KASPERSKY lab

KASPERSKY SECURITY FOR BUSINESS 2015

‘DE KRACHT OM UW ORGANISATIE TE BESCHERMEN’

Elk bedrijf, groot of klein, staat bloot aan de gevaren van malware. Kaspersky Lab bevindt zich in een unieke positie om veel van deze dreigingen waar te nemen en te ontdekken.

Nieuwe malware gericht op afzonderlijke gebruikers en bedrijven zoals dat van u is verantwoordelijk voor meer dan 325.000 unieke dreigingen per dag.

Bij Kaspersky Lab maken we ons zorgen over deze dreigingen en het risico daarvan voor uw bedrijf. Daarom adviseren we organisaties zoals die van u om een IT-beveiligingsstrategie te hanteren die aan drie belangrijke criteria voldoet:

- **Ten eerste** moet u toegang hebben tot superieure kennis van dreigingen. Daarmee bedoelen we een grondig begrip van hoe een dreiging eruit ziet, dus hoe de code is geschreven en gecompileerd. Het is belangrijk dat er continu belangrijke informatie aan uw beveiligingssysteem wordt toegevoegd en dat uw leverancier malwarebronnen overal ter wereld controleert om nieuwe dreigingen te ontdekken.

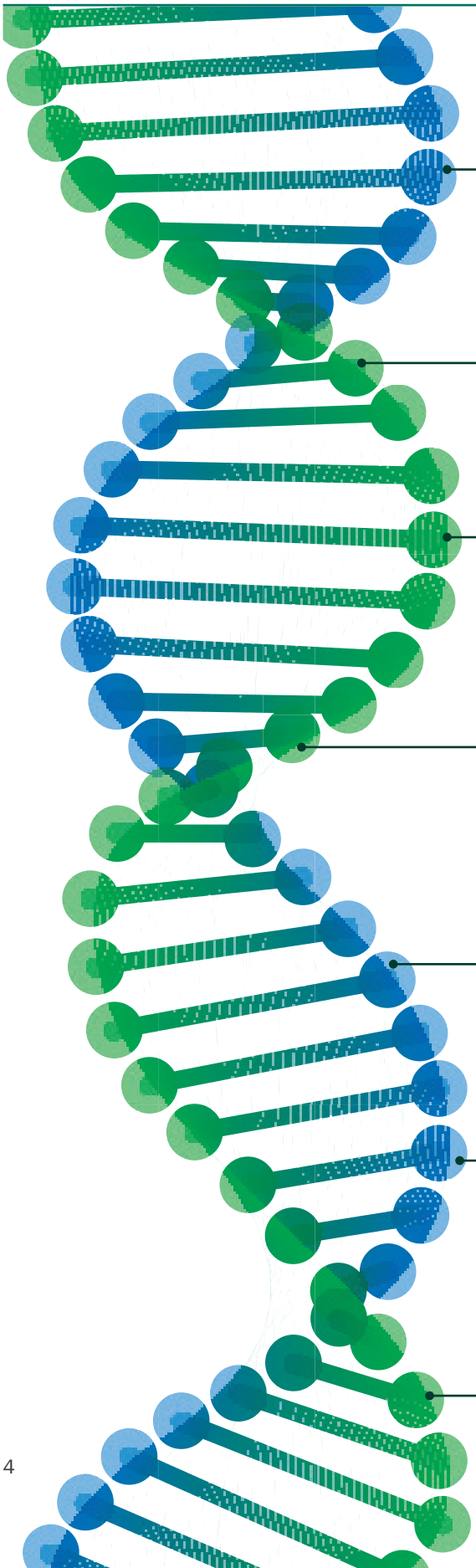
- **Ten tweede** moet u over de beveiligingstools en -technieken beschikken om bekende, onbekende en geavanceerde malware te kunnen detecteren en elimineren. Tegelijkertijd moet uw beveiligingssoftware uw systemen zo min mogelijk belasten en snel kunnen scannen, zodat uw bedrijf niet stil komt te liggen.

- **Ten derde:** omdat zakelijke IT-omgevingen steeds complexer worden, moet deze technologie naadloos, efficiënt en via één platform voorbij fysieke, mobiele en virtuele endpoints kunnen reiken, zonder softwareconflicten of gaten in de beveiliging te veroorzaken en zonder dat er verschillende consoles nodig zijn.

Alleen Kaspersky biedt één uitgebreid beveiligingsplatform met de essentiële, toonaangevende beveiligingskennis die uw bedrijf nodig heeft en de technologie om die kennis toe te passen.

Oplossingen van Kaspersky zijn eenvoudig af te stemmen op de doelstellingen van uw bedrijf. Dat betekent dat we altijd stand-by staan om uw organisatie te beschermen tegen bedreigingen van uw fysieke en virtuele endpoints en van uw mobiele apparaten, e-mailsystemen, servers, gateways en SharePoint-portals. Neem vandaag nog contact op met ons of uw IT-reseller voor informatie over de producten, oplossingen en services die in dit document worden genoemd. We laten u graag zien hoe we kunnen samenwerken om uw bedrijf tegen cyberdreigingen te beschermen.

DIGITALE BEVEILIGING ZIT IN ONZE GENEN



Expertise op alle vlakken

Toonaangevende kennis van wereldwijde dreigingen, met GREAT-team

Door de bekendste beveiligingsorganisaties gerespecteerd

Op technologie gebaseerd

Als toonaangevend erkend in onafhankelijke tests

Pionier in het ontdekken van de meest geavanceerde dreigingen

Beveiligingsincidenten zien en voorspellen met Kaspersky Security Network

BEVEILIGING MET EEN VERSCHIL

Kaspersky Lab brengt de krachtigste anti-malware op de markt door de toonaangevende beveiligingskennis te benutten die in onze genen zit en een rol speelt bij alles wat we doen – en de manier waarop we het doen.

- Onze hele verticale organisatie illustreert dat we een op technologie gebaseerd bedrijf zijn. Dat begint al bij onze CEO: Eugene Kaspersky.
- Ons Global Research & Analysis Team (GReAT), een eliteteam van IT-beveiligingsexperts, heeft een pioniersrol vervuld bij het identificeren en bestrijden van veel van de gevaarlijkste malwaredreigingen en doelgerichte aanvallen.
- Veel van de meest gerespecteerde organisaties en wetshandhavingsinstanties ter wereld hebben ons om hulp gevraagd.
- Doordat het interne team van Kaspersky Lab al zijn kerntechnologieën zelf ontwikkelt en perfectioneert, zijn onze producten stabieler en efficiënter dan die van de concurrentie.
- Kaspersky Lab doet vaker aan onafhankelijke tests mee dan andere leveranciers. Ook komen we veel vaker dan andere leveranciers als beste uit de bus!
- Alom gerespecteerde brancheanalisten, zoals Gartner, Inc., Forrester Research en International Data Corporation (IDC), bestempelen ons tot trendsetter in diverse belangrijke IT-beveiligingscategorieën.
- Meer dan 130 OEM's, waaronder Microsoft®, Cisco® Meraki, Juniper Networks en Alcatel Lucent, passen onze technologieën toe in hun eigen producten en diensten.

Dat maakt het verschil!

ONZE ANTI-MALWARETECHNOLOGIE

De effectiviteit van IT-beveiligingssoftware is volledig afhankelijk van de beveilingsengine. Patchbeheer, MDM, encryptie, apparaatbeheer, anti-phishing — al deze technologieën, en nog vele andere, vormen aanvullende, waardevolle beveiligingsniveaus. Organisaties moeten de beveiliging tegen bekende, onbekende en geavanceerde dreigingen uiterst serieus nemen.

De beveilingsengine van Kaspersky Lab wordt non-stop aangedreven en verbeterd door onze ongeëvenaarde, dynamische dreigingsintelligentie. Onze volledige focus op beveiliging, gecombineerd met onze kennis van dreigingen en onze wereldwijde ervaring, onderscheidt ons van onze concurrenten.

De toonaangevende prestaties van de anti-malware-engine van het Kaspersky Endpoint Security for Business-platform zijn bij verschillende onafhankelijke tests bewezen. Uit alles blijkt dat Kaspersky een ongeëvenaarde beveiliging biedt.

Wat maakt de anti-malware van Kaspersky Lab zo krachtig en zoveel effectiever dan andere oplossingen?

BELANGRIJKSTE PRODUCTKENMERKEN

- **Detectie van bekende, onbekende en geavanceerde dreigingen**
- **Gedragsanalyse en heuristische voorzieningen**
- **Kaspersky Security Network voor cloudondersteunde bescherming**
- **Active Disinfection**
- **Bescherming tegen encryptie en ransomware**
- **Automatic Exploit Prevention**
- **HIPS en personal firewall**
- **Network Attack Blocker**
- **Eenvoudige, overzichtelijke beheerconsole**

VOORDELEN

MEERDERE BESCHERMINGSLAGEN

De verschillende beschermingslagen van Kaspersky Lab zijn één van de redenen waarom we momenteel de meest effectieve beveiliging kunnen bieden. Omdat de technologieën van Kaspersky Lab intern worden ontwikkeld, kan de krachtige, gestroomlijnde bescherming op verschillende niveaus naadloos samenwerken, waarbij de prestaties minimaal worden beïnvloed.

In elke beschermingslaag worden cyberdreigingen vanuit een ander perspectief benaderd, waardoor IT-professionals technologieën kunnen implementeren die nauw met elkaar zijn verweven en die zowel in de diepte als de breedte bescherming bieden.

TOONAANGEVENDE KENNIS VAN DREIGINGEN — UW GARANTIE DAT U CONTINU BESCHERMD BENT

De toonaangevende kennis van dreigingen van Kaspersky Lab is wereldbefaamd. Die expertise wordt direct teruggekoppeld naar onze beveiligingsoplossingen, die ontworpen zijn om continu te evolueren in de dynamische wereld van de IT.

FUNCTIES

HEURISTISCHE BEVEILIGING OM UW SYSTEMEN MINDER TE BELASTEN

Patroongebaseerde malware-identificatie zorgt voor een betere detectie, kleinere update-bestanden en een betere beveiliging.

GEDRAGSANALYSE

De anti-malware van Kaspersky gebruikt twee specifieke componenten om programma-activiteit te analyseren:

- **Emulator** — reproduceert en verifieert de verwachte programma-activiteiten.
- **System Watcher** — controleert de activiteiten van actieve programma's en herkent en analyseert gedragspatronen die kenmerkend zijn voor malware.

CLOUDONDERSTEUNDE MALWAREDETECTIE — KASPERSKY SECURITY NETWORK (KSN)

Realtime-reactie op nieuwe en onbekende malwaredreigingen. 60 miljoen vrijwillige gebruikers van Kaspersky Lab-software leveren een constante informatiestroom met gegevens over aanvalspogingen van malware en verdacht gedrag. Op basis van deze informatie kunnen bepaalde bestanden direct als malware worden herkend, waardoor alle klanten profiteren van realtime bescherming met minder valse meldingen.

AUTOMATIC EXPLOIT PREVENTION

Automatic Exploit Prevention richt zich specifiek op malware die misbruik maakt van software-vulnerabilities in populaire applicaties door kenmerkende of verdachte gedragspatronen te herkennen. De technologie voorkomt dat de exploit kan toeslaan en dat gedownloade kwaadaardige code wordt uitgevoerd.

TEGENMAATREGELEN TEGEN ENCRYPTIE-RANSOMWARE

System Watcher bewaart kopieën van belangrijke bestanden in een tijdelijke opslagruimte, voor het geval een verdacht proces er toegang toe probeert te krijgen. Als ransomware probeert om de oorspronkelijke bestanden van encryptie te voorzien, kan de versie zonder encryptie van deze bestanden worden hersteld.

ACTIVE DISINFECTION

Gebruikt verschillende technieken om gedetecteerde infecties te 'genezen' en voorkomt het uitvoeren van bestanden en processen (zoals automatisch starten), vernietigt malware en herstelt opgeslagen bestanden.

HOST-BASED INTRUSION PREVENTION SYSTEM (HIPS) EN PERSONAL FIREWALL

Bepaalde programma-activiteiten zijn zo gevaarlijk dat ze het best kunnen worden beperkt, zelfs als de activiteiten niet als kwaadaardig bevestigd zijn. Het Host-based Intrusion Prevention System (HIPS) van Kaspersky Lab beperkt systeemactiviteiten op basis van het vertrouwensniveau van de applicatie — met behulp van een personal firewall op applicatieniveau die de netwerkactiviteit beperkt.

NETWORK ATTACK BLOCKER

Controleert verdachte activiteiten in uw netwerk — en stelt u in staat vooraf te definiëren hoe uw systemen reageren als er verdacht gedrag wordt waargenomen.

