KASPERSKY ENDPOINT SECURITY FOR ENTERPRISE

Bescherming van de volgende generatie tegen geavanceerde bedreigingen voor uw endpoints en gebruikers

De dreigingsomgeving ontwikkelt zich ongekend snel, waardoor kritische bedrijfsprocessen, vertrouwelijke gegevens en financiële middelen een steeds groter risico lopen door zero-day-aanvallen. Om het risico voor uw organisatie te beperken moet u slimmer, beter uitgerust en beter geïnformeerd zijn dan de cyberprofessionals die u schade proberen te berokkenen.

Maar één simpel feit is waar: de meeste cyberaanvallen op zakelijke omgevingen worden uitgevoerd via endpoints. Als u elke zakelijke endpoint, statisch en mobiel, effectief kunt beveiligen, hebt u een sterke basis voor uw algehele beveiligingsstrategie.

KRACHTIGE BEVEILIGING

Elke endpoint volledig beveiligen tegen elke vorm van bekende en onbekende cyberdreiging is geen sinecure. Traditionele anti-virusbescherming is zeker niet voldoende. Alleen met een geavanceerd beveiligingsplatform en meerlaagse aanpak kunt u elk endpoint binnen en buiten uw omgeving volledig beschermen.

KRACHTIGE PRESTATIES

De bescherming van endpoints dient zo natuurlijk en vanzelfsprekend aan te voelen als ademhalen. Het unieke geïntegreerde beveiligingsplatform van Kaspersky Lab klopt voortdurend in het hart van uw IT-infrastructuur. De krachtige endpointbeveiliging vindt plaats met minimale gevolgen voor de systeemsnelheid of -bronnen. De oplossing is in-house ontwikkeld als één volledig schaalbaar geïntegreerd platform en biedt optimale prestaties zonder softwareconflicten en hiaten in de beveiliging.

