwe en bestaande gebruikers. Met technologie voor systeemprovisioning kunnen diskimages vanaf een centrale locatie worden gemaakt, beheerd en geïmplementeerd.

De beveiliging verbeteren
Beheerders vertellen ons dat zij vaak dagenlang alleen maar controleren of de patches up-to-date zijn. Kaspersky vermindert de complexiteit door vast te stellen welke vulnerabilities kritiek zijn en welke reparaties kunnen worden uitgesteld tot na werktijd. Dankzij deze prioritering kunnen beheerders hun dag beter indelen en de beveiliging verbeteren.

Efficiënt werken
Beheerders kunnen op afstand images, updates, patches en applicaties installeren. Als een gebruiker een probleem heeft, kan de IT zich op afstand aanmelden bij het systeem en beginnen met probleemoplossing. Dit betekent dat de beheerder niet alle bureaus hoeft af te lopen of urenlang weinig productieve en frustrerende telefoongesprekken hoeft te voeren.

Deze en andere functies van Kaspersky Systems Management zijn toegankelijk via de beheerconsole van Kaspersky Security Center. Omdat de tools niet allemaal een eigen console nodig hebben, zijn de opdrachten consistent en intuïtief en vereisen deze geen aanvullende training.

FUNCTIES VOOR SYSTEMS MANAGEMENT:

PROVISIONING VAN BESTURINGSSYSTEEM EN APPLICATIES
Eenvoudig systeemimages maken, opslaan, klonen en implementeren vanaf een centrale locatie. Garanderen dat systemen zonder problemen en met optimale beveiligingsinstellingen aan de gebruiker worden geleverd. Deze tool is uitermate geschikt voor de migratie naar Microsoft Windows 8.

VULNERABILITIES BETEUGELEN
Met een hardware- en softwarescan via één klik op de knop worden resultaten in meerdere databases met beveiligingslekken vergeleken, zodat u kunt bepalen welke risico's onmiddellijke aandacht vereisen en welke kunnen worden uitgesteld tot na werktijd.

FLEXIBELE SOFTWARE-INSTALLATIE OP AFSTAND
Minimaliseer de netwerkbelasting door handmatige of geplande implementaties te gebruiken.

EXTERNE AGENTS
Stel een werkstation in een externe vestiging of een extern filiaal in als een centrale update-agent. Bespaar bandbreedte door één update naar een externe vestiging te verzenden en deze verder op de desbetreffende locatie te distribueren met het ingestelde lokale werkstation.

ONDERSTEUNING VOOR WAKE-ON-LAN-TECHNOLOGIE
Voor implementatie of ondersteuning na werktijden kan Kaspersky Systems Management een werkstation op afstand inschakelen.

TOOLS VOOR PROBLEEMOPLOSSING
Externe en veilige verbindingen met clientsystemen om problemen op te lossen via dezelfde beheerconsole.

ONDERSTEUNING VOOR MICROSOFT WINDOWS SERVER UPDATE SERVICES (WSUS)
Kaspersky Systems Management synchroniseert regelmatig gegevens over beschikbare updates en hotfixes met servers, waaronder Microsoft Windows Update, om deze vervolgens via Windows Update Services te downloaden en op efficiënte wijze te distribueren.

NETWORK ADMISSION CONTROL (NAC)
Met Network Admission Control (NAC) kunt u een beleid voor 'gasten' in het netwerk definiëren. Gastapparaten (waaronder mobiele apparaten) worden automatisch herkend en naar een bedrijfsportal doorgestuurd waar deze met behulp van het juiste identificatiewachtwoord gebruik kunnen maken van de informatiebronnen die u hebt goedgekeurd.

HARDWARE- EN SOFTWARE-INVENTARISATIE
Pc's, harde schijven en zelfs verwisselbare apparaten worden automatisch gedetecteerd en geïnventariseerd. Wanneer een apparaat wordt toegevoegd, ontvangt de beheerder direct een melding. Dankzij deze functie kan de beheerder de status en het gebruik van hardware in het netwerk volgen.