REGELMATIGE UPDATES

Uw beveiligingsdatabase wordt rechtstreeks voorzien van updates die u tegen nieuwe malwaredreigingen beschermen. Dit gebeurt door middel van de snelste updatecyclus in de sector en continu bijgewerkte gegevens over recent ontdekte malware via de cloud van Kaspersky Security Network (KSN).

TOONAANGEVENDE BESCHERMING — ONAFHANKELIJK BEWEZEN

In 2014 namen producten van Kaspersky Lab deel aan **93 onafhankelijke tests en beoordelingen**. Onze producten eindigden **66 keer bij de beste drie**, oftewel in **71% van de tests**, en werden **51 keer als beste beoordeeld**, oftewel in meer dan de helft van alle tests.

Geen product of oplossing van onze belangrijkste concurrenten komt zelfs maar in de buurt.

BEVEILIGINGSPRODUCTEN, -OPLOSSINGEN EN -SERVICES VOOR BEDRIJVEN

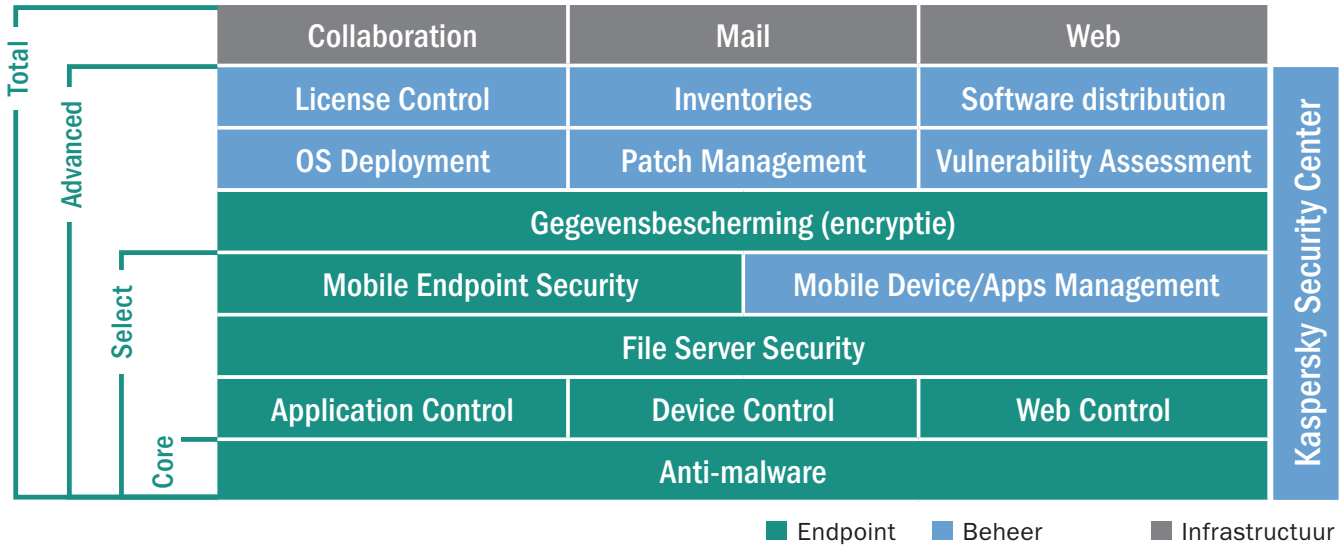
Kaspersky Endpoint Security for Business	Kaspersky Endpoint Security for Business, dat profiteert van de expertise van het beste ecosysteem voor dreigingsintelligentie ter wereld, is één geïntegreerd platform met verschillende beveiligingsniveaus. U beschikt over een robuuste applicatie, tools voor apparaat- en webbeheer, mobiele endpointbeveiliging, MDM en systeem- en patchbeheer. U kunt alles beheren vanaf één centrale console: het Kaspersky Security Center. Kaspersky Total Security for Business beveiligt uw mail-, web- en samenwerkingsservers en beschermt de grenzen en de volledige IT-omgeving van uw bedrijf.
Kaspersky Targeted Solutions	Afzonderlijke oplossingen waarmee de beveiliging van Kaspersky Lab op specifieke onderdelen van uw IT-systeem kan worden toegepast. Een aantal hiervan, zoals Kaspersky Security for Mobile, maakt ook deel uit van Kaspersky Endpoint Security for Business. Andere, zoals Kaspersky Security for Virtualization, zijn uitsluitend verkrijgbaar als gerichte oplossing. Ze maken allemaal gebruik van dezelfde toonaangevende technologieën en kennis van dreigingen en alle beveiligingsoplossingen voor fysieke, mobiele en virtuele endpoints worden centraal beheerd via het Kaspersky Security Center.
Kaspersky Security Intelligence Services en Enterprise Solutions	Profiteer van Kaspersky's kennis van dreigingen, technische expertise, gegevens en trainingsvaardigheden om uw merk, uw organisatie en uw medewerkers beter te beveiligen. Enterprise Solutions richt zich op de beveiligingsproblemen van specifieke sectoren en infrastructuren en specifieke aanvallen zoals Distributed Denial of Service (DDoS).
KASPERSKY SMALL OFFICE SECURITY	Praktische bescherming voor kleine bedrijven.
ONDERHOUDS- EN SERVICEOVEREENKOMSTEN	Verschillende ondersteuningsopties voor uw beveiligingsoplossing van Kaspersky.

OVER KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Kaspersky Endpoint Security for Business is een allesomvattende beveiligingsoplossing die is ontworpen door de beste beveiligingsexperts ter wereld. De meest grondige en proactieve bescherming, de efficiënte prestaties en het eenvoudige beheer kunnen in de vorm van progressieve lagen worden toegevoegd om uw bedrijf volledig te beveiligen.

Alle onderdelen zijn door onszelf ontworpen en gebouwd om zo één beveiligingsplatform te kunnen vormen dat specifiek is afgestemd op uw zakelijke behoeften. Het resultaat hiervan is een stabiele geïntegreerde oplossing zonder zwakke plekken, zonder compatibiliteitsproblemen en zonder extra werk wanneer uw beveiliging wordt uitgebreid.

Met Kaspersky Endpoint Security for Business kunnen beheerders evenwel de gehele IT-omgeving bewaken, beheren en beschermen. Wij leveren tools en technologieën op uitgebalanceerde en progressieve productniveaus om aan uw toenemende beveiligings- en IT-behoeften te voldoen. Kaspersky Lab kan uw werk gemakkelijker maken.

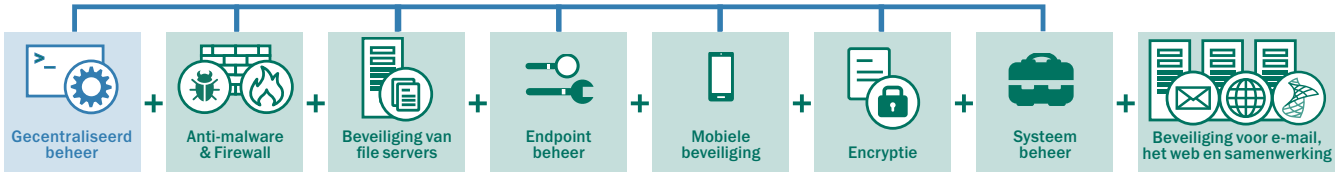


Kaspersky beschikt over een uitgebreide lijst technologieën — die allemaal op dezelfde codebasis zijn gebaseerd en daardoor optimaal samenwerken en bovendien worden ondersteund door het cloudgebaseerde Kaspersky Security Network — om onze klanten de superieure bescherming te bieden die zij nodig hebben.

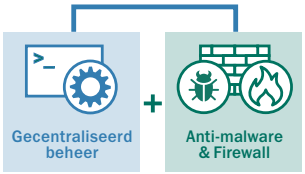
Kortom, wij hebben het eerste – geheel nieuw ontwikkelde – beveiligingsplatform in de branche geleverd, waarmee de beheerder eenvoudig uw gehele omgeving kan bewaken, beheren en beschermen.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Krachtige bescherming met meerdere lagen tegen bekende, onbekende en geavanceerde dreigingen, ontworpen en gebouwd door de beste beveiligingsexperts in de branche. Kaspersky Endpoint Security for Business biedt ongeëvenaarde IT-beveiliging en -beheer, ondersteund door wereldwijd vermaarde informatie over dreigingen.



KASPERSKY ENDPOINT SECURITY FOR BUSINESS — CORE



De allerbeste bescherming tegen malware — de basis van het beveiligingsplatform van Kaspersky Lab

De beveiligingstechnologieën met meerdere beschermingslagen van Kaspersky Lab worden intern ontwikkeld door mensen met een passie voor beveiliging. Het resultaat, en dit wordt bevestigd door onafhankelijke tests, is de krachtigste, effectiefste beveiligingsoplossing in de industrie — er bestaat geen betere bescherming voor uw organisatie.

Bescherming tegen bekende, onbekende en geavanceerde dreigingen — Unieke, geavanceerde technologieën identificeren en elimineren bestaande en nieuwe dreigingen.

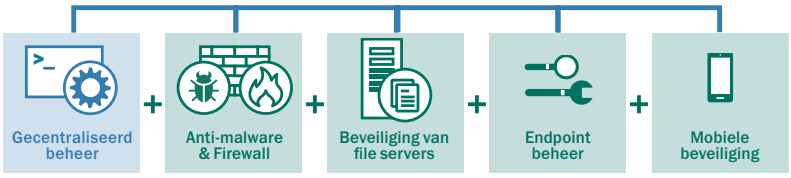
Automatic Exploit Prevention — Proactieve identificatie van en bescherming tegen onbekende en geavanceerde dreigingen.

Cloudondersteunde bescherming — Op basis van realtime gegevens van het wereldwijde Kaspersky Security Network.

System Watcher — Een unieke functie voor het herstel van bestanden bij besmetting van het systeem.

Host-based Intrusion Prevention System (HIPS) met personal firewall — HIPS beperkt activiteiten in overeenstemming met het vertrouwensniveau van de applicatie, ondersteund door een personal firewall op applicatieniveau die netwerkactiviteit beperkt.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — SELECT



Krachtige, granulaire tools voor endpointbeheer, gecombineerd met proactieve beveiliging en beheer van mobiele apparaten en gegevens

Beheer voor applicaties, internet en apparaten, inclusief dynamische whitelists ondersteund door het unieke interne lab van Kaspersky, voegen een extra laag toe aan de grondige endpointbeveiliging. Mobiele (BYOD-)apparaten van het bedrijf en de werknemers worden ook beveiligd. Alle platformen worden samen met alle beschermde endpoints beheerd via de Kaspersky Security Center-console. Bescherming van file servers voorkomt dat infecties zich via opgeslagen gegevens verspreiden naar beveiligde endpoints.

ENDPOINTBEHEER

Applicatiebeheer met dynamische whitelists — Op basis van realtime informatie van het Kaspersky Security Network over de reputatie van bestanden kunnen IT-beheerders applicaties toestaan, blokkeren of reguleren, bijvoorbeeld door een 'Default Deny'-scenario toe te passen in een actieve omgeving of testomgeving. Application Privilege Control en Vulnerability Scanning controleren applicaties en beperken applicaties die verdacht gedrag vertonen.

Web Control — Een beleid voor internetgebruik kan worden ontwikkeld rond vooraf ingestelde of aanpasbare categorieën voor uitgebreid toezicht en efficiënt beheer.

Device Control — Een granulair gegevensbeleid dat de aansluiting regelt van verwisselbare storage-apparaten en overige randapparatuur kan worden ingesteld, gepland en afgedwongen met masks voor gelijktijdige implementatie op meerdere apparaten.

BEVEILIGING VAN FILE SERVERS

Wordt samen met endpointbeveiliging beheerd via het Kaspersky Security Center.

MOBIELE BEVEILIGING

Krachtige beveiliging voor mobiele apparaten — Geavanceerde, proactieve en cloudondersteunde technologieën bieden samen meerdere realtime beschermingslagen voor mobiele endpoints.

Componenten voor webbeveiliging, anti-spam en anti-phishing schroeven de beveiliging van apparaten verder op.

Anti-diefstaltools zoals vergrendelen, wissen, traceren, SIM Watch, alarm, Mugshot en Full of Selective Wipe voorkomen ongeautoriseerde toegang tot bedrijfsgegevens als een mobiel apparaat is zoekgeraakt of gestolen. Dankzij autorisatie van beheerders en eindgebruikers en ondersteuning van Google Cloud Management, kan er snel actie worden ondernomen als dit nodig is.