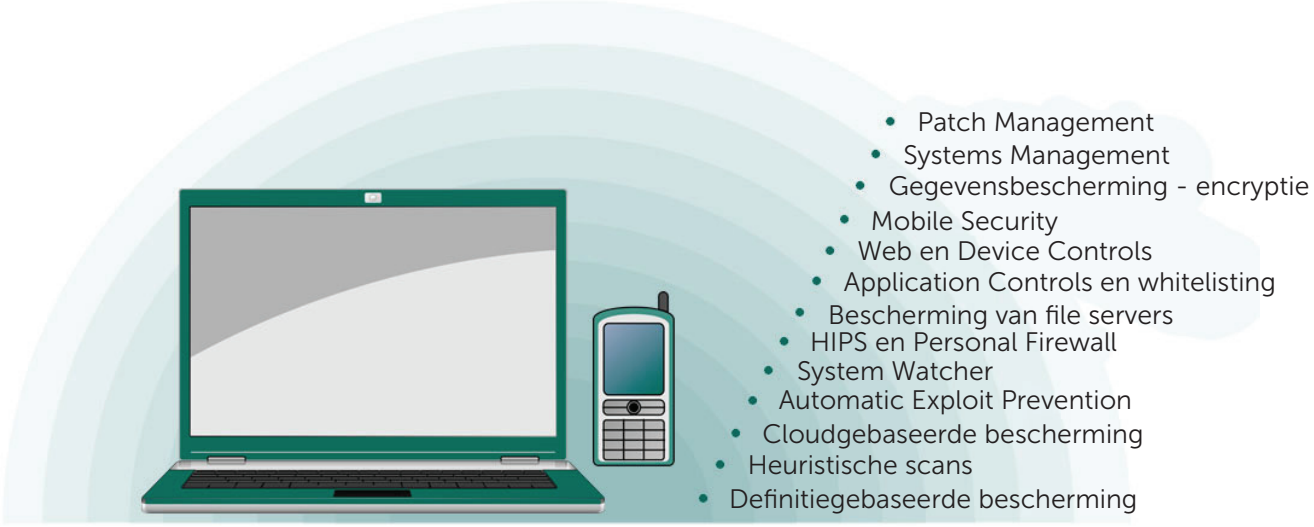
KRACHTIGE DREIGINGSINFORMATIE

Onze technologieën op basis van ongeëvenaarde bronnen voor realtime dreigingsinformatie ontwikkelen zich voortdurend om uw bedrijf zelfs tegen de nieuwste, meest geavanceerde dreigingen, waaronder zero-day-exploits, te beschermen. Door uw beveiligingsstrategie af te stemmen op de wereldleider in de geavanceerde detectie van dreigingen, kiest u voor de beste endpointbeveiliging, nu en in de toekomst. Er is geen betere beveiligingsoplossing voor uw organisatie.

GECENTRALISEERD BEHEER

Beheer meerdere platforms en apparaten vanaf dezelfde console als andere endpoints. Vergroot inzicht en controle zonder extra inspanning of beheertechnologie.

Meerlaagse beveiliging



Ongeëvenaarde dreigingspreventie en -eliminatie van de volgende generatie

De kern van uw beveiligingsstrategie - het krachtigste en meest effectieve endpointbebeveiligingssysteem in de branche, zoals telkens weer aangetoond door onafhankelijke tests[1].

Laag op laag proactieve, intelligente bescherming zorgt samen voor een krachtige en veerkrachtige beveiliging tegen de meest geavanceerde bekende en onbekende cyberdreigingen.

- Multi-algoritme **heuristische analyse**: detecteert onbekende malware ter aanvulling op traditionele **definitiegebaseerde** technologieën.
- **Cloudondersteund Kaspersky Security Network (KSN)**: faciliteert de identificatie en blokkering van nieuwe malwaredreigingen in realtime zodra ze zich voordoen.
- **Automatic Exploit Prevention**: stopt proactief zelfs de meest geavanceerde dreigingen door exploits te blokkeren die cybercriminelen gebruiken.
- **System Watcher**: blokkeert onbekende dreigingen door verdachte gedragspatronen te detecteren en herstelt belangrijke bestanden als het systeem is getroffen
- **Host-based Intrusion Prevention System (HIPS)**: beperkt activiteiten en kent rechten toe overeenkomstig het vertrouwensniveau van de software
- **Personal firewall**: beperkt netwerkactiviteit
- **Network Attack Blocker**: stopt netwerkgebaseerde aanvallen
- **File servers**: worden ook volledig beschermd

Elk endpoint onder uw controle

Minimaliseer risico's bij de endpoints en verhoog tegelijkertijd de productiviteit. Beheer de toegang van elk endpoint tot applicaties, websites en plug-ins: identificeer en blokkeer alles dat ongepast is, reguleer toegang tot onnodige aspecten en bevorder alles dat waardevol en vertrouwd is.

Alle beheertools integreren met Active Directory, en vereenvoudigde, aanpasbare of geautomatiseerde aanmaak en handhaving van beleidsregels kunnen naar wens gecentraliseerd of op rollen gebaseerd worden.

BEPERK UW BLOOTSTELLING AAN AANVALLEN VIA APPLICATIES

Powered by **Dynamic Whitelisting, Application Control** beperkt uw blootstelling aan zero-day-aanvallen aanzienlijk door u totale controle geven over de software die mag worden uitgevoerd. Blacklisted applicaties worden geblokkeerd. Applicaties die zich verdacht of ongepast gedragen, worden gedetecteerd, geanalyseerd en vervolgens geblokkeerd of beperkt met de hulp van System Watcher en HIPS. Uw goedgekeurde en betrouwbare applicaties worden intussen probleemloos uitgevoerd.

FLEXIBELE WHITELISTING IN DE CLOUD

Van onze in-house Whitelisting Lab ondersteunt een Default Deny-scenario, dat in een testbedomgeving kan worden uitgevoerd.