PROVISIONING EN BEHEER VAN LICENTIES
Kaspersky Systems Management rapporteert exact welke software in gebruik is in uw omgeving. Hierdoor kunt u uw licentiekosten aanpassen en vaststellen welke gebruikers niet aan het beleid voldoen. Indien deze oplossing wordt geïmplementeerd met beheertools voor endpoints van Kaspersky Lab, kunt u instellen dat alleen goedgekeurde applicaties en versies mogen worden gebruikt en kunt u het aantal licenties beperken dat tegelijkertijd wordt gebruikt.

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security voor File Server zorgt voor een betrouwbare bescherming van servers waarop Microsoft® Windows®, Novell NetWare of Linux is geïnstalleerd, tegen alle typen schadelijke programma's.

Anti-virusbescherming voor de opslag van gedeelde bestanden is essentieel, omdat één geïnfecteerd bestand op een server de werkstations van alle gebruikers van de bron kan infecteren. Een goede beveiliging van de fileserver zorgt er niet alleen voor dat gebruikers en hun gegevens worden beschermd, maar voorkomt ook dat schadelijke programma's binnendringen in back-ups van bestanden, wat kan leiden tot terugkerende malware-uitbraken en andere incidenten.

PRODUCTVOORDELEN*

- Ondersteuning voor de nieuwste versies van Microsoft® Windows®- en Linux-platformen
- Optimaal gebruik van systeembronnen
- Ondersteuning voor HSM-systemen (Hierarchical Storage Management)
- Bescherming van terminal- en clusterservers
- VMware Ready-certificering
- Ondersteuning voor NSS-bestandssysteem
- Gratis BSD-ondersteuning

FUNCTIES

- Bescherming van fileservers waarop Windows® (inclusief Windows Server® 2008 R2), Linux (inclusief Samba) en Novell NetWare is geïnstalleerd
- Verbeterde proactieve bescherming tegen nieuwe schadelijke programma's
- Realtime anti-virusbescherming
- Afhandeling van actieve infecties
- Gepland scannen van opgeslagen bestanden
- Scannen van kritieke systeemgebieden
- Isolatie van geïnfecteerde werkstations
- Schaalbaarheid
- Back-up van gegevens voorafgaand aan uitschakeling of verwijdering
- Gecentraliseerd(e) installatie, beheer en updates
- Diverse installatie- en beheermethoden
- Flexibel systeem voor scans en reacties op incidenten
- Systeem voor meldingen over applicatiesstatus
- Uitgebreide rapporten over netwerkbeschermingsstatus

APPLICATIES

- Kaspersky Anti-Virus for Windows® Servers Enterprise Edition
- Kaspersky Anti-Virus for Linux File Server
- Kaspersky Endpoint Security for Windows®
- Kaspersky Anti-Virus for Novell NetWare
- Kaspersky Security Center

*Welke productfuncties deze bevat, is afhankelijk van de combinatie van de gebruikte componenten. Lees de componentbeschrijvingen op www.kaspersky.nl voor meer informatie over afzonderlijke componentfuncties.

KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server beschermt e-mail- en groupwareservers tegen schadelijke programma's en spam.

Het product bevat applicaties die e-mailverkeer beschermen voor alle populaire servers, waaronder Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim en CommuniGate Pro. De oplossing kan ook worden gebruikt om een speciale e-mailgateway in te stellen.

PRODUCTVOORDELEN*

BESCHERMING VAN E-MAILSERVER
Antimalware- en antispambescherming voor e-mailverkeer voor alle populaire e-mailsystemen.

OPTIMALISATIE VAN SYSTEEMBRONNEN
De nieuwe anti-virusengine, een gelijkmatige verdeling van de belasting voor serverbronnen en scanuitsluitingen zorgen samen voor een lagere belasting van uw systeem.

KSN-INTEGRATIE VOOR BESCHERMING TEGEN SPAM
Zorgt voor een hogere detectieratio voor spam dankzij de integratie met de cloudgebaseerde dreigingsidentificatie-engine (KSN) van Kaspersky Lab.

MINDER BELASTING DOOR VERKEER
Intelligente spamfilters met cloudondersteuning zorgen voor een aanzienlijk lagere belasting door verkeer.