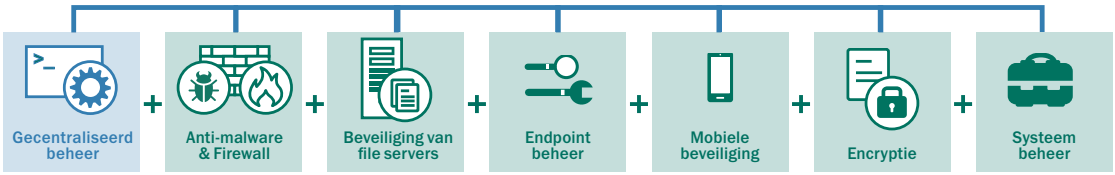
Mobile Application Management (MAM) — Laat gebruikers alleen applicaties op whitelists uitvoeren en voorkomt zo het gebruik van ongewenste of onbekende software. **Application Wrapping** isoleert bedrijfsgegevens op eigen apparaten van werknemers. Aanvullende encryptie en 'Selective Wipe' kunnen op afstand worden gehandhaafd.

Mobile Device Management (MDM) — Een uniforme interface voor apparaten met **Microsoft® Exchange ActiveSync** of **iOS MDM** met OTA-beleidshandhaving (Over The Air). **Samsung KNOX** voor Android™-apparaten wordt ook ondersteund.

Self-Service Portal — Hiermee kunnen werknemers zelf hun eigen goedgekeurde apparaten registreren bij het netwerk. Alle vereiste certificaten en codes worden automatisch geïnstalleerd en gebruikers/eigenaars kunnen zelf anti-diefstalfuncties activeren om IT-medewerkers taken uit handen te nemen.

Kaspersky Endpoint Security for Business — SELECT bevat ook alle onderdelen van het niveau CORE.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS — ADVANCED



Systeembeheertools voor optimale IT-efficiëntie en beveiliging, terwijl geïntegreerde encryptie gevoelige gegevens beschermt

Geautomatiseerd patchbeheer, beheer van besturingssysteemimages, softwaredistributie op afstand en SIEM-integratie stroomlijnen het beheer, terwijl hardware- en software-inventarisatie en licentiebeheer inzicht en controle bieden. Geïntegreerde encryptietechnologie voegt een krachtige gegevensbeschermingslaag toe.

SYSTEEMBEHEER

Vulnerability- en patchbeheer — Geautomatiseerde vulnerabilitydetectie en -prioritering in besturingssystemen en applicaties in combinatie met een snelle geautomatiseerde distributie van patches en updates.

Implementatie van besturingssystemen — U kunt eenvoudig Golden Images maken, opslaan en implementeren vanaf een centrale locatie, inclusief UEFI-ondersteuning.

Softwaredistributie en probleemoplossing — Op afstand software en applicaties installeren en handmatig of gepland het besturingssysteem bijwerken, met Wake-on-LAN-ondersteuning. Tijdbesparende probleemoplossing op afstand en efficiënte softwaredistributie met Multicast-technologie.

Hardware- en software-inventarisatie en licentiebeheer — Identificatie, zichtbaarheid en beheer (inclusief blokkering), in combinatie met beheer van licentiegebruik, voor een overzicht van alle software en hardware die in de omgeving wordt gebruikt, inclusief verwisselbare apparaten. Licentiebeheer voor software en hardware, detectie van gastapparaten, beheer van machtigingen en toegangsprovisioning zijn ook beschikbaar.

SIEM-integratie — Ondersteuning voor IBM® QRadar- en HP ArcSight SIEM-systemen.

Role-Based Access Control (RBAC) — In complexe netwerken kunnen beheertaken worden toegewezen met consoleweergaven die op basis van toegewezen functies en rechten worden aangepast.

ENCRYPTIE

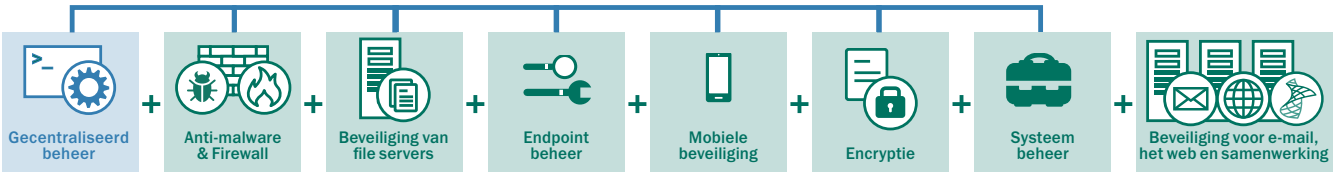
Krachtige gegevensbescherming — File/Folder Encryption (FLE) en Full Disk Encryption (FDE) kunnen op endpoints worden toegepast. Ondersteuning van een 'draagbare modus' maakt encryptiebeheer mogelijk voor apparaten die beheerdomeinen verlaten.

Flexibele gebruikersaanmelding — Pre-Boot Authentication (PBA) voor extra beveiliging, met optionele Single-Sign-On met volledige transparantie voor gebruikers. Dubbele of op tokens gebaseerde verificatie is ook beschikbaar.

Geïntegreerde beleidscreatie — Unieke integratie van encryptie bij beheer van applicaties en apparaten biedt een extra beschermingslaag en beheergemak.

Kaspersky Endpoint Security for Business — ADVANCED bevat ook alle onderdelen van de niveaus SELECT en CORE.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Organisaties die op zoek zijn naar uitgebreide bescherming voor hun volledige IT-omgeving kiezen Kaspersky Total Security for Business

Kaspersky Total Security for Business biedt het meest complete beschermings- en beheerplatform dat momenteel in de branche beschikbaar is. Kaspersky 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.

BEVEILIGING VAN MAILSERVER

Hiermee kunt u effectief malwaredreigingen via e-mail, phishingaanvallen en spam voorkomen met behulp van cloudondersteunde realtime updates voor een uitstekend detectiepercentage en een zeer laag aantal false positives. Anti-malwarebeveiliging voor IBM® Domino® is ook inbegrepen. DLP-functionaliteit voor Microsoft Exchange is apart verkrijgbaar.

BEVEILIGING VOOR INTERNETGATEWAYS

Garandeert veilige internettoegang in de gehele organisatie door automatisch schadelijke en potentieel gevaarlijke programma's in HTTP-/HTTPS-, FTP-, SMTP- en POP3-verkeer te verwijderen.

COLLABORATION SECURITY

Beschermt SharePoint®-servers en -farms tegen alle soorten malware. DLP-functionaliteit voor Sharepoint (apart verkrijgbaar) biedt content- en bestandsfiltering om vertrouwelijke gegevens te identificeren en te beschermen tegen gegevenslekken.

Kaspersky Total Security for Business bevat ook alle onderdelen van de niveaus ADVANCED, SELECT en CORE.

PRODUCTKENMERKEN

Welke oplossing is geschikt voor u?

	Core	Select	Advanced	Total	Beheerd door het Security Center	Targeted Solutions
Anti-malware	●	●	●	●	●	
Firewall	●	●	●	●	●	
Application Control		●	●	●	●	
Device Control		●	●	●	●	
Web Control		●	●	●	●	
File Server Security		●	●	●	●	●
Mobile Endpoint Security		●	●	●	●	●
Mobile Device/Apps Management		●	●	●	●	●
Encryptie			●	●	●	
Vulnerability Assessment			●	●	●	●
Patch Management			●	●	●	●
Inventories			●	●	●	●
License Control			●	●	●	●
Software distribution			●	●	●	●
Operating Systems Deployment			●	●	●	●
Collaboration Server Security				●		●
Mail Server Security				●	●	●
Internet Gateway Security				●		●
Virtual Infrastucture Security					●	●
Storage Server Security					●	●

● Beschikbaar ● Gedeeltelijk beschikbaar — zie productpagina's voor meer informatie

KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server biedt voordelige, betrouwbare, schaalbare beveiliging voor gedeelde bestandsstorage zonder dat dit de systeemprestaties nadelig beïnvloedt.

VOORDELEN

KRACHTIGE BESCHERMING TEGEN MALWARE

De bekroonde anti-malware-engine van Kaspersky Lab zorgt voor krachtige serverbescherming en voorkomt dat bekende en potentiële malwaredreigingen het lokale netwerk binnendringen via schadelijke of gevaarlijke programma's.

HOGE PRESTATIES EN BETROUWBAARHEID

U kunt erop vertrouwen dat Kaspersky Security for File Server uw systeem niet vertraagt of bedrijfsactiviteiten verstoort bij een zware netwerkbelasting.

ONDERSTEUNING VOOR MEERDERE PLATFORMEN

Eén effectieve beveiligingsoplossing voor heterogene servernetwerken, waarbij de nieuwste platforms en servers worden ondersteund, met inbegrip van terminal-, cluster- en virtuele servers, zonder compatibiliteitsproblemen.

KRACHTIGE FUNCTIES VOOR BEHEER EN RAPPORTAGE

Met de effectieve en gebruiksvriendelijke beheertools, informatie over de beschermingsstatus van servers, flexibele tijdsinstellingen voor scans en een uitgebreid rapportagesysteem kunt u de beveiliging van file servers op efficiënte wijze beheren en brengt u de totale eigendomskosten omlaag.

FUNCTIES

- **Realtime bescherming tegen malware** voor file servers waarop de nieuwste versies van Windows® (waaronder Windows Server® 2012/R2), Linux® en FreeBSD (beide met Samba) worden uitgevoerd.
- **Bescherming van Citrix- en Microsoft®-terminalservers.**
- **Volledige ondersteuning voor clusterservers.**
- **Schaalbaarheid** — Ondersteunt en beveiligt met gemak de meest complexe heterogene infrastructuren.
- **Betrouwbaarheid, stabiliteit en hoge fouttolerantie.**
- **Geoptimaliseerde intelligente scantechnologie** voor onder andere het on-demand scannen van essentiële systeemzones.
- **Vertrouwde zones** verhogen de beveiligingsprestaties en zorgen dat er minder bronnen nodig zijn voor het scannen.
- **In quarantaine plaatsen en back-up maken** van gegevens alvorens deze worden gedesinfecteerd of verwijderd.
- **Isolatie** van geïnfecteerde werkstations.
- **Centrale uitvoering van installatie, beheer en updates** met flexibele configuratieopties.
- **Flexibele scenario's voor afhandeling van incidenten.**
- **Uitgebreide rapporten** over de netwerkbeschermingsstatus.
- **Meldingssysteem voor applicatiestatus.**
- **Ondersteuning voor HSM-systemen** (Hierarchical Storage Management).
- **Bewezen Hyper-V- en Xen Desktop-ondersteuning.**
- **VMware Ready.**
- **Ondersteuning voor ReFS.**

Kaspersky Security for File Server wordt meegeleverd met Kaspersky Endpoint Security for Business — SELECT en ADVANCED en met Kaspersky Total Security for Business. Het is ook apart verkrijgbaar als Targeted Solution.

INFORMATIE OVER ONZE TECHNOLOGIE VOOR ENDPOINTBEHEER

Krachtige tools voor endpointbeheer, naadloze integratie met de allernieuwste anti-malware en het enige speciale whitelistlaboratorium binnen de branche helpen om uw bedrijf te beschermen tegen de dynamische dreigingen in de hedendaagse omgeving.

BESCHERMEN, AFDWINGEN, CONTROLEREN

- Vulnerabilities in vertrouwde applicaties, internet-malware en gebrek aan controle over randapparaten zijn onderdelen van het steeds complexere dreigingslandschap. De tools voor applicatie-, internet- en apparaatbeheer van Kaspersky Lab bieden u volledige controle over uw endpoints, zonder nadelige gevolgen voor de productiviteit.

