



▶ **KASPERSKY
VIRKSOMHEDS-
PRODUKTER 2013**

SEE IT. CONTROL IT.

PROTECT IT.

► OM KASPERSKY LAB

Kaspersky Lab er verdens største, uafhængige sikkerhedssoftwarefirma. Vi yder den bedst mulige it-sikkerhed til din virksomhed gennem en kombination af effektiv anti-malware-beskyttelse, fleksible administrationsværktøjer, krypteringsteknologi og værktøjer til systemadministration. Kasperskys sikkerhed strækker sig fra klient til dine servere og gateways, og vores unikke, integrerede designtilgang betyder, at du kan sikre og styre alle dine fysiske, virtuelle og mobile enheder fra en enkelt, central administrationskonsol, uanset størrelsen af din infrastruktur. Kasperskys teknologi anvendes også på verdensplan i produkter og tjenester fra markedets førende it-producenter og softwarefirmaer.

Læs mere på: www.kaspersky.com.

Få alle de seneste opdateringer om antivirus, anti-spyware, anti-spam, it-sikkerhedsproblemer og tendenser på: www.securelist.com.

▶ BRANCHENS ENESTE ÆGTE, INTEGREREDE SIKKERHEDSPLATFØRM

EN ENKELT KONSOL.

Kasperskys produkter er udviklet, så administrator fra et enkelt vindue kan se og administrere hele sikkerhedsscenen - både virtuelle maskiner, fysiske og mobile enheder.

EN PLATFORM

Hos Kaspersky Lab har vi internt i virksomheden udviklet vores egen konsol, sikkerhedsmoduler og værktøjer, frem for at overtage dem fra andre selskaber. De samme programmører arbejder fra samme kodebase med at udvikle teknologier, der taler sammen og fungerer sammen. Resultatet er stabilitet, integrerede politikker, nyttige rapporter og intuitive værktøjer.

EN PRIS

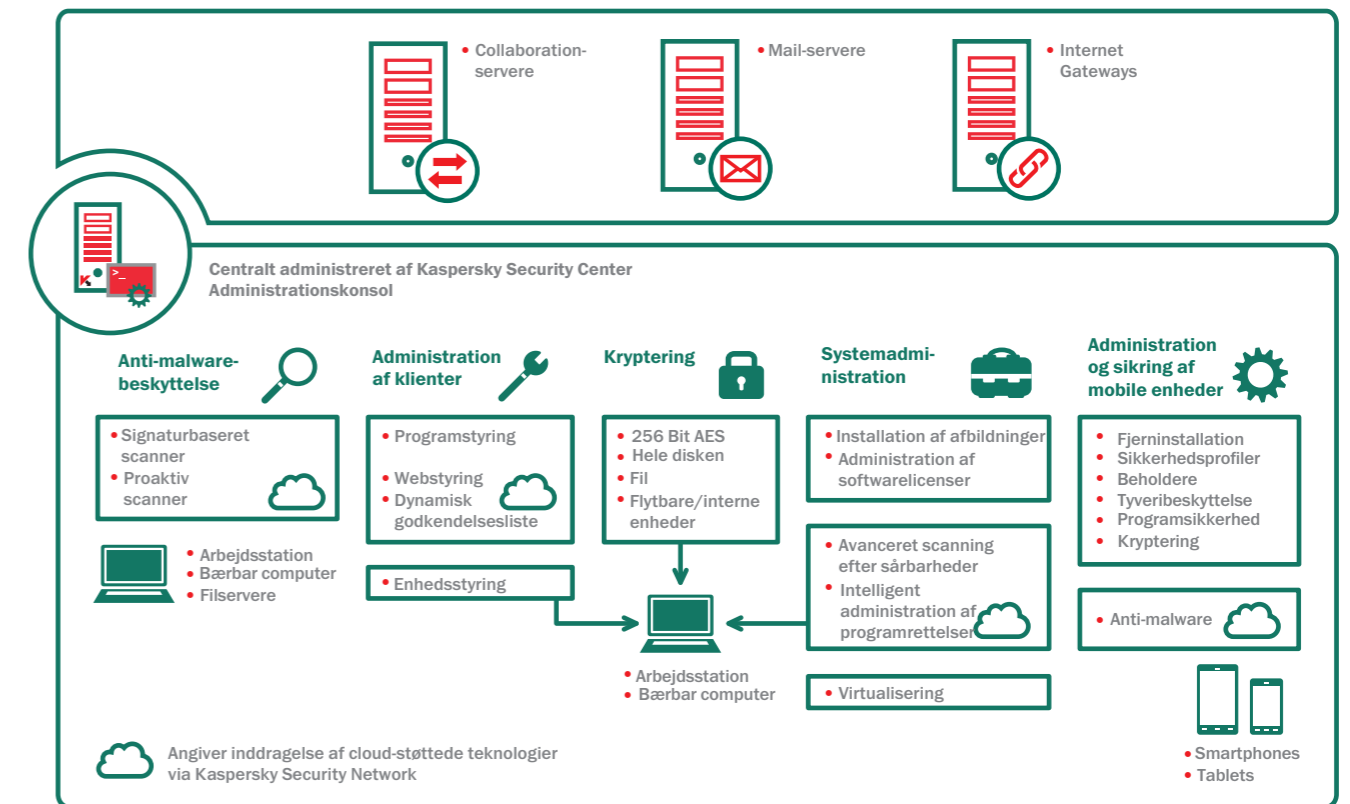
Alle Kasperskys produkter og værktøjer kommer fra én leverandør og leveres med én installation - så du ikke behøver at lave nye budgetter og argumentere for ændringer, hver gang du skal tilpasse din sikkerhed til virksomhedens mål.