FUNCTIES

- Geïntegreerde bescherming van e-mailservers tegen alle typen schadelijke programma's
- Efficiënte bescherming tegen spam
- Realtime anti-virusbescherming
- Gepland scannen van e-mails en databases
- Bescherming voor Sendmail-, qmail-, Postfix-, Exim- en CommuniGate Pro-e-mailservers
- Scannen van berichten, databases en andere objecten op Lotus® Domino®-servers
- Scannen van alle berichten op de Microsoft® Exchange-server, inclusief openbare mappen
- Filteren van berichten op type bijlage
- Schaalbaarheid
- Ondersteuning voor Microsoft® Exchange Server 2007-clusters en DAG voor Microsoft® Exchange Server 2010
- Back-up van gegevens voorafgaand aan uitschakeling of verwijdering
- Isolatie van geïnfecteerde objecten
- Annulering van terugkerende e-mailscans
- Handige tools voor installatie, beheer en updates
- Uitgebreide rapporten over beschermingsstatus
- Flexibel systeem voor scans en reacties op incidenten
- Systeem voor meldingen over applicatiesstatus

APPLICATIES

- Kaspersky Security for Microsoft® Exchange Servers
- Kaspersky Anti-Virus for Lotus® Domino®
- Kaspersky Security for Microsoft® Exchange Server 2003
- Kaspersky Security for Linux Mail Server

*Welke productfuncties deze bevat, is afhankelijk van de combinatie van de gebruikte componenten. Lees de componentbeschrijvingen op www.kaspersky.nl voor meer informatie over afzonderlijke componentfuncties.

KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway biedt beveiligde internettoegang voor alle medewerkers van een organisatie.

Kaspersky Security for Internet Gateway ondersteunt de populairste gateways op Windows- en Linux-platformen. Bekende schadelijke en potentieel gevaarlijke programma's die worden uitgevoerd via HTTP-, HTTPS-, FTP-, POP3- en SMTP-protocol worden automatisch verwijderd uit de gegevensstroom. Dankzij optimalisatietechnologie, schaalbaarheid en ondersteuning voor de nieuwste platformen is dit het ideale product voor grote organisaties met een enorme hoeveelheid verkeer.

PRODUCTVOORDELEN*

- Bescherming van Microsoft® Forefront® TMG
- Breed scala aan beleidsbeheer- en configuratietools
- Scannen van VPN-verbindingen
- Beveiliging van e-mailverkeer (via POP3- en SMTP-protocol)
- Scannen van HTTP- en FTP-verkeer van openbare servers
- VMware Ready-certificering

FUNCTIES

- Realtime scans van internetverkeer met behulp van HTTP-, HTTPS-, FTP-, POP3- en SMTP-protocol
- Geïntegreerde bescherming tegen alle typen schadelijke programma's
- Ondersteuning voor Squid-, Blue Coat- en Cisco®-proxyservers
- Back-ups
- Gelijkmatige verdeling van belasting voor serverprocessoren
- Schaalbaarheid
- Handige tools voor installatie, beheer en updates
- Flexibel systeem voor scans en reacties op incidenten
- Uitgebreide rapporten over netwerkbeschermingsstatus

APPLICATIES

- Kaspersky Anti-Virus for Microsoft® ISA Server en Forefront® TMG Standard Edition
- Kaspersky Anti-Virus for Microsoft® ISA Server Enterprise Edition
- Kaspersky Anti-Virus for Proxy Server

*Welke productfuncties deze bevat, is afhankelijk van de combinatie van de gebruikte componenten. Lees de componentbeschrijvingen op www.kaspersky.nl voor meer informatie over afzonderlijke componentfuncties.