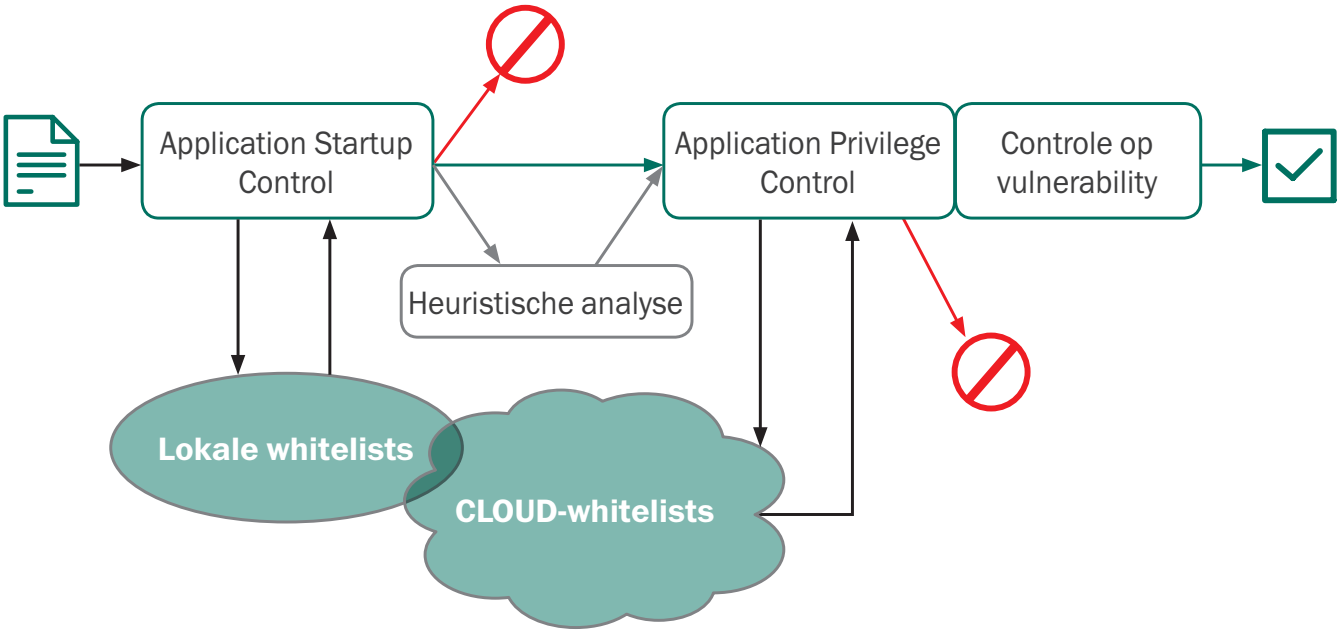
APPLICATION CONTROL EN DYNAMISCHE WHITELISTS

Bescherm systemen tegen bekende en onbekende dreigingen door beheerders volledige controle te geven over de applicaties en programma's die op endpoints mogen worden uitgevoerd, los van het gebruikersgedrag. Daarnaast kunt u de integriteit van applicaties controleren om het gedrag van applicaties te evalueren en onverwachte acties te voorkomen die het endpoint of netwerk in gevaar kunnen brengen. Eenvoudige, aanpasbare of automatische opties voor het maken en afdwingen van een beleid:

- **Application Start-Up Control**: Het starten van applicaties toestaan, blokkeren of controleren. Verhoog de productiviteit door de toegang tot niet-zakelijke applicaties te beperken.
- **Application Privilege Control**: De toegang van applicaties tot systeembronnen en gegevens reguleren en beheren. Classificeer applicaties als vertrouwd, niet-vertrouwd of beperkt. Beheer de toegang van applicaties tot gegevens met encryptie op endpoints, bijvoorbeeld informatie die via webbrowsers of Skype wordt verzonden.
- **Application Vulnerability Scanning**: Proactieve bescherming tegen aanvallen die op vulnerabilities in vertrouwde applicaties zijn gericht.

De meeste beheeroplossingen bieden alleen eenvoudige opties voor het blokkeren of verlenen van toegang. De unieke beheertools van Kaspersky Lab maken gebruik van cloudondersteunde whitelisting-databases, waardoor ze bijna in realtime over de nieuwste informatie over applicaties beschikken.

De technologieën waarmee Kaspersky Lab applicaties beheert, gebruiken cloudondersteunde whitelisting-databases om applicaties in elk stadium te analyseren en te controleren: tijdens het downloaden, installeren en uitvoeren.



Dynamische whitelists, die kunnen worden ingeschakeld met een uitgebreid 'Default Deny'-scenario, blokkeren alle applicaties die op een willekeurig werkstation worden gestart, behalve applicaties die beheerders expliciet hebben toegestaan.
Kaspersky Lab is het enige beveiligingsbedrijf met een speciaal whitelistlaboratorium met een database met meer dan 500 miljoen programma's, die non-stop wordt gecontroleerd en bijgewerkt.

'Default Deny' van Kaspersky Lab kan in een testomgeving worden toegepast, zodat beheerders de legitimiteit van applicaties kunnen testen voordat de applicaties worden geblokkeerd. Daarnaast kunnen er op basis van digitale kenmerken applicatiecategorieën worden gemaakt om te voorkomen dat gebruikers legitieme software gebruiken die door malware is aangepast of die van een verdachte bron afkomstig is.

EENVOUDIG BEHEER
Alle beheertools van Kaspersky Lab zijn in Active Directory geïntegreerd, zodat u snel en eenvoudig overkoepelende beleidsinstellingen kunt opgeven. Alle tools voor endpointbeheer zijn in één console en via één interface beschikbaar.

WEBBEHEER
U kunt de websites bewaken, filteren en beheren die eindgebruikers vanaf hun werkplek kunnen openen, Zo verhoogt u de productiviteit en bent u tegelijkertijd beschermd tegen malware en aanvallen vanaf het internet.

De geavanceerde functies voor webbeheer van Kaspersky Lab zijn gebaseerd op een lijst met websites die continu wordt bijgewerkt en is ingedeeld op categorie (zoals content voor volwassen, games, sociale netwerken of goksites). Beheerders kunnen eenvoudig een beleid instellen om het gebruik van afzonderlijke websites of bepaalde categorieën door eindgebruikers te verbieden, te beperken of te controleren. Ook kunnen ze zelf lijsten maken. Kwaadaardige websites worden automatisch geblokkeerd.

Door het gebruik te beperken, helpen de functies voor webbeheer van Kaspersky Lab om het verlies van gegevens via sociale netwerken en chatdiensten te beperken. Met flexibele beleidsregels kunnen beheerders instellen dat er alleen op bepaalde tijden op internet gesurfd kan worden. Dankzij de integratie met Active Directory kunnen beleidsregels snel en eenvoudig in de gehele organisatie worden toegepast.

Voor extra veiligheid worden de functies voor webbeheer van Kaspersky Lab direct bij het endpoint geactiveerd, wat betekent dat het beleid ook wordt afgedwongen als een gebruiker zich buiten het netwerk bevindt.

APPARAATBEHEER
Met het uitschakelen van een USB-poort zijn problemen met verwisselbare apparaten niet altijd opgelost. Een uitgeschakelde USB-poort kan bijvoorbeeld gevolgen hebben voor andere beveiligingsmaatregelen, zoals op tokens gebaseerde VPN-toegang.

Het apparaatbeheer van Kaspersky Lab ondersteunt een gedetailleerder beheer op bus-, type- en apparaatniveau, waardoor de productiviteit van de eindgebruikers behouden blijft terwijl de beveiliging wordt geoptimaliseerd. De beheerfuncties kunnen zelfs worden toegepast op het specifieke serienummer van het apparaat.

- Machtigingen voor verbinden/lezen/schrijven en een tijdschema voor apparaten instellen.
- Apparaatbeheerregels baseren op masks, waardoor geen fysieke verbinding nodig is om apparaten op de whitelist te zetten. Verschillende apparaten tegelijk op whitelists zetten.
- Gegevensuitwisseling via verwisselbare apparaten binnen en buiten de organisatie beheren, waardoor het risico op gegevensverlies of -diefstal afneemt.
- Integratie met encryptietechnologieën van Kaspersky Lab om een encryptiebeleid af te dwingen op bepaalde soorten apparaten.

Technologie voor endpointbeheer wordt meegeleverd met Kaspersky Endpoint Security for Business – SELECT en ADVANCED en met Kaspersky Total Security for Business.

KASPERSKY SECURITY FOR MOBILE

Mobiele apparaten vormen een steeds aantrekkelijker doelwit voor cybercriminelen. Tegelijkertijd maakt 'Bring Your Own Device' (BYOD) de mix van apparaten steeds ingewikkelder en wordt het lastiger voor IT-beheerders om alles te beheren en te besturen.

Kaspersky Security for Mobile zorgt ervoor dat uw apparaat veilig is, ongeacht waar het zich bevindt. Bescherm uzelf tegen steeds geavanceerdere mobiele malware. Krijg snel en gemakkelijk inzicht in en controle over de smartphones en tablets in uw omgeving, vanaf één centrale locatie en met minimale verstoring.

BELANGRIJKSTE PRODUCTKENMERKEN

- Krachtige anti-malware
- Anti-phishing en anti-spam
- Webbeveiliging
- Application Control
- Detectie van rooting/jailbreak
- Plaatsing in containers
- Diefstalbescherming
- Mobile Device Management
- Self Service Portal
- Gecentraliseerd beheer
- Webconsole
- Ondersteunde platformen:
  - Android™
  - iOS
  - Windows® Phone

VOORDELEN

GEAVANCEERDE ANTI-MALWARE VOOR MOBIELE APPARATEN EN GEGEVENSBEVEILIGING

Alleen al in 2014 verwerkte Kaspersky Lab bijna 1,4 miljoen unieke aanvallen van mobiele malware. Kaspersky Security for Mobile combineert anti-malware met diepe beveiligingslagen om gegevens op mobiele apparaten te beschermen tegen bekende en onbekende dreigingen.

MOBILE DEVICE MANAGEMENT (MDM)

De integratie met alle toonaangevende platformen voor het beheer van mobiele apparaten maakt implementatie en beheer via OTA (Over The Air) mogelijk, zodat Android-, iOS- en Windows Phone-apparaten gemakkelijker gebruikt en beheerd kunnen worden.

MOBILE APPLICATION MANAGEMENT (MAM)

Ter ondersteuning van BYOD-initiatieven kunnen zakelijke en persoonlijke gegevens op hetzelfde apparaat gescheiden worden gehouden door plaatsing in containers en selectieve wismogelijkheden. In combinatie met onze encryptiefunctionaliteit en anti-malware is Kaspersky Security for Mobile een proactieve mobiele beschermingsoplossing, die meer doet dan alleen het apparaat en de gegevens erop isoleren.

GECENTRALISEERD BEHEER

U kunt verschillende platformen en apparaten via dezelfde console als andere endpoints beheren, en zo uw inzicht en controle verhogen zonder extra moeite of aanvullende technologieën.

FUNCTIES VOOR BEVEILIGING EN BEHEER VAN MOBIELE APPARATEN

KRACHTIGE ANTI-MALWARE

Definitiegebaseerde proactieve en cloudondersteunde bescherming (via Kaspersky Security Network — KSN) tegen bekende en onbekende mobiele malwaredreigingen. Handmatige en geplande scans met automatische updates combineren voor een betere bescherming.

ANTI-PHISHING EN ANTI-SPAM

Krachtige anti-phishing- en anti-spamtechnologieën beschermen apparaten en de gegevens erop tegen phishingaanvallen en filteren ongewenste oproepen en sms-berichten.

WEBBEHEER/VEILIGE BROWSER
Deze technologieën, die worden ondersteund door Kaspersky Security Network (KSN), blokkeren in realtime de toegang tot kwaadaardige en ongeautoriseerde websites. Een veilige browser levert voortdurend de nieuwste reputatieanalyses en maakt mobiel surfen veilig.

APPLICATION CONTROL
Functies voor applicatiebeheer, geïntegreerd met KSN, zorgen ervoor dat alleen toegestane software kan worden gebruikt en maken het gebruik van 'grijze' of ongeautoriseerde software onmogelijk. Maakt het gebruik van het apparaat afhankelijk van de installatie van vereiste applicaties. Met Application Inactivity Control kunnen beheerders ervoor zorgen dat een gebruiker zich opnieuw moet aanmelden wanneer een applicatie gedurende een bepaalde tijd niet is gebruikt. Hierdoor zijn gegevens ook beschermd als een applicatie is geopend wanneer iemand het apparaat kwijtraakt of als het wordt gestolen.

DETECTIE VAN ROOTING/ JAILBREAK
Na de automatische detectie en melding van rooting of een jailbreak kan de toegang tot containers automatisch worden geblokkeerd en kan het apparaat selectief of volledig worden gewist.

PLAATSING IN CONTAINERS
U kunt zakelijke en persoonlijke gegevens van elkaar scheiden door applicaties in containers te plaatsen. Een aanvullend beleid, zoals encryptie, kan worden gebruikt om gevoelige gegevens te beschermen. Als een werknemer vertrekt, kunt u met selectief wissen gegevens in een container op het apparaat wissen, zonder gevolgen voor de persoonlijke gegevens van deze werknemer.

DIEFSTALBESCHERMING
In geval van verlies of diefstal kunt u anti-diefstalfuncties op afstand uitvoeren, zoals wissen, apparaatvergrendeling, traceren, SIM Watch, Mugshot en apparaatdetectie via een alarm. Afhankelijk van de situatie kunnen de anti-diefstalopdrachten zeer flexibel worden toegepast. Bij de integratie met Google Cloud Messaging (GCM) beschikt u bijvoorbeeld bijna direct over deze opdrachten, zodat u sneller kunt reageren en beter beveiligd bent. Als de opdrachten via de Self-Service Portal worden verzonden, hoeft er geen beheerder aan te pas te komen.