DE GEVAREN VAN SURFEN OP INTERNET AANPAKKEN

Web Control bewaakt, filtert en beheert welke websites eindgebruikers vanaf hun werkplek kunnen openen. Zo verhoogt u de productiviteit en is uw systeem tegelijkertijd minder kwetsbaar voor inbreuken en infiltratie via websites en social media.

HET GEBRUIK VAN DRAAGBARE APPARATEN BEHEREN

Device Control beschermt tegen de schadelijke gevolgen van het verlies van bedrijfs- en klantgegevens op niet-goedgekeurde draagbare apparaten of apparaten zonder encryptie, en tegen het uploaden van geïnfecteerde gegevens vanaf het apparaat.

Bescherming van gegevens door geïntegreerde encryptie

Krachtige, gebruikerstransparante **encryptie** beveiligt volledig vertrouwelijke en gevoelige gegevens onderweg, op draagbare apparaten en op locatie. Geïntegreerde technologie betekent dat u de encryptie van bedrijfsgegevens centraal kunt handhaven op bestands-, schijf- apparaatniveau met eenvoudige beveiligingsbeleidsregels voor groepen endpoints of zelfs afzonderlijke apparaten.

---

1 Referentie hier – Top3.

Eliminatie van vulnerabilities door intelligente patching

Aangetroffen vulnerabilities misbruiken in een vertrouwde applicatie is een van de meest gebruikte manieren om toegang te krijgen tot IT infrastructuur via een endpoint. De tijdige, efficiënte patching van vulnerabilities prioriteren en beheren vereist een grondige kennis van exploits, hun gedragingen en hun huidige doelwitten. Het **geautomatiseerde Vulnerability Assessment- en Patch Management**-systeem van Kaspersky Lab is gebaseerd op realtime wereldwijde informatie over exploitactiviteiten en houdt kritieke patching up-to-date, zonder gevolgen voor drukke systemen en gebruikers.

Beveiliging van mobiele endpoints buiten uw omgeving

Bedrijfsgegevens zijn overal en altijd toegankelijk geworden op smartphones en tablets in uw IT-omgeving. **Beveiliging van mobiele apparaten** beschermt tegen dreigingen die specifiek gevoelige gegevens onderweg als doelwit hebben, alsook tegen pogingen om zwakke plekken in zakelijke of eigen apparaten te gebruiken als 'toegangspoort' voor infiltratie in de systemen.

Beschikbare functies

- **Krachtige meerlaagse bescherming** tegen malwaredreigingen voor alle toonaangevende mobiele platforms.
- **Anti-phishing**-technologie: blokkeert gevaarlijke links in berichten en webpagina's, terwijl oproep-/sms-filters ongewenste communicatie voorkomen
- **Application Wrapping**: zorgt voor aparte opslag in containers, encryptie en wissen van bedrijfsgegevens in apparaten van werknemers.
- **Application Control en Web Control** ondersteund door KSN, blokkeren ongeoorloofde toegang tot software en websites.
- **Anti-diefstal**: met functies zoals wipe, apparaatvergrendeling, lokaliseren, SIM Watch, 'mugshot' en 'alarm'-apparaatdetectie die ervoor zorgen dat u apparaten snel kunt uitschakelen en gevoelige gegevens kunt wissen bij verlies of diefstal van een apparaat.
- Detectie en rapportage van **jailbroken of rooted apparaat**, zodat actie mogelijk is.
- **Gecentraliseerd beheer**: inclusief mobiele apparaten en applicaties. (MDM/MAM)-functionaliteit. Beleidsregels zijn toe te passen op heterogene apparaten op alle gangbare platforms via één interface.