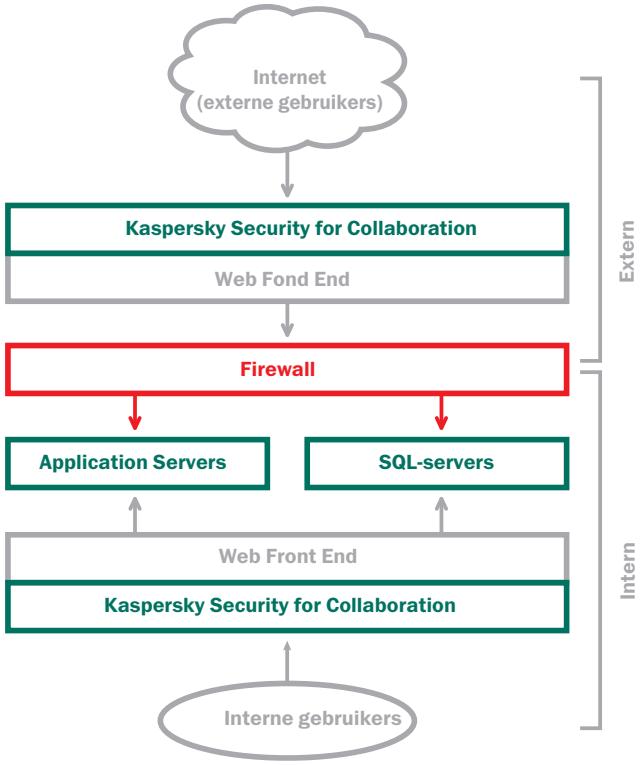
KASPERSKY SECURITY FOR COLLABORATION

Kaspersky Security for Collaboration past de nieuwste beveiligingstechnologieën toe op uw samenwerkingsplatform en combineert daarbij eenvoudig beheer met een hoog niveau op het gebied van malwaredetectie.

Kaspersky Security for Collaboration maakt gebruik van de bekroonde anti-virusengine van Kaspersky om Microsoft® SharePoint®-omgevingen te beschermen. Met de bekroonde malwaredetectietechnologie kan het product één server of complete SharePoint-farms beschermen, terwijl de functionaliteit voor content- en bestandsfiltering voorkomt dat ongewenste gegevens worden opgeslagen.

FUNCTIES

- Innovatieve detectietechnologie is ontworpen om dreigingen te identificeren en uploads of downloads in realtime te voorkomen
- Voorkomt dat eindgebruikers bepaalde typen bestanden (zoals muziek-, video- of uitvoerbare bestanden) of bestanden met ongewenste tekst opslaan
- Algemene beheerinstellingen kunnen vanaf één dashboard worden geconfigureerd op alle beveiligde servers
- Eenvoudig, intuïtief beheer - geen speciale training vereist
- Integratie met Active Directory zorgt voor een soepele installatie en gebruikersverificatie
- Gedetailleerde logbestanden en de functie voor het maken van back-ups van gewijzigde bestanden helpen beheerders bij het reageren op schendingen of beveiligingsproblemen
- Gedetailleerde, flexibele rapportage



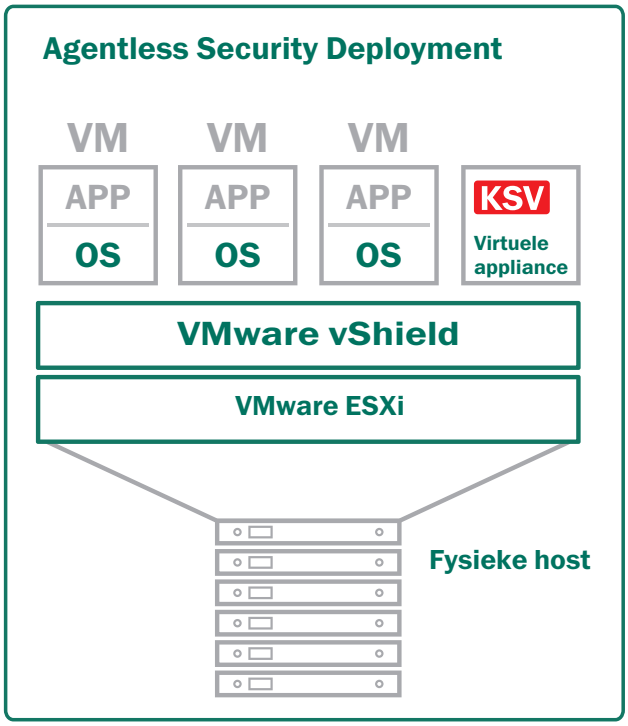
KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization, dat speciaal is ontwikkeld voor de unieke vereisten van gevirtualiseerde IT-omgevingen, biedt gevirtualiseerde servers, desktops en datacenters bekroonde bescherming tegen malware.