MOBILE DEVICE MANAGEMENT (MDM)
Ondersteuning voor Microsoft® Exchange ActiveSync, Apple MDM en Samsung KNOX 2.0 – Maakt het gebruik van talloze beleidsregels mogelijk, via één uniforme interface en onafhankelijk van het platform. U kunt bijvoorbeeld het gebruik van encryptie en wachtwoorden afdwingen, het gebruik van de camera beperken, een beleid op gebruikers- of groepsniveau afdwingen, APN/VPN-instellingen beheren, enz.

SELF SERVICE PORTAL
Delegeer routinebeveiligingsbeheer aan werknemers en maak eigen registratie van goedgekeurde apparaten mogelijk. Bij de inschakeling van nieuwe apparaten kunnen alle vereiste certificaten automatisch via de portal worden geleverd, zonder dat er een beheerder aan te pas komt. In geval van verlies van een apparaat kan de werknemer alle beschikbare anti-diefstalbewerkingen zelf uitvoeren via de portal.

GECENTRALISEERD BEHEER
Beheer alle mobiele apparaten centraal, vanaf één console, waarmee u ook de IT-beveiliging van alle andere endpoints beheert. Via een webconsole kunnen beheerders apparaten op afstand besturen en beheren vanaf elke computer.

Kaspersky Security for Mobile wordt meegeleverd met Kaspersky Endpoint Security for Business — SELECT en ADVANCED en met Kaspersky Total Security for Business. Het is ook apart verkrijgbaar als Targeted Solution.

ONZE ENCRYPTIETECHNOLOGIE

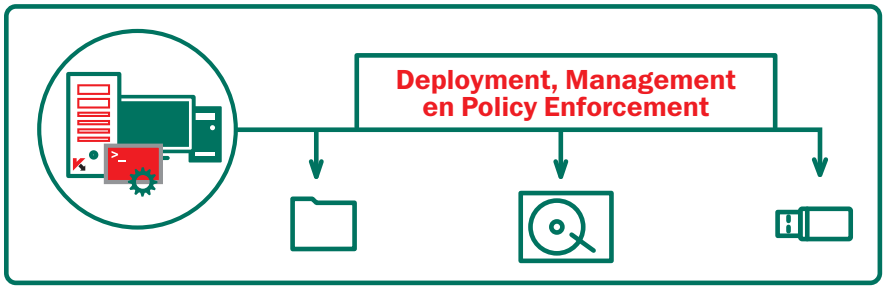
Voorkom ongeautoriseerde gegevenstoegang na verlies of diefstal van een apparaat of na gegevensdiefstal via malware.

Proactieve gegevensbeveiliging en naleving van de regelgeving is wereldwijd een must. De encryptietechnologie van Kaspersky Lab beschermt waardevolle gegevens bij verlies of diefstal van apparaten en gerichte malwareaanvallen. Ons geïntegreerde platform, dat een krachtige encryptietechnologie combineert met de toonaangevende technologieën voor endpointbeveiling van Kaspersky Lab, beschermt inactieve gegevens en gegevens die in gebruik zijn.

Omdat het een product van Kaspersky Lab betreft, is het eenvoudig te implementeren en te beheren via een gecentraliseerde beheerconsole en één beleid.

Voorkom gegevensverlies en ongeautoriseerde gegevenstoegang met de encryptietechnologie van Kaspersky Lab:

- **Encryptie van volledige schijf (FDE)**
- **Op bestands-/mapniveau (FLE)**
- **Verwisselbare en interne apparaten**



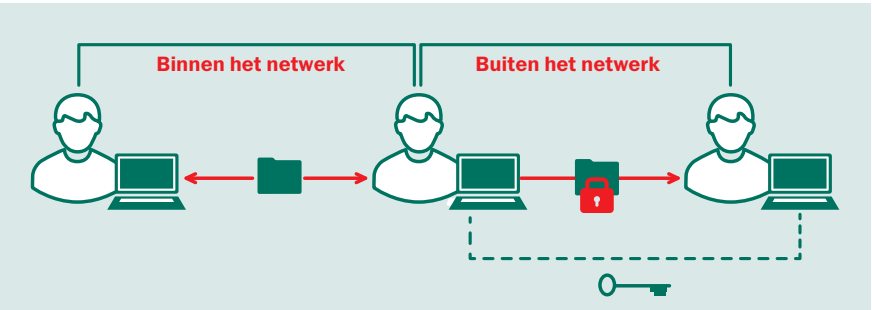
BEHEERD VIA ÉÉN BEHEERCONSOLE

VEILIGE CRYPTOGRAFIE OP BASIS VAN INDUSTRIESTANDAARD
Kaspersky Lab gebruikt Advanced Encryption Standard (AES) met een sleutellengte van 256 bits, met vereenvoudigd sleutelbeheer en opslag bij derden. Ondersteunt Intel® AES-NI-technologie, UEFI- en GPT-platformen.

VOLLEDIGE FLEXIBILITEIT
Kaspersky Lab biedt encryptie op bestands- en mapniveau (File and Folder Level Encryption of FLE) en volledige schijf-encryptie (Full Disk Encryption of FDE) voor alle mogelijke gebruiksscenario's. U kunt gegevens op harde schijven en op verwisselbare apparaten beschermen. De 'Draagbare modus' maakt het mogelijk om gegevens op verwisselbare media met encryptie te gebruiken en te verplaatsen, zelfs op computers waarop geen encryptie-software is geïnstalleerd. Dit maakt de veilige uitwisseling van gegevens buiten de eigen omgeving een stuk eenvoudiger.

SINGLE-SIGN-ON, TRANSPARANTIE VOOR DE EINDGEBRUIKER
De encryptietechnologie van Kaspersky Lab werkt transparant in alle applicaties, zonder nadelige gevolgen voor de productiviteit van eindgebruikers. Single-Sign-On zorgt voor een naadloze encryptie, waarbij de eindgebruiker mogelijk niet eens merkt dat de technologie wordt gebruikt.

Bij encryptie met Kaspersky Lab is de bestandsoverdracht tussen gebruikers binnen en buiten het netwerk naadloos en transparant.



ENCRYPTIEFUNCTIES

NAADLOZE INTEGRATIE MET BEVEILIGINGSTECHNOLOGIEËN VAN KASPERSKY LAB

Volledige integratie met anti-malware, endpointbeheer en beheertechnologieën van Kaspersky Lab voor een meerlaagse beveiliging met een gemeenschappelijke codebasis. Met één beleid kunt u bijvoorbeeld encryptie op bepaalde verwisselbare apparaten afdwingen. U kunt encryptie-instellingen op het endpoint toepassen onder hetzelfde beleid als anti-malware, apparaatbeheer en alle andere onderdelen voor endpointbeveiliging. Zo hebt u niet langer verschillende oplossingen nodig. De compatibiliteit van netwerkhardware wordt automatisch gecontroleerd voordat de encryptie wordt uitgevoerd en UEFI- en GPT-platformen worden standaard ondersteund.

ROLE-BASED ACCESS CONTROL

In grotere organisaties kunt u het encryptiebeheer met een RBAC-functie (Role-Based Access Control) delegeren. Encryptiebeheer wordt hierdoor minder ingewikkeld.

PRE-BOOT AUTHENTICATION (PBA)

Nog voordat het besturingssysteem wordt opgestart moeten er aanmeldgegevens worden ingevoerd voor extra beveiliging, met Single-Sign-On-optie. De PBA-encryptietechnologie van Kaspersky Lab is ook beschikbaar voor non-QWERTY-toetsenborden.

VERIFICATIE MET SMARTCARD EN TOKEN

Ondersteunt dubbele verificatie met bekende smartcards en tokens. Gebruikersnamen en wachtwoorden zijn hierdoor niet meer nodig, wat de gebruikerservaring ten goede komt.

HERSTEL BIJ NOODGEVALLEN

Beheerders kunnen gegevens decoderen in het geval van hardware- of softwarefouten. Herstel van gebruikerswachtwoorden voor PBA of gegevenstoegang met encryptie vindt plaats via een eenvoudig vraag- en antwoordmechanisme.

GEOPTIMALISEERDE IMPLEMENTATIE, AANPASBARE INSTELLINGEN

De encryptiefunctionaliteit van Kaspersky Lab is alleen ingeschakeld op de niveaus 'Advanced' en 'Total' van Kaspersky Endpoint Security for Business. U hoeft deze functionaliteit dus niet apart te installeren. De encryptie-instellingen zijn vooraf gedefinieerd (maar kunnen worden aangepast) voor gemeenschappelijke mappen zoals Mijn documenten, het bureaublad, nieuwe mappen, bestandsextensies en groepen, zoals Microsoft® Office-documenten of archieven van berichten.

Encryptietechnologie wordt meegeleverd met Kaspersky Endpoint Security for Business — ADVANCED en met Kaspersky Total Security for Business.

KASPERSKY SYSTEMS MANAGEMENT

Verbeter de beveiliging en beperk de complexiteit met gecentraliseerde IT-beheertools.

Niet-gepatchte vulnerabilities in populaire applicaties behoren tot de grootste gevaren voor de IT-beveiliging van bedrijven. Het risico wordt vergroot door de toenemende IT-complexiteit — als u niet weet wat u hebt, hoe kunt u het dan beveiligen?

Door het centraliseren en automatiseren van belangrijke taken voor beveiliging, configuratie en beheer, zoals vulnerabilitybeoordeling, patch- en update-distributie, inventarisatiebeheer en het uitrollen van applicaties, besparen IT-beheerders niet alleen tijd, maar wordt ook de beveiliging geoptimaliseerd.

Kaspersky Systems Management helpt om de IT-beveiligingsrisico's te beperken en om met de complexiteit van IT om te gaan. Het geeft beheerders via één scherm een volledig overzicht van en realtime controle over verschillende apparaten, applicaties en gebruikers.

BELANGRIJKSTE PRODUCTKENMERKEN

- **Vulnerabilitybeoordeling en Patch Management**
- **Hardware- en software-inventarisatie**
- **Software-installatie en probleemoplossing op afstand, bijvoorbeeld voor externe vestigingen**
- **Implementatie van besturingssystemen**
- **SIEM-integratie**
- **Role-Based Access Control**
- **Gecentraliseerd beheer**

DE BEVEILIGING VERBETEREN

Verbeter de IT-beveiliging en verminder de belasting van routinetaken met tijdige en geautomatiseerde patches en updates. Automatische vulnerabilitydetectie en -prioritering vergroten de efficiëntie en verminderen de werkdruk. Uit onafhankelijke tests[1] blijkt dat Kaspersky Lab de meest uitgebreide geautomatiseerde patch- en updatedekking biedt in de kortste tijd.

CONTROLE MET COMPLEET INZICHT

Met een totaaloverzicht van het netwerk via één console hoeven beheerders nooit meer iets te raden en is altijd duidelijk welke applicaties en apparaten (met inbegrip van gastapparaten) het netwerk betreden. Dit stimuleert gecentraliseerd beheer van gebruikers- en apparaattoegang tot bedrijfsgegevens en softwareapplicaties in overeenstemming met de IT-beleidsregels.

CENTRAAL BEHEREN

Systems Management van Kaspersky Lab is een beheerde component van het Kaspersky Security Center. Alle functies kunnen vanuit deze centrale console worden beheerd via logische, intuïtieve opdrachten en interfaces voor de automatisering van routinetaken voor IT-beheer.

FUNCTIES

VULNERABILITYBEOORDELING EN PATCHMANAGEMENT

Met geautomatiseerde softwarescans worden vulnerabilities snel gedetecteerd, geprioriteerd en verholpen. Patches en updates kunnen automatisch en razendsnel worden geleverd[2]. Dit geldt voor Microsoft®- en non-Microsoft-software. De beheerder krijgt bericht over de status van de patchinstallatie. Niet-kritieke fixes kunnen via Wake-on-LAN worden uitgesteld tot na werktijd, zelfs als de computers uitgeschakeld zijn. Met Multicast-technologie

1, 2 Test van patchbeheersystemen in opdracht van Kaspersky Lab en uitgevoerd door AV-TEST GmbH (juli 2013)

kunnen patches en updates lokaal naar externe vestigingen worden gedistribueerd, zodat er minder bandbreedte nodig is.

HARDWARE- EN SOFTWARE-INVENTARISATIE
De automatische detectie, inventarisatie, melding en controle van hardware en software, inclusief verwisselbare apparaten, geeft beheerders een gedetailleerd inzicht in de apparaten en middelen die in het bedrijfsnetwerk worden gebruikt. Gastapparaten kunnen worden gedetecteerd en kunnen internettoegang krijgen. Licentiebeheer biedt inzicht in het aantal nodes en de vervaldatum ervan.