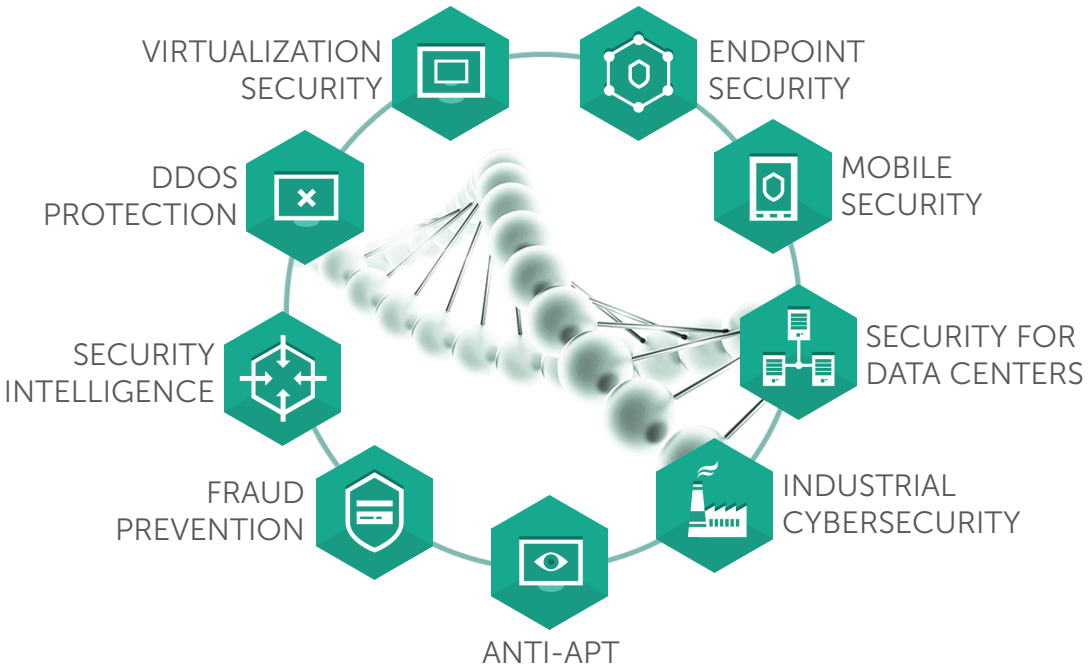
Optimale efficiëntie – geïntegreerd beheer

Kaspersky Endpoint Security for Enterprise biedt uw beveiligingsteams volledig inzicht in en volledige controle over elk endpoint, statisch of mobiel, onder uw beheer, waar het zich ook bevindt en wat het ook doet. De oplossing is vrijwel onbeperkt schaalbaar en biedt toegang tot inventarisaties, licenties, probleemoplossing op afstand en netwerkcontroles, allemaal vanaf één console - het **Kaspersky Security Center**.

Gecentraliseerd beheer via één console wordt aangevuld met rolgebaseerde beheerfunctionaliteit. Toegangsrechten en taken kunnen zo naar behoefte worden toegekend aan individuele beveiligingsprofessionals.

Het grote plaatje - Kaspersky Enterprise Security-oplossingen

Endpointbeveiliging is weliswaar essentieel, maar vormt slechts het begin. Of u nu de beste beveiligingsstrategie in zijn soort gebruikt, of uw strategie baseert op een enkele bron, Kaspersky Lab biedt **een reeks bedrijfsoplossingen** die samen (of los van elkaar) functioneren. Zo is de keuze geheel aan u terwijl de prestaties en efficiëntie behouden blijven. Oplossingen voor **virtuele** plus **fysieke systemen, servers en infrastructuren** worden aangevuld met doelgerichte oplossingen voor **specifieke brancheproblemen**, zoals financiële fraude en DDoS-aanvallen (Denial of Service), en met onze reeks **Security Intelligence Services**.



Onderhoud en support

In meer dan 200 landen wordt u vanuit 34 kantoren wereldwijd 24 uur per dag en 365 dagen per jaar geholpen op basis van onze **Maintenance Service Agreement (MSA)**-supportpakketten. Onze **Professional Services**-teams staan klaar om u optimaal te laten profiteren van uw Kaspersky Lab-beveiligingsinstallatie.

Neem voor meer informatie over de effectievere beveiliging van uw endpoints contact op met het verkoopteam van Kaspersky Lab voor bedrijven.

Kaspersky Enterprise Security for Endpoints/V 1.0/Nov 15/Global