▶ DEN RIGTIGE LØSNING FOR DIG

Kaspersky Security for Business leverer den rigtige løsning til din virksomhed - hvad enten du ønsker at beskytte og styre dine klienter (fra arbejdsstationer til smartphones og virtuelle maskiner) for at sikre dine servere og gateways, eller at fjernstyre hele dit sikkerhedsmiljø.

Kaspersky kan prale af en omfattende liste over teknologier, fra kryptering og administration af mobile enheder til administration af programrettelser og licensopgørelser. Alt arbejder problemfrit sammen, understøttet af det cloud-baserede Kaspersky Security Network, for at give vores kunder den førsteklasses beskyttelse, de har brug for til at bekæmpe stadig mere avancerede og forskelligartede cybertrusler.

Kort sagt, har vi leveret branchens første sikkerhedsplatform, som er bygget op fra bunden, hvilket gør det nemt for it-administratorer at se, styre og beskytte deres verden.

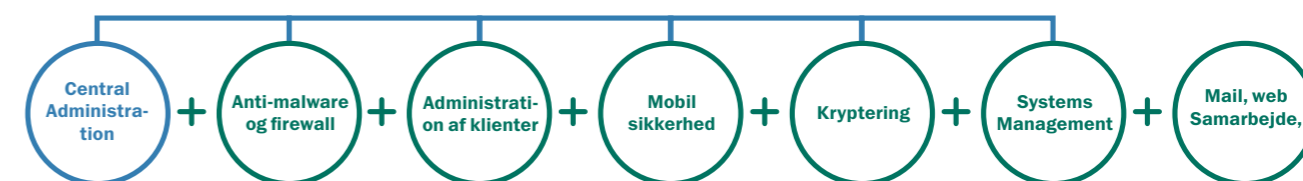


► KASPERSKY SECURITY FOR BUSINESS

Vores teknologier, og hvordan de arbejder sammen for dig

	Core	Select	Advanced	Total	Styret af Security Center	Findes i en målrettet løsning
Anti-malware	•	•	•	•	•	
Firewall	•	•	•	•	•	
Programstyring		•	•	•	•	
Enhedsstyring		•	•	•	•	
Webstyring		•	•	•	•	
Filservere		•	•	•	•	•
Agent til mobile klienter		•	•	•	•	•
Administration af mobile enheder		•	•	•	•	•
Krypteringsteknologi			•	•	•	
Administration af OS-image			•	•	•	•
Administration af licenser			•	•	•	•
Administration af sårbarheder			•	•	•	•
Administration af programrettelser			•	•	•	•
Administration af netværksadgang			•	•	•	•
Samarbejde				•		•
Mail-servere				•		•
Internet gateways				•		•
Virtualisering					•	•
Lagring					•	•

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS



CORE NIVEAU

Med udgangspunkt i Kaspersky's prisbelønnede og effektive ikke-server anti-malware-teknologi og en beskyttende firewall tilføjer vi Kaspersky Security Center - vores intuitive styringskonsol. For kunder, der kun har brug for anti-malware, er det løsningen.

SELECT NIVEAU

Ovenpå CORE-niveauet har vi tilføjet **filserver sikkerhed, godkendelse og kontrol af programmer, enhedsstyring og webstyring** til beskyttelsesopgaverne. Der er også en **enmobil beskyttelsesløsning**, som består af en **agentbaseret sikkerhedsløsning til klienterne** og **Mobile Device Management (MDM)**. Hvis dine behov omfatter beskyttelse af en mobil arbejdsstyrke og håndhævelse af it-politik, kan SELECT være det rette niveau for dig.