FLEXIBELE PROVISIONING VAN BESTURINGSSYSTEEM EN APPLICATIES
Gecentraliseerde installatie van optimaal beveiligde systeemimages, met eenvoudige functies voor aanmaken, opslag en klonen. Installatie buiten werktijd via Wake-on-LAN, met wijzigingen na de installatie voor meer flexibiliteit. UEFI-ondersteuning.

SOFTWAREDISTRIBUTIE
Op afstand installeren/bijwerken, via één console. Er kunnen automatisch meer dan 100 populaire applicaties worden geïnstalleerd (geïdentificeerd via Kaspersky Security Network), desgewenst buiten werktijd. Volledige ondersteuning voor probleemoplossing op afstand, met verbeterde beveiliging door middel van gebruikersrechten en sessielogboeken/-audits. Verminder het verkeer naar externe vestigingen met Multicast-technologie voor lokale softwaredistributie.

SIEM-INTEGRATIE
Direct rapporteren en events overzetten naar bekende SIEM-systemen — IBM® QRadar en HP ArcSight. Logboeken en andere beveiligingsgerelateerde gegevens voor analyse verzamelen om de werkdruk van beheerders en tools te verminderen en de rapportage op enterpriseniveau te vereenvoudigen.

ROLE-BASED ACCESS CONTROL
Beheerrollen en -verantwoordelijkheden toewijzen in complexe netwerken. De consoleweergave kan worden afgestemd op rol en rechten.

GECENTRALISEERD BEHEER
Eén geïntegreerde beheerconsole, het Kaspersky Security Center, ondersteunt het beheer van de systeembeveiliging voor alle desktops, mobiele apparaten en virtuele endpoints in het netwerk via één interface.

Kaspersky Systems Management wordt meegeleverd met Kaspersky Endpoint Security for Business — ADVANCED en met Kaspersky Total Security for Business, en is ook apart verkrijgbaar als Targeted Solution.

KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server levert uitmuntende bescherming voor al het verkeer dat uw mailservers passeert. U bent optimaal beschermd tegen spam, phishing en zowel eenvoudige als geavanceerde malwaredreigingen, zelfs in de meest complexe heterogene infrastructuren.

Ook Microsoft® Exchange-serveromgevingen zijn beschermd tegen het verlies van vertrouwelijke gegevens via e-mails en bijlagen.

VOORDELEN

BESCHERMING TEGEN MALWAREDREIGINGEN

De krachtige malwarebescherming wordt verschaft door de bekroonde anti-malware-engine van Kaspersky, met realtime ondersteuning door het cloudondersteunde Kaspersky Security Network, dat ook proactief bescherming biedt tegen misbruik van beveiligingslekken en schadelijke URL's.

BESCHERMING TEGEN SPAM

De cloudondersteunde anti-spam-engine van Kaspersky Lab blokkeert 99,96% van alle tijd en bronnen verspillende spamberichten die worden verzonden naar mailservers die op Microsoft Exchange of Linux® zijn gebaseerd, met een minimum aan false positives.

BESCHERMING TEGEN GEGEVENSVERLIES EN BEHEER (MICROSOFT EXCHANGE-SERVERS)*

Door het identificeren van ingevoegde zakelijke, financiële, persoonlijke en andere gevoelige gegevens in uitgaande e-mails en bijlagen op Microsoft Exchange-servers en door de stroom van deze informatie te beheren, beschermt Kaspersky Security for Mail Servers de vertrouwelijke gegevens van u en uw werknemers in overeenstemming met wetgeving betreffende gegevensbescherming. Aan de hand van geavanceerde analytische technieken, zoals gestructureerd zoeken in gegevens en bedrijfsspecifieke woordenlijsten worden verdachte e-mails geïdentificeerd en eventueel geblokkeerd. Het systeem kan zelfs de lijnmanager van de afzender waarschuwen bij een potentiële inbreuk op de gegevensbeveiliging.

EENVOUDIG, FLEXIBEL BEHEER

Gebruikersvriendelijke beheer- en rapportagetools en flexibele scaninstellingen bieden efficiënte controle over de beveiliging van uw mail en documenten en helpen u de totale eigendomskosten omlaag te brengen.

FUNCTIES

- Realtime bescherming tegen malware ondersteund door het cloudondersteunde Kaspersky Security Network.
- Directe bescherming tegen onbekende exploits en zelfs zero-day-vulnerabilities.
- Geavanceerde bescherming tegen spam — de nieuwe anti-spam-engine blokkeert meer dan 99% van het ongewenste e-mailverkeer.
- Bescherming tegen gegevenslekken (Microsoft Exchange-servers)*. Detectie van vertrouwelijke informatie in e-mails en bijlagen op basis van categorieën (zoals persoonlijke gegevens en betaalkaartgegevens), woordenlijsten en grondige analyse van gestructureerde gegevens.
- Realtime scannen van alle berichten op Microsoft® Exchange-servers op spam, met cloudondersteuning en inclusief openbare mappen, via Kaspersky Security Network.
- Geplande scans van e-mail en Lotus Domino-databases.
- Scannen van berichten, databases en andere objecten op IBM® Domino®-servers.
- Berichten filteren op basis van herkende bijlage-indeling, grootte en naam.
- Eenvoudig en gemakkelijk updateproces voor anti-malware- en anti-spamdatabase.
- Back-upopslag van gegevens voordat deze worden gedesinfecteerd of verwijderd.
- Schaalbaarheid en fouttolerantie.
- Eenvoudige installatie en flexibel geïntegreerd beheer.
- Krachtig meldingssysteem.
- Uitgebreide rapporten van netwerkbeschermingsstatus.

*Bij de aankoop van dit product is de optie om het verlies of lekken van vertrouwelijke informatie te voorkomen apart verkrijgbaar.

KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway is een anti-malwareoplossing van wereldklasse die veilige permanente internettoegang garandeert voor al uw medewerkers.

VOORDELEN

KRACHTIGE BESCHERMING BEPERKT UITVALTIJD EN VERSTORINGEN

De bekroonde anti-malware-engine van Kaspersky Lab voorkomt dat bekende en potentiële malwaredreigingen het lokale netwerk binnendringen via schadelijke of gevaarlijke programma's.

EFFICIËNTERE PRESTATIES DOOR OPTIMALISERING

Dankzij de geoptimaliseerde, intelligente scantechnologie en werklastverdeling wordt de belasting van bronnen beperkt, waardoor waardevolle bandbreedte wordt gespaard zonder dat dit gevolgen heeft voor de beveiligingsprestaties.

ONDERSTEUNING VOOR MEERDERE PLATFORMEN

Ondersteuning voor de nieuwste platformen en servers, met inbegrip van proxyservers, ideaal voor hoge volumes netwerkverkeer in een heterogene omgeving. De ondersteuning voor Microsoft® Forefront® TMG maakt beveiliging van zakelijke e-mailsystemen en webgateways mogelijk.

EENVOUDIG BEHEREN EN RAPPORTEREN

Eenvoudige en gebruikersvriendelijke beheertools, flexibele scaninstellingen en rapportagesystemen voor de beveiligingsstatus.

FUNCTIES

- **Permanente proactieve bescherming** tegen bekende en potentiële malwaredreigingen.
- **Uitmuntende malwaredetectiepercentages** gecombineerd met een zeer laag aantal 'false positives'.
- **Geoptimaliseerde intelligente scantechnologie.**
- **Realtime scannen** van HTTP-, HTTPS- en FTP-verkeer vanaf gepubliceerde servers.
- **Bescherming voor Squid**, de meest gebruikte Linux-proxyserver.
- **Handige tools** voor installatie, beheer en updates.
- **Flexibele scantools en scenario's voor afhandeling van incidenten**.
- **Verdeling van belasting** voor serverprocessors.
- **Schaalbaarheid en fouttolerantie.**
- **Uitgebreide rapportage** over de netwerkbeschermingsstatus.

SPECIFIEKE FUNCTIES VOOR MICROSOFT® FOREFRONT® TMG- EN ISA-SERVERS:

- Realtime monitoring van applicatiestatus.
- Scannen van VPN-verbindingen.
- Realtime scannen van HTTPS-verkeer (alleen TMG).
- Beveiliging van e-mailverkeer (via POP3- en SMTP-protocol).
- Opslag van back-ups (alleen TMG).

Kaspersky Security for Mail Server en Kaspersky Security for Internet Gateway worden meegeleverd met Kaspersky Total Security for Business en zijn ook apart verkrijgbaar als Targeted Solutions.

KASPERSKY SECURITY FOR COLLABORATION

Gegevensbescherming en controle voor collaboration-platforms, waaronder SharePoint-farms.

VOORDELEN

VOLLEDIGE BESCHERMING VOOR UW SHAREPOINT-PLATFORM
Het cloudondersteunde Kaspersky Security Network levert krachtige bescherming tegen nieuwe en onbekende bedreigen, terwijl de anti-phishingtechnologie bescherming biedt tegen webgebaseerde bedreigingen voor samenwerkingsgegevens.

LEKKEN VAN VERTROUWELIJKE GEGEVENS VOORKOMEN*
Kaspersky Security for Collaboration gebruikt geïnstalleerde of aangepaste woordenlijsten en gegevenscategorieën om elk document op de SharePoint-servers te controleren op gevoelige informatie, woord voor woord, zin voor zin.

COMMUNICATIEBELEIDSREGELS AFDWINGEN
Met content- en filterfuncties kunt u de regels en normen van uw communicatiebeleid handhaven, ongepaste content identificeren en blokkeren en schijfruimteverlies door het opslaan van ongepaste bestanden en bestandsindelingen voorkomen.

FUNCTIES

BESCHERMING TEGEN MALWARE
- **Scannen bij toegang** — Bestanden worden tijdens het uploaden of downloaden in realtime gescand.
- **Achtergrondscan** — Bestanden op de server worden regelmatig gecontroleerd aan de hand van de meest recente malwaredefinities.
- **Integratie met Kaspersky Security Network** — Realtime, cloudondersteunde bescherming tegen zero-day-dreigingen.

ONDERSTEUNING VAN HET COMMUNICATIEBELEID VAN UW ORGANISATIE
- **Bestandsfiltering** — Helpt bij het instellen van beleidsregels voor documentopslag en het verlagen van de belasting op opslagapparaten. De applicatie kan door het analyseren van werkelijke bestandsindelingen, ongeacht de extensienaam, voorkomen dat gebruikers verboden bestandsextensies gebruiken die het beveiligingsbeleid schenden.
- **Bescherming voor wiki's/blogs** — Beschermt alle SharePoint-opslagplaatsen, zoals wiki's en blogs.
- **Contentfilters** — Voorkomt de opslag van bestanden met ongewenste content. De content van ieder bestand wordt geanalyseerd op basis van trefwoorden. Klanten kunnen hun eigen woordenlijsten maken en als contentfilter gebruiken.

VERLIES VAN VERTROUWELIJKE GEGEVENS VOORKOMEN*
- **Documenten scannen op vertrouwelijke informatie**. De oplossing bevat modules die specifieke gegevenstypen identificeren en kunnen bevestigen dat de gegevens aan relevante standaarden voldoen, zoals persoonlijke gegevens (gedefinieerd door regelgeving zoals HIPAA of EU Directive 95/46EC) of PCI DSS-standaardgegevens (Payment Card Industry Data Security Standard). Gegevens worden gescand aan de hand van ingebouwde, regelmatig bijgewerkte thematische woordenlijsten en aangepaste woordenlijsten.
- **Zoeken op gestructureerde gegevens** — Als er in een bericht informatie wordt gevonden met een specifieke structuur, wordt het bericht beschouwd als potentieel vertrouwelijk. Op die manier hebt u controle over gevoelige gegevens zoals klantdatabases die in complexe configuraties zijn opgeslagen.

FLEXIBEL BEHEER
- **Eenvoudig beheer** — U kunt een hele serverfarm centraal beheren via één console. Een intuïtieve interface met alle veelgebruikte beheerscenario's.
- **Eén dashboard** — Een overzichtelijk dashboarddisplay zorgt voor realtime toegang tot de huidige productstatus, databaseversie en licentiestatus voor alle beschermde servers.
- **Back-up van gewijzigde bestanden** — In het geval van incidenten kunnen de originele bestanden altijd worden hersteld en gedetailleerde back-upinformatie over de gewijzigde bestanden kan helpen bij uw onderzoek.
- **Integratie met Active Directory®** — Maakt de verificatie van Active Directory-gebruikers mogelijk.

Kaspersky Security for Collaboration wordt meegeleverd met Kaspersky Total Security for Business en is ook apart verkrijgbaar als Targeted Solution.