Kaspersky Security for Virtualization is een agentless anti-malwareoplossing voor een efficiëntere bescherming van uw gevirtualiseerde infrastructuur, waarbij de prestaties verbeteren en de impact op de virtualisatiedichtheid afneemt. De applicatie kan eenvoudig worden geïmplementeerd en biedt geavanceerde beheerfuncties die u helpen om allerlei beveiligingstaken eenvoudiger uit te voeren, zowel op fysieke als virtuele computerassets.

BEVEILIGINGS- EN PRESTATIEFUNCTIES

- Gecentraliseerde beveiliging. Kaspersky Security for Virtualization is een virtuele appliance die met vShield Endpoint van VMware wordt geïntegreerd en antimalwarescanmogelijkheden biedt. Daarbij wordt gebruikgemaakt van één gecentraliseerde antimalware-engine en -database voor elke fysieke host.
- Geavanceerde anti-virusengine. De bekroonde anti-malwaretechnologieën en ongeëvenaarde updatefrequentie van Kaspersky beschermen u tegen nieuwe en potentiële dreigingen. Een heuristische analyse biedt bescherming tegen polymorfe malware.
- Automatische beveiliging. Nieuwe virtuele systemen worden automatisch tegen malware beschermd, waardoor beveiligingsproblemen en foutieve configuraties worden voorkomen. Elke gast-VM wordt altijd beschermd tegen de nieuwste definitiedatabase, ongeacht het feit of een VM voorheen offline is geweest.
- Hogere virtualisatiedichtheid. Omdat Kaspersky Security for Virtualization een agentless oplossing is, worden updatestormen en scanstormen voorkomen, wordt een hogere virtualisatiedichtheid bereikt, is de invloed op de prestaties beperkt en worden oplossingen geboden voor beveiligingsproblemen die door bepaalde agentgebaseerde producten kunnen worden geïntroduceerd.



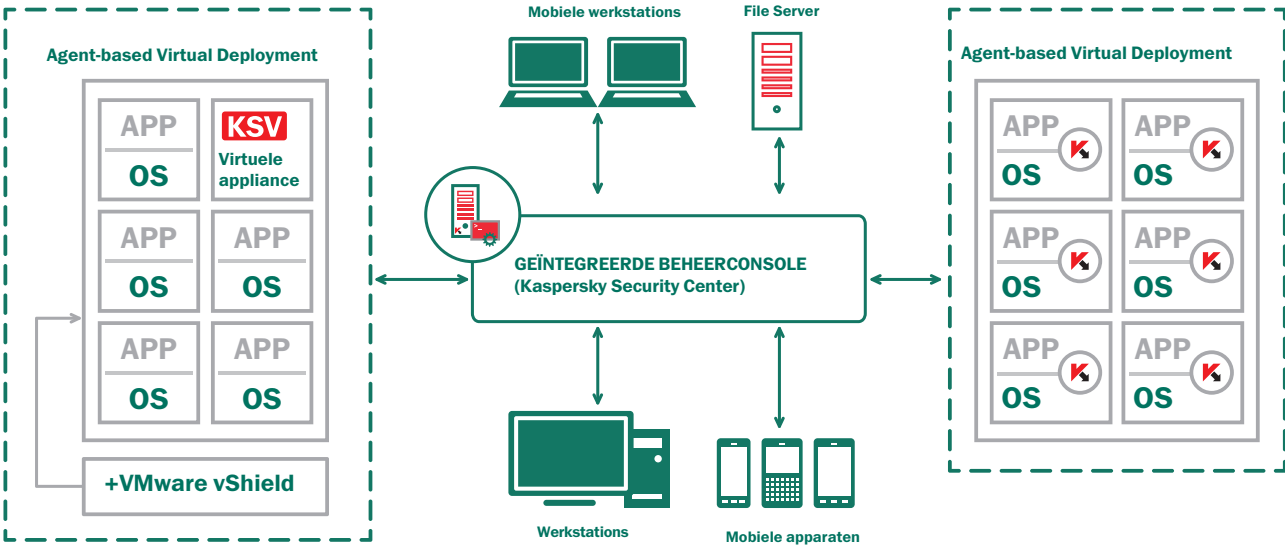
Kaspersky Security for Virtualization biedt agentloze antivirus voor VMware-implementaties.