ADVANCED NIVEAU

På ADVANCED-niveauet tilføjer Kaspersky **dataskytselse** i form af kryptering af fil eller hele disken. Et andet, nyt tilbud, **Kaspersky Systems Management**, kombinerer sikkerhed med effektivitet. Disse brede funktioner omfatter væsentlige værktøjer, så administratoren kan:

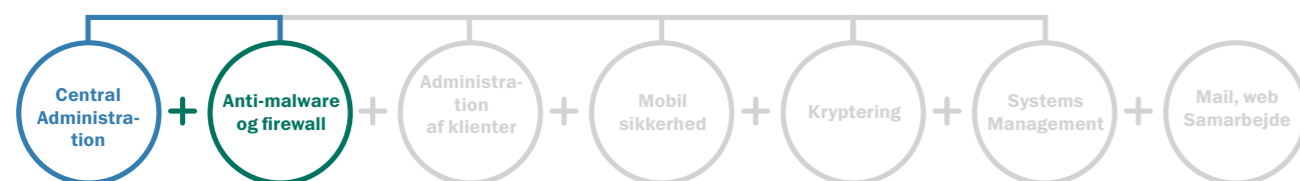
- Oprette afbildninger og installere systemer ved hjælp af modulet til afbildningsadministration.
- Prioritere behandlingen af hardware- og software-sårbarheder med en stærk kombination af avanceret scanning af sårbarheder og intelligent administration af programrettelser.
- Spore brugen af licenser og overholdelse af regler for administration af softwarelicenser.
- Oprette adgangsregler for data og infrastruktur for brugere og gæster med styring af netværksadgang.
- Installere opdateringer og nye programmer til brugere fjernt fra den centrale konsol.

KASPERSKY TOTAL SECURITY FOR BUSINESS

Vores flagskip, Kaspersky Total Security for Business, kombinerer alle tre foregående niveauer og forbedrer desuden din sikkerhed med ekstra beskyttelse af web-, mail- og samarbejdsservere. Dette er den perfekte løsning til virksomheder med omfattende sikkerhedskrav og som kræver den bedste beskyttelse af hvert netværk.

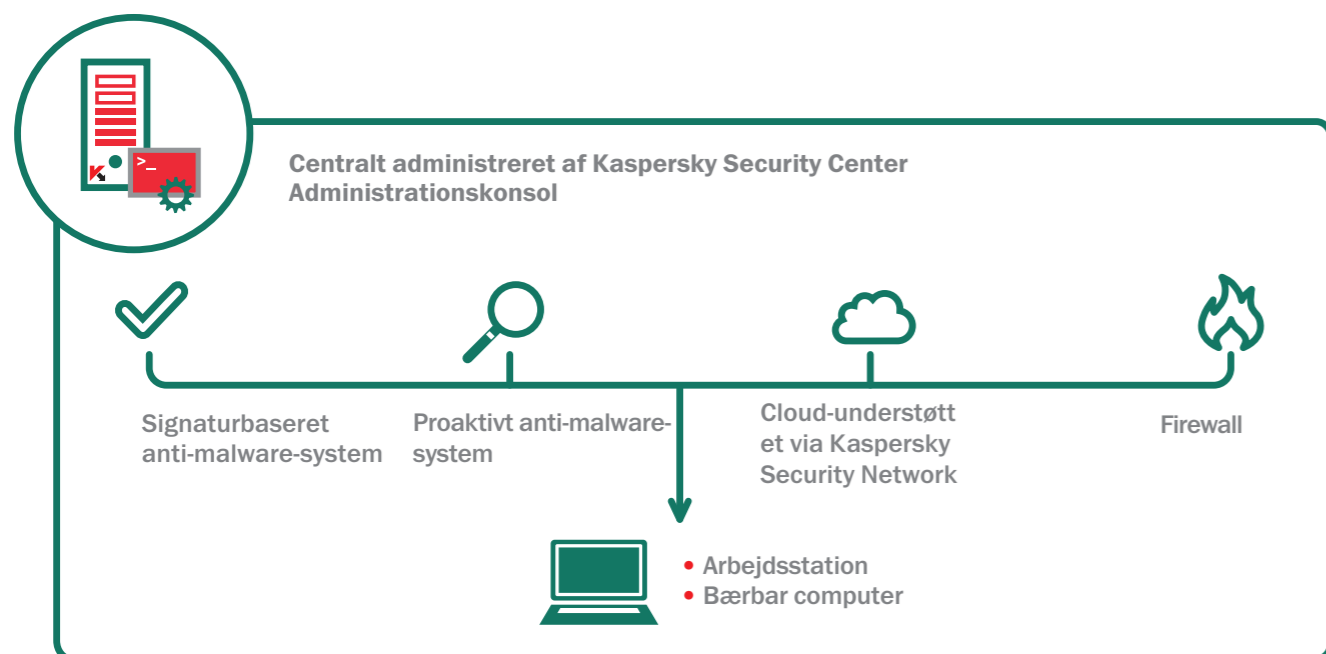
► KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Core