*Bij de aankoop van dit product is de optie om het verlies of lekken van vertrouwelijke informatie te voorkomen apart verkrijgbaar.

KASPERSKY SECURITY FOR STORAGE

Hoogwaardige bescherming voor EMC, NetApp, Hitachi en IBM®-storage.

VOORDELEN

KRACHTIGE REALTIME BESCHERMING TEGEN MALWARE
Permanente proactieve bescherming voor NAS-oplossingen (Network Attached Storage). De krachtige anti-malware-engine van Kaspersky Lab scant elk bestand dat wordt geopend of bewerkt op enige vorm van malware, zoals virussen, wormen of Trojans. De geavanceerde heuristische analyse identificeert zelfs nieuwe en onbekende dreigingen.

GEOPTIMALISEERDE PRESTATIES
Hoogwaardige scanprestaties dankzij geoptimaliseerde scantechnologie en flexibele uitzonderingsinstellingen zorgen voor een maximale beveiliging en een minimale impact op de systeemprestaties.

BETROUWBAAR
Uitzonderlijke fouttolerantie wordt gerealiseerd door een eenvoudige architectuur met geïntegreerde onderdelen die ontworpen en gebouwd zijn om probleemloos samen te werken. Het resultaat is een stabiele, robuuste oplossing die, als deze geforceerd wordt afgesloten, automatisch opnieuw opstart voor betrouwbare en ononderbroken bescherming.

BEHEERGEMAK
Servers worden op afstand geïnstalleerd en zijn standaard en zonder noodzakelijke herstart beschermd. Ze worden, evenals uw andere beveiligingsoplossingen van Kaspersky, samen beheerd via één eenvoudige en intuïtieve centrale console: Kaspersky Security Center.

FUNCTIES

PERMANENTE PROACTIEVE BEVEILIGING
De toonaangevende anti-malware-engine, ontwikkeld door 's werelds grootste deskundigen op het gebied van informatieverzameling over dreigingen, voorziet in proactieve bescherming tegen nieuwe en potentiële dreigingen met intelligente technologieën voor hogere detectiepercentages.

AUTOMATISCHE UPDATES
De anti-malwaredatabases worden automatisch bijgewerkt zonder het scannen te onderbreken. Zo beschikt u over ononderbroken bescherming, terwijl de werklast voor de beheerder wordt geminimaliseerd.

EXEMPTED PROCESSES EN TRUSTED ZONES
De scanprestaties kunnen verder worden verfijnd door 'vertrouwde zones' te creëren en door aan te geven dat bepaalde bestandsindelingen en processen, zoals het maken van back-ups van gegevens , kunnen worden uitgesloten bij het scannen.

AUTORUN OBJECT SCANNING
Om het beveiligingsniveau van servers verder te verhogen, kunnen automatisch uitvoerbare bestanden en het besturingssysteem worden gescand om te voorkomen dat malware opstart bij het starten van het systeem.

FLEXIBEL SCANNEN VOOR GEOPTIMALISEERDE PRESTATIES
Verkort de scan- en configuratietijd en bevordert de werklastverdeling, hetgeen helpt de serverprestaties te optimaliseren. De beheerder kan de diepte, omvang en timing van de scanactiviteit opgeven en daarbij bepalen welke bestandstypen en zones moeten worden gescand. On-demand scans kunnen worden ingepland voor momenten met beperkte serveractiviteit.

BESCHERMT HSM- EN DAS-OPLOSSINGEN
Ondersteunt offline scanmodi voor een effectieve bescherming van HSM-systemen (Hierarchical Storage Management). Bescherming voor DAS-oplossingen (Direct Attached Storage) bevordert het gebruik van betaalbare opslagoplossingen.

ONDERSTEUNING VOOR ALLE BELANGRIJKE PROTOCOLLEN
Kaspersky Security for Storage ondersteunt de belangrijkste protocollen die door verschillende storagesystemen worden gebruikt: CAVA agent, RPC en ICAP.

BESCHERMING VAN VIRTUELE SYSTEMEN EN TERMINALSERVERS
Flexibele beveiliging omvat beveiliging voor virtuele (gast)besturingssystemen in virtuele Hyper-V- en VMware-omgevingen en voor Microsoft®- en Citrix-terminalinfrastructuren.

BEHEER

GECENTRALISEERDE INSTALLATIE EN CENTRAAL BEHEER
Installatie, configuratie en beheer op afstand, met meldingen, updates en flexibele rapportage via het intuïtieve Kaspersky Security Center. Indien gewenst is ook beheer via de opdrachtregel mogelijk.

CONTROLE OVER BEHEERDERSRECHTEN
Verschillende rechtenniveaus kunnen worden toegewezen aan serverbeheerders, waardoor compliance met specifieke bedrijfsbeleidsregels voor IT-beveiligingsbeleid kan worden gegarandeerd.

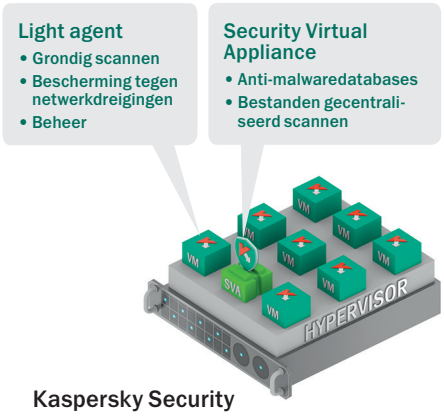
FLEXIBELE RAPPORTAGE
Rapportage kan plaatsvinden via grafische rapporten of via de gebeurtenislogboeken van Microsoft Windows® of Kaspersky Security Center. Zoek- en filtertools bieden snelle toegang tot gegevens in omvangrijke logboeken.

KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization is een flexibele oplossing die zowel bescherming als prestaties biedt voor uw omgeving.

LIGHT AGENT VOOR GEAVANCEERDE BESCHERMING

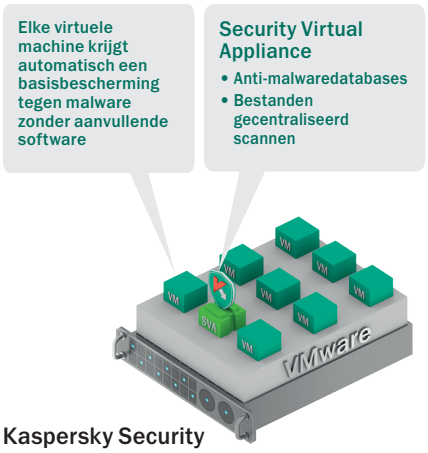
Kaspersky Security for Virtualization bevat een krachtige maar lichte agent die wordt geïmplementeerd op elke virtuele machine. Hierdoor kunnen geavanceerde beveiligingsfuncties voor endpoints worden geactiveerd. Denk hierbij aan controle op vulnerability's, Application-, Device- en Web Control, anti-virusbescherming voor chatberichten, e-mail en internet en geavanceerde heuristische voorzieningen. Het resultaat is een krachtige, meerlaagse beveiliging in combinatie met efficiënte prestaties.



Kaspersky Security for Virtualization
Light agent configuratie

OPTIONELE AGENTLESS CONFIGURATIE VOOR VMWARE-OMGEVINGEN

Nauwe integratieniveaus met VMware-technologieën betekenen dat Kaspersky Security for Virtualization ook gemakkelijk kan worden geïmplementeerd en beheerd op dit platform in een agentless beveiligingsconfiguratie. Alle beveiligingsactiviteiten zijn geconcentreerd in de Security Virtual Appliance, die communiceert met vShield voor onmiddellijke automatische bescherming van de virtuele machine en met vCloud voor netwerkbescherming.



Kaspersky Security for Virtualization
Agentless configuratie*

BELANGRIJKSTE PRODUCTKENMERKEN

- Gecentraliseerd beheer via Kaspersky Security Center
- Gecentraliseerde SVA op basis van VM-bescherming
- Geavanceerde bescherming tegen malware
- Host-based Intrusion Prevention (HIPS) en firewall
- Endpointbeheer voor applicaties, toegang tot internet en randapparatuur
- Cloudondersteunde beveiliging via Kaspersky Security Network
- Network attack blocker
- Anti-phishing
- Anti-virus voor IM, e-mail en internetverkeer
- Geen aanvullende installatie of opnieuw opstarten voor nieuwe VM's**

FLEXIBELE LICENTIES

Afhankelijk van uw wensen is Kaspersky Security for Virtualization beschikbaar met de volgende licentieopties:

- Systeemgebaseerde licentieverlening:
  - Per desktop
  - Per server
- Brongebaseerde licentieverlening:
  - Per core.

MEERDERE PLATFORMEN, ÉÉN PRIJS

Eén licentie van Kaspersky Security for Virtualization biedt ondersteuning voor virtuele omgevingen op basis van Citrix, Microsoft® en VMware.

SECURITY VIRTUAL APPLIANCE (SVA)

Kaspersky Lab biedt twee aantrekkelijke oplossingen in deze ruimte, die beide vertrouwen op een Security Virtual Appliance.

Kaspersky Lab's Security Virtual Appliance (SVA) scant alle VM's centraal in de host-omgeving. Deze architectuur biedt efficiënte VM-bescherming zonder in te leveren op endpointresources. Tegelijkertijd worden AV-scans, 'updatestormen' en 'risico's bij inschakeling' geëlimineerd en zijn de consolidatieratio's groter.

INTEGRATIE MET PLATFORMARCHITECTUUR

Kaspersky Security for Virtualization ondersteunt platformen met VMware, Microsoft® Hyper-V® en Citrix Xen, en hun belangrijkste technologieën.

VMware	Microsoft Hyper-V	Citrix Xen
High availability	Dynamic Memory	Dynamic Memory Control
vCenter-integratie	Cluster Shared Volumes	VM Protection & Recovery (VMPR)
vMotion – host-DRS	Live Backup	Xenmotion (Live Migration)
Horizon View (volledige kopieën en gekoppelde kopieën)	Live Migration	Multi-stream ICA
		Citrix Receiver
		Personal vDisk

* Geavanceerde beveiligingsfuncties zoals bestandsquarantaine, HIPS, scannen op vulnerability's en beheer van endpoints zijn niet beschikbaar in deze configuratie.

** Voor niet-persistente VM's is onmiddellijke bescherming beschikbaar nadat de light agent in de image van de VM wordt opgenomen. Voor persistente VM's moet de beheerder de light agent handmatig tijdens installatie implementeren.

KASPERSKY SECURITY INTELLIGENCE SERVICES

Als CISO of senior IT-beveiligingsmedewerker is het uw verantwoordelijkheid om uw organisatie te beschermen tegen de vele beveiligingsrisico's waarmee deze wordt geconfronteerd, zowel nu als in de toekomst. Dit vereist een niveau van strategische beveiligingskennis dat maar weinig bedrijven met interne middelen kunnen ontwikkelen.

Kaspersky Lab is een waardevolle zakelijke partner die altijd voor u klaarstaat om de meest actuele informatie over dreigingen voor uw IT-beveiliging via verschillende kanalen met uw team te delen, zodat het uw SOC/IT-beveiligingsteam aan niets ontbreekt om de organisatie tegen onlinedreigingen te beschermen.

TRAINING VOOR CYBERBEVEILIGING
Het trainingsprogramma voor cyberbeveiliging van Kaspersky Lab is speciaal ontwikkeld voor organisaties die waarde hechten aan cyberbeveiliging om hun infrastructuur en intellectuele eigendom beter te beschermen.

In het programma komt alles aan bod: van de basisbeginselen op het gebied van beveiliging tot geavanceerde digitale forensische analyse en malwareanalyse. Zo helpen we klanten hun kennis op het gebied van cyberbeveiliging op drie hoofddomeinen te vergroten:

- Fundamentele kennis van het onderwerp
- Digitale forensische analyse en afhandeling van incidenten
- Malwareanalyse en reverse engineering

INFORMATIE OVER DREIGINGEN
Kaspersky Lab verspreidt actuele feeds met informatie over dreigingen die in bestaande SIEM-systemen (Security Information & Event Management) kunnen worden geïntegreerd en die zo een extra beschermingslaag bieden.

MALWAREANALYSE, DIGITALE FORENSISCHE ANALYSE, AFHANDELING VAN INCIDENTEN
De Investigation Services van Kaspersky Lab kunnen organisaties helpen verdedigingsstrategieën te formuleren dankzij diepgravende dreigingsanalyses en adviezen over de stappen die de organisatie moet nemen om het incident op te lossen.

Er zijn drie onderzoeksniveaus:

- Malwareanalyse — biedt inzicht in de werking en doelen van specifieke malwarebestanden die worden gebruikt om uw organisatie aan te vallen.
- Digitale forensische analyse — geeft een compleet beeld van het incident en welke gevolgen dit heeft voor uw organisatie.
- Afhandeling van incidenten — een volledig onderzoek naar incidenten, waarbij de deskundigen van Kaspersky Lab ook op locatie bij de klant komen.