BEHEERFUNCTIES:

ÉÉN BEHEERCONSOLE.
Kaspersky Security Center, dat niets extra's kost, is een centrale beheerconsole waarmee de beveiliging van virtuele systemen, fysieke systemen en mobiele apparaten kan worden beheerd.

ONDERSTEUNING VAN VMWARE VMOTION.
De volledige ondersteuning van VMware vMotion biedt u de garantie dat de bescherming door Kaspersky Security for Virtualization niet wordt onderbroken wanneer een werklast van de ene ESXi-host naar de andere wordt verplaatst. Als de nieuwe host over de vereiste licenties beschikt, volgt de bescherming de werklast en blijven alle beveiligingsinstellingen ongewijzigd.

INTEGRATIE MET VMWARE VCENTER.
Kaspersky Security for Virtualization ontvangt informatie over virtuele systemen van vCenter, waaronder een overzicht van alle virtuele systemen en relevante parameters. Deze integratie met vCenter vergroot niet alleen de zichtbaarheid voor het IT-team, maar zorgt er ook voor dat nieuwe virtuele systemen automatisch worden beschermd.



KSV Kaspersky Security for Virtualization

Kaspersky Lab Security Solution

KASPERSKY ANTI-VIRUS FOR STORAGE

Kaspersky Anti-Virus for Storage beschermt de EMC Celerra-productfamilie voor storage producten tegen elk type malware.

Gegevensopslagsystemen op een netwerk voorzien medewerkers van organisaties van elke omvang van snelle en eenvoudige gedeelde toegang tot informatie. Als een bedrijfsnetwerk echter onbeveiligd is, kan toegang tot gedeelde bestanden een aantal zeer ongewenste gevolgen hebben. Eén geïnfecteerd bestand dat in een systeem wordt opgeslagen, kan het complete netwerk in problemen brengen en mogelijk aanzienlijke financiële en reputatieschade voor het bedrijf opleveren. Daarom is uitgebreide beveiliging voor netwerkopslagsystemen absoluut essentieel.

Kaspersky Anti-Virus for Storage is volledig compatibel met de EMC Celerra-productlijn. Dit product is door experts ontworpen om het hoogste beschermingsniveau te bieden en malware in bestanden en archieven die zijn opgeslagen in Celerra-systemen te detecteren en te neutraliseren. Met deze oplossing kunnen beheerders het systeem zodanig configureren dat er in realtime scans worden uitgevoerd wanneer objecten worden opgeslagen of gewijzigd. Bovendien kunnen er op elk ander gewenst moment scans worden uitgevoerd.

FUNCTIES

- Beveiliging voor EMC Celerra-data storage systemen
- Ondersteuning voor Windows Server® 2008 R2
- Ondersteuning voor HSM-systemen (Hierarchical Storage Management)
- Verbeterde proactieve bescherming tegen nieuwe schadelijke programma's
- Realtime anti-virusbescherming
- Gepland scannen van opgeslagen bestanden
- Scannen van critical system areas
- Optimaal gebruik van system resources
- Back-up van gegevens voorafgaand aan uitschakeling of verwijdering
- Scalability
- VMware Ready-certificering
- Gecentraliseerd(e) installatie, beheer en updates via Kaspersky Security Center
- Volledig geïntegreerd met het Kaspersky Endpoint Security for Business-platform en andere Kaspersky-producten
- Systeem voor meldingen over applicatiesstatus
- Uitgebreide rapporten over netwerkbeschermingsstatus

Kaspersky Lab B.V.
Papendorpseweg 79
3528 BJ Utrecht
The Netherlands
sales@kaspersky.nl
www.kaspersky.nl

Alles over internetbeveiliging:
www.securelist.com

Vind een partner bij u in de buurt:
www.kaspersky.nl/partners

KASPERSKY lab