Prisvindende anti-malware med centraliseret installation, administration og rapportering.

En lagdelt sikkerhedsmodel begynder med klassens bedste anti-malware. Da Kaspersky længe har været kendt som førende i opdagelse og fjernelse af skadelig software, findes der ikke noget bedre fundament. Kaspersky Endpoint Security for Business Core Tier styres centralt af Kaspersky Security Center og understøttes af det cloud-baserede Kaspersky Security Network.



KasperskyEndpointSecurityforBusinessCoreTier-effektivbeskyttelsemodmalwaremedcloud-baseretbeskyttelse.

HOVEDFUNKTIONER:

EFFEKTIV ANTI-MALWARE-BESKYTTELSE AF KLIENTER

Kasperskys scanningssystemer fungerer på flere niveauer i operativsystemet og udrydder malware.

CLOUD-UNDERSTØTTET BESKYTTELSE

Med det cloud-baserede Kaspersky Security Network er brugerne beskyttet i realtid mod nye trusler.

CENTRALISERET ADMINISTRATION

Administratorer kan centralt fjerne eksisterende antivirussoftware, konfigurere og installere Kaspersky og udføre rapportering - alt fra samme konsol.

ANTI-MALWARE-FUNKTIONER TIL KLIENTER;

HYPPIGE OPDATERINGER OG SIGNATUR-BASERET BESKYTTELSE

Traditionel signatur-baseret metode, der er gennemprøvet i branchen, til påvisning af trusler fra malware.

HOST-BASERET INTRUSION PREVENTION SYSTEM (HIPS) MED PERSONLIG FIREWALL

Foruddefinerede regler for hundredvis af de hyppigst anvendte programmer reducere tidsforbruget til konfiguration af firewall.

ADFÆRD ANALYSERES AF SYSTEM WATCHER

Kaspersky Security Network (KSN) reagerer meget hurtigere end traditionelle metoder til beskyttelse på mistanke om trusler. KSN's reaktionstider kan være helt ned til 0,02 sekunder!

BRED UNDERSTØTTELSE AF PLATFORME

Kaspersky Endpoint Security til Windows®, Macintosh® og Linux® letter arbejdsbyrden for administratoren, der understøtter forskellige netværk.

FUNKTIONER I KASPERSKY SECURITY CENTER

ÉN CENTRAL KONSOL

Til fjernstyring af alle dine klienter, der er beskyttet af Kaspersky.

SKALERBAR UNDERSTØTTELSE

Uanset størrelsen af din infrastruktur tilbyder Kaspersky Security Center installations- og administrationsværktøjer, fleksible politikmuligheder og robust rapportering for at kunne leve op til dine stigende behov.

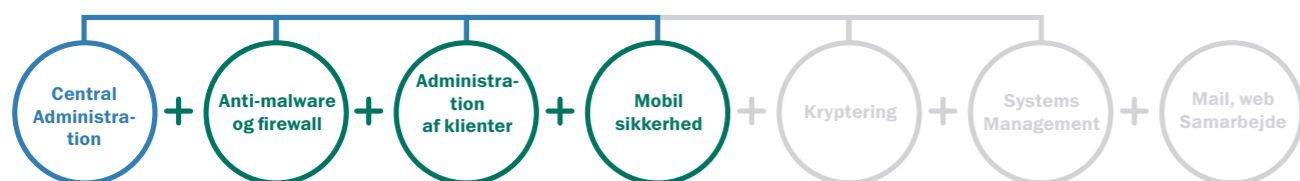
INTUITIV BRUGERGRÆNSEFLADE

Klare og brugbare oplysninger i et overskueligt kontrolpanel gør det muligt for administratorer at se aktuel status for beskyttelse, angive politikker, styre systemer og få rapporter.

WEB-BRUGERGRÆNSEFLADE