TRACERING VAN BOTNETDREIGINGEN
De deskundige oplossing van Kaspersky Lab traceert de botnetactiviteit en zorgt voor een snelle melding (binnen 20 minuten) van dreigingen, zodat de gebruikers van individuele onlinebetalings- en banksystemen kunnen worden gewaarschuwd. Aan de hand van deze informatie kunt u uw klanten, aanbieders van beveiligingsservices en de lokale digitale recherche adviseren en informeren over de actuele dreigingen.

INFORMATIEVERZAMELING OVER DREIGINGEN
De rapportages van Kaspersky Lab over dreigingen bevatten uiterst actuele en relevante informatie op basis van statistische informatie die is verkregen van meer dan 80 miljoen gebruikers in 200 landen. Zo wordt u bewuster van de dreigingen waaraan uw organisatie is blootgesteld en vergroot u uw kennis.

Dankzij onze kennis, ervaring en grondige informatieverzameling is Kaspersky Lab uitgegroeid tot een vertrouwde partner van vooraanstaande wetshandhavings- en overheidsinstellingen. Vanaf vandaag kan ook uw organisatie hiervan profiteren.

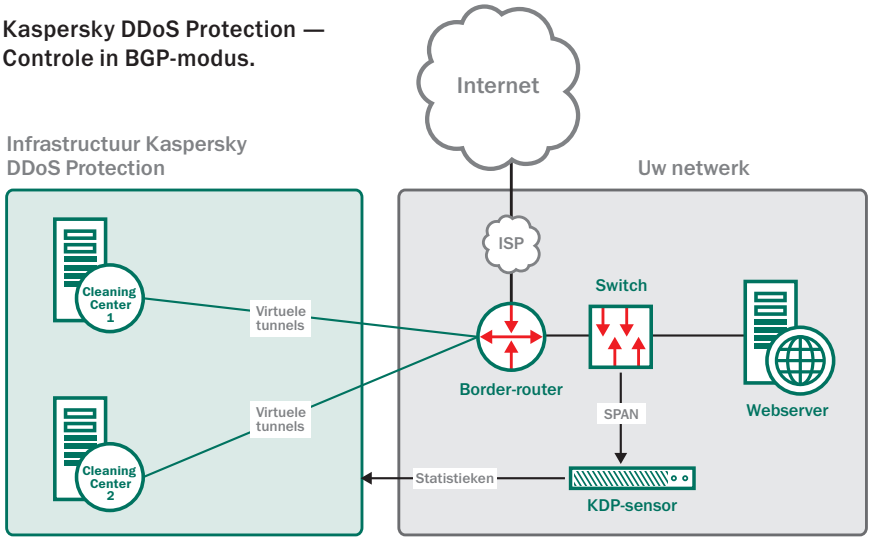
KASPERSKY ENTERPRISE SOLUTIONS

DDOS PROTECTION — VOLLEDIGE BESCHERMING EN RISICOBEPERKING

Alle noodzakelijke stappen om uw bedrijf te beschermen tegen Distributed Denial of Service-aanvallen.

Kaspersky DDoS Protection biedt alles wat uw bedrijf nodig heeft om u te beschermen tegen alle soorten DDoS-aanvallen en om de gevolgen van een dergelijke aanval tot een minimum te beperken. Dit omvat het non-stop analyseren van al uw onlineverkeer, het verzenden van waarschuwingen bij een mogelijke aanval en vervolgens het ontvangen van het omgeleide verkeer, het schoonmaken van het verkeer en het terugleiden van het 'schone' verkeer.

Kaspersky DDoS Protection — Controle in BGP-modus.



KASPERSKY FRAUD PREVENTION — VOOR BANKEN EN FINANCIËLE INSTELLINGEN

Een uitgebreid en gebruiksvriendelijk technologieplatform dat maatoplossingen kan bieden om risco's op fraude bij onlinebetalingen en mobiele betalingstransacties te beperken.

Kaspersky Fraud Prevention beschermt klanten van financiële instellingen, ongeacht het type apparaat dat ze gebruiken om toegang tot de services te krijgen (pc, laptop, smartphone of tablet). Het platform bevat ook een softwarecomponent voor de bank die malware detecteert en die automatisch abnormale gedragspatronen bij transacties van individuele klanten identificeert. Zelfs als Kaspersky Fraud Prevention for Endpoints niet is geïnstalleerd, kan de Clientless Engine frauduleuze transacties voorkomen.

BESCHERMING VAN KRITIEKE INFRASTRUCTUUR

Industriële beheersystemen en netwerken beveiligen

Kaspersky Endpoint Security for Business biedt effectieve 'industrial mode'-bescherming en bewaakt ICS/SCADA-endpoints tegen de dreigingen en vulnerabilities waarop vele criminelen zich richten die kritieke systemen als doelwit hebben.

In samenwerking met toonaangevende leveranciers van industriële automatiseringssystemen, zoals Emerson, Rockwell Automation en Siemens, heeft Kaspersky Lab allerlei gespecialiseerde procedures opgesteld om goedkeuring te verkrijgen en voor compatibiliteit met de technologieën van klanten. Zo kunnen we garanderen dat kritieke infrastructuren effectief worden beschermd, zonder gevolgen voor de operationele continuïteit en consistentie.

KASPERSKY LAB PROFESSIONAL SERVICES

Voor klanten met complexe IT-installaties zijn er de Professional Deployment and Upgrade-, Training- en Health Check-services van Kaspersky. Deze zorgen ervoor dat de Kaspersky Security for Business-oplossingen op de juiste wijze en voor optimale prestaties worden geconfigureerd, gebruikt en beheerd.

KASPERSKY SMALL OFFICE SECURITY

Praktische bescherming voor kleine bedrijven.

Voor uw unieke uitdagingen is er een unieke oplossing. Krachtige, eersteklas bescherming die u sneller en gemakkelijker dan ooit in gebruik kunt nemen.

- Speciaal ontwikkeld voor bedrijven met maximaal 25 gebruikers.
- Eenvoudig te installeren en te gebruiken.
- Webconsole voor online beheer vanaf elke plek.

PRAKTISCH
Kaspersky Small Office Security is zelfs voor niet-technische personen eenvoudig te installeren en gebruiken. De gebruiksvriendelijke wizards leiden u automatisch door verschillende processen, zoals:

- Installeren, inclusief het verwijderen van bestaande anti-malware
- Opgeven van instellingen en het definiëren van een beleid dat het beste werkt voor u en uw bedrijf
- Automatisch downloaden van deze wijzigingen naar meerdere computers tegelijkertijd

Dit gebeurt allemaal via een onlinedashboard, zodat u - of een bevoegd persoon - uw IT-beveiliging op afstand via internet kan beheren.

Kaspersky Small Office Security biedt een uitstekende beveiliging, maar werkt toch zo soepel en efficiënt op de achtergrond dat u bijna vergeet dat de software aanwezig is.

MEERDERE BESCHERMINGSLAGEN
Kaspersky Small Office Security voorziet uw pc's en Macs, servers, tablets en smartphones van meerdere beschermingslagen. Alle beveiligingstools voor uw onderneming en meer in één suite. U kunt erop vertrouwen dat Kaspersky Small Office Security uw IT-beveiliging op zich neemt, zodat u zich volledig op uw bedrijf kunt richten.

- Cloudondersteunde, realtime beveiliging tegen nieuwe en opkomende cyberdreigingen.
- Beveiliging voor Windows®- en Mac-computers, Windows-servers en mobiele apparaten met Android™.
- Bekroonde Veilig bankieren-technologie beschermt uw online financiële transacties tegen hackers en identiteitsdieven.
- Functies waarmee u het surfgedrag en gebruik van social media van uw werknemers kunt beheren.
- Encryptie ter bescherming van vertrouwelijke bedrijfs- en klantgegevens.
- Anti-phishingtechnieken om te beschermen tegen valse en schadelijke websites.
- Krachtige spamfiltering.
- Veilig wachtwoordbeheer.*
- Automatische back-ups via Dropbox tegen verlies van gegevens.

HELPT U OM GELD TE BESPAREN
Kaspersky Small Office Security beschermt u niet alleen tegen hackers die uw geld willen stelen, maar vergroot ook de productiviteit van uw werknemers. U kunt namelijk het internetgebruik van uw werknemers beheren en bepalen wanneer ze mogen surfen of berichten kunnen versturen. Dankzij geavanceerde beveiligingsvoorzieningen zoals encryptie kunnen uw klanten er zeker van zijn dat hun gegevens bij u in goede handen zijn, waardoor uw verkoopkansen en de klanttevredenheid toenemen.

* Alleen geschikt voor 32-bits applicaties. Inclusief Android- en iOS-apparaten.

KASPERSKY MAINTENANCE AND SUPPORT AGREEMENTS

Een hoogwaardige ondersteuning bij incidenten, configuratieproblemen, incompatibiliteit en andere problemen voor de IT-beveiliging is van groot belang voor organisaties die naar gemoedsrust en een optimale productiviteit streven.

De Maintenance and Support Agreements (MSA's) van Kaspersky Lab bieden garanties voor uptime en een continue zorg voor de kwaliteit van de IT-beveiligingsnetwerken van uw organisatie. Deze overeenkomsten zorgen voor een superieure ondersteuning bij onverwachte incidenten, van onjuiste configuraties tot malwarebesmettingen, en dragen zo bij aan de stabiliteit en efficiëntie van de hele organisatie.

De Maintenance and Support Agreements van Kaspersky Lab bieden dekking bij de volgende problemen:

- Onverwachte wereldwijde virusuitbraken
- Ernstige downtime vanwege complexe infrastructuur
- Implementatie-optimalisatie en aangepaste fixes
- Problemen vanwege netwerkincompatibiliteit
- Kaspersky Lab-productupgradeproces
- Onderzoek naar malware-incidenten
- Ondersteuning bij productinstallatie en configuratie*
- Implementatie van patches en andere updates*

Als uw team hulp nodig heeft, zijn de specialisten van Kaspersky Lab in lokale talen beschikbaar via speciale voorrangstelefoonnummers, met een reactietijd die op de behoeften van uw organisatie is afgestemd. De onderstaande tabel bevat informatie over de beschikbare ondersteuningsopties.

	Standard Support		Extended Support	
	MSA Starter	MSA Plus	MSA Business	MSA Enterprise
Direct telefoonnummer	Ja	Ja	Ja	Ja
Technische Account Manager	Nee	Nee	Ja	Ja
Ondersteuning in lokale taal	8x5	8x5	8x5	24x7x365
Ondersteuning bij ernstniveau 1	8x5	8x5	24x7x365	24x7x365
Reactietijd bij ernstniveau 1	8 kantooruren	6 kantooruren	4 uur	30 minuten
Ondersteuning bij ernstniveau 2	8x5	8x5	8x5	24x7x365
Professioneel service-consult	Nee	Nee	Aanvullende kosten	Health Check en aangepaste rapportage
Maximum aantal incidenten	6	12	36	Onbeperkt

* Betaalde opties voor MSA Business. Niet beschikbaar voor MSA Starter en MSA Plus.

KASPERSKY LAB WORLDWIDE

Kaspersky Lab ondersteunt lokale en internationale bedrijven vanuit vestigingen over de hele wereld. Neem contact op met uw lokale reseller voor meer informatie over het aanschaffen van Kaspersky Security for Business-oplossingen.

kaspersky.com/nl

APAC

1. Australië
2. China
3. Hongkong
4. India
5. Korea
6. Maleisië

Europa

7. Oostenrijk
8. Frankrijk
9. Duitsland
10. Italië
11. Nederland
12. Portugal
13. Spanje
14. Noorwegen
15. Zwitserland
16. Verenigd Koninkrijk

Opkomende markten

17. Letland
18. Polen
19. Roemenië
20. Slovenië
21. Zuid-Afrika
22. Turkije
23. Oekraïne
24. Verenigde Arabische Emiraten

Japan

25. Japan (Tokio)

Noord-Amerika

26. Canada
27. Verenigde Staten (Boston)
28. Verenigde Staten (Miami)

Rusland en GOS

29. Rusland
30. Kazachstan


Twitter.com/
Kaspersky


https://www.facebook.com/
KasperskyLabBenelux


Youtube.com/
Kaspersky

Kaspersky Lab BV,
kaspersky.com/nl

Alles over
internetbeveiliging:
www.securelist.com

Zoek een partner bij u in de buurt:
http://www.kaspersky.com/nl/partners

Catalog_SP1/Feb15/Global

KASPERSKY lab