▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS

ANTI-MALWARE

Ongeëvenaarde beveiliging

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

De toonaangevende prestaties van de anti-malware-engine van het Kaspersky Endpoint Security for Business-platform worden voortdurend bij verschillende onafhankelijke tests bevestigd. 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?

- 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.

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**, ofwel in **71% van de tests** en werden **51 keer als beste beoordeeld**, ofwel in meer dan de helft van alle tests.

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

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 softwarevulnerability's 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.

Verkoopinformatie

Anti-malware van Kaspersky Lab wordt niet afzonderlijk verkocht. Het is geactiveerd binnen alle niveaus van Kaspersky Endpoint Security for Business, en in Kaspersky Small Office Security.

TEGENMAATREGELEN TEGEN ENCRYPTIERANSOMWARE

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' – 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 elke 2 uur voorzien van updates die u tegen nieuwe malwaredreigingen beschermen. Dit gebeurt door middel van de snelste updatecyclus, naar wij menen, in de sector en continu bijgewerkte gegevens over recent ontdekte malware via de cloud van Kaspersky Security Network (KSN).

Kaspersky Endpoint Security for Business/Anti-malware/Feb 15/Global

KASPERSKY lab