KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Encryptietechnologie

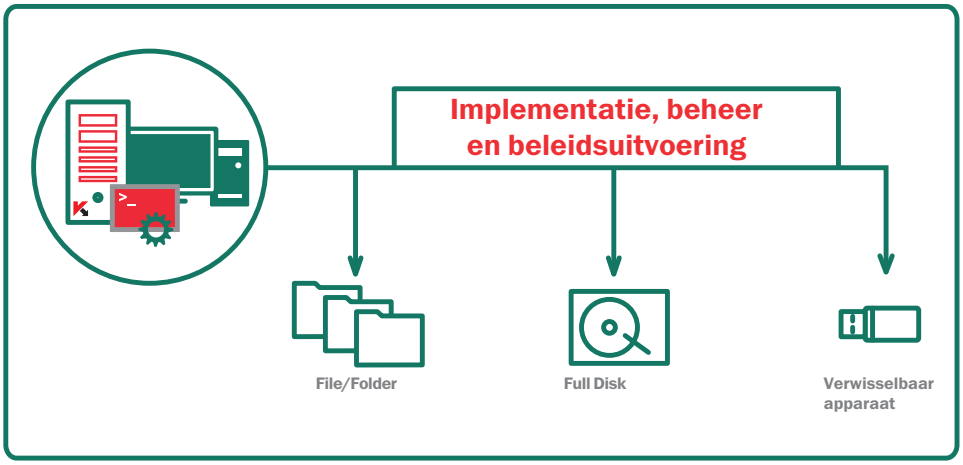
Encryptie voorkomt ongeoorloofde gegevenstoegang als een pc of medium in verkeerde handen komt.

De encryptietechnologie van Kaspersky Lab beschermt waardevolle gegevens wanneer apparaten zoekraken of worden gestolen. Bij onze oplossing wordt sterke encryptie op organische wijze geïntegreerd in de toonaangevende beschermingstechnologieën voor endpoints van Kaspersky. Omdat het een Kaspersky-product betreft, is het eenvoudig te implementeren en beheren via een gecentraliseerde beheerconsole en één beleid.

Bescherm uw gegevens eenvoudig en veilig met encryptietechnologie van Kaspersky:

- FULL DISK
- SCHIJF- EN MAPNIVEAU
- VERWISSELBARE/INTERNE APPARATEN

BEHEERD VIA ÉÉN BEHEERCONSOLE.



BEWEZEN VEILIGE CRYPTOGRAFIE

Kaspersky benut een AES-encryptiealgoritme op basis van een sleutel die een effectieve lengte van 256-bits heeft.

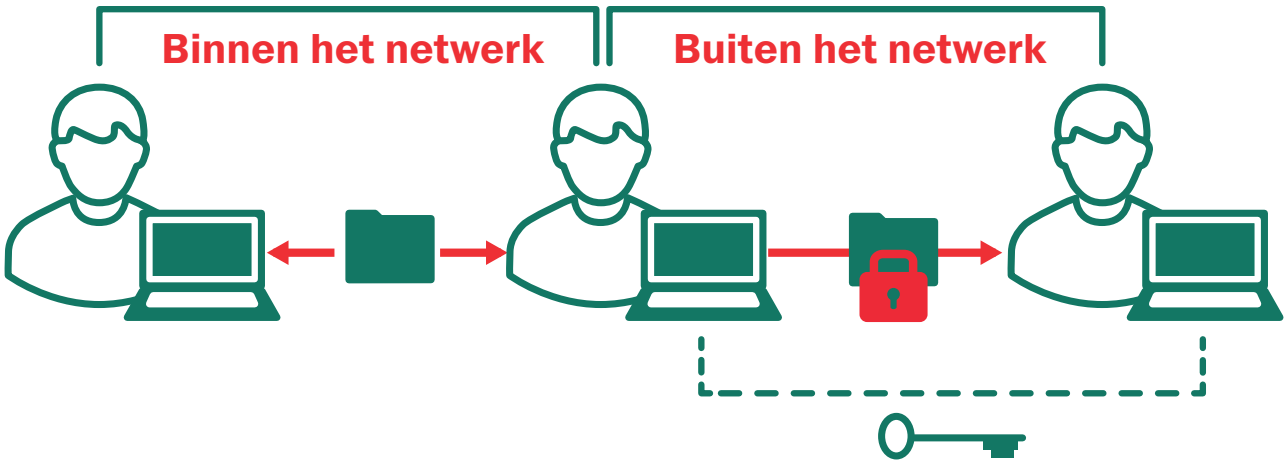
FLEXIBILITEIT BIJ DE KEUZE VAN DE ENCRYPTIEMETHODE

Met het oog op alle mogelijke gebruiksscenario's zijn alle combinaties van encryptie op bestands- en mapniveau en full disk encryptie beschikbaar voor gegevensbescherming van schijfstations en verwisselbare apparaten.

TRANSPARANTIE VOOR EINDGEBRUIKERS

De encryptietechnologie van Kaspersky Lab blijft te allen tijde transparant voor alle applicaties, ook bij het installeren. De technologie werkt direct met beveiligde informatie en verstoort de productiviteit van eindgebruikers niet. Door middel van Single-Sign-On bij het gecodeerde systeem wordt de transparantie voor de gebruiker verbeterd.

Tijdens bestandsoverdracht is de encryptie van Kaspersky Encryption naadloos en transparant voor de gebruiker binnen het netwerk. Gegevens die voor externe gebruikers zijn bedoeld, kunnen worden verpakt in speciale met een wachtwoord beveiligde containers. Het wachtwoord kan naar de ontvanger worden verzonden voor decryptie via een afzonderlijk kanaal.



ENCRYPTIEFUNCTIES:

GEÏNTEGREERDE CODEBASIS
Omdat alle functies voor meerlaagse bescherming van endpoints op één softwarecomponent zijn gebaseerd, is het niet nodig om afzonderlijke oplossingen voor bescherming tegen malware, endpointbeheer en encryptie te implementeren en te beheren.

ONDERLING VERBONDEN EN ORGANISCH GEÏNTEGREERD BELEID
Dankzij de geïntegreerde codebasis kan de beheerder afzonderlijke beleidsregels maken. Voorbeeld: de IT kan instellen dat alleen goedgekeurde verwisselbare media kunnen worden aangesloten en kan tevens een encryptiebeleid afdwingen op de betrokken apparaten (zodat beleidsregels voor Device Control en encryptietechnologieën worden gecombineerd).

AANPASBARE VOORAF GEDEFINIEERDE INSTELLINGEN
De encryptieinstellingen zijn vooraf gedefinieerd (maar kunnen worden aangepast) voor gemeenschappelijke mappen zoals Mijn documenten en het bureaublad, nieuwe mappen, bestandsextensies en groepen met bestandsextensies (bijvoorbeeld Microsoft Office-documenten, archieven van e-mailberichten).

GECENTRALISEERDE CODE VOOR NOODBEHEER
Hiermee kan de beveiligingsbeheerder gegevens op schijven decoderen in het geval van een hardware- of softwarefout.

GEBRUIKERSWACHTWOORD HERSTELLEN
Hiermee kan de gebruiker het opstartwachtwoord herstellen of toegang tot gecodeerde gegevens verkrijgen via een vraag-/antwoordmechanisme.

Verkoopinformatie

De encryptietechnologie van Kaspersky wordt niet afzonderlijk verkocht maar is beschikbaar op deze productniveaus van **Kaspersky Security for Business**:

- Endpoint Security, Advanced
- Kaspersky Total Security for Business

NIET ALLE FUNCTIES ZIJN BESCHIKBAAR OP ALLE PLATFORMEN. Ga voor meer informatie naar **www.kaspersky.nl**

KASPERSKY LAB B.V.
PAPENDORPSEWEG 79
3528 BJ UTRECHT
THE NETHERLANDS
SALES@KASPERSKY.NL
WWW.KASPERSKY.NL

KESB-ET/Version 0.1/Nov12/Global

KASPERSKY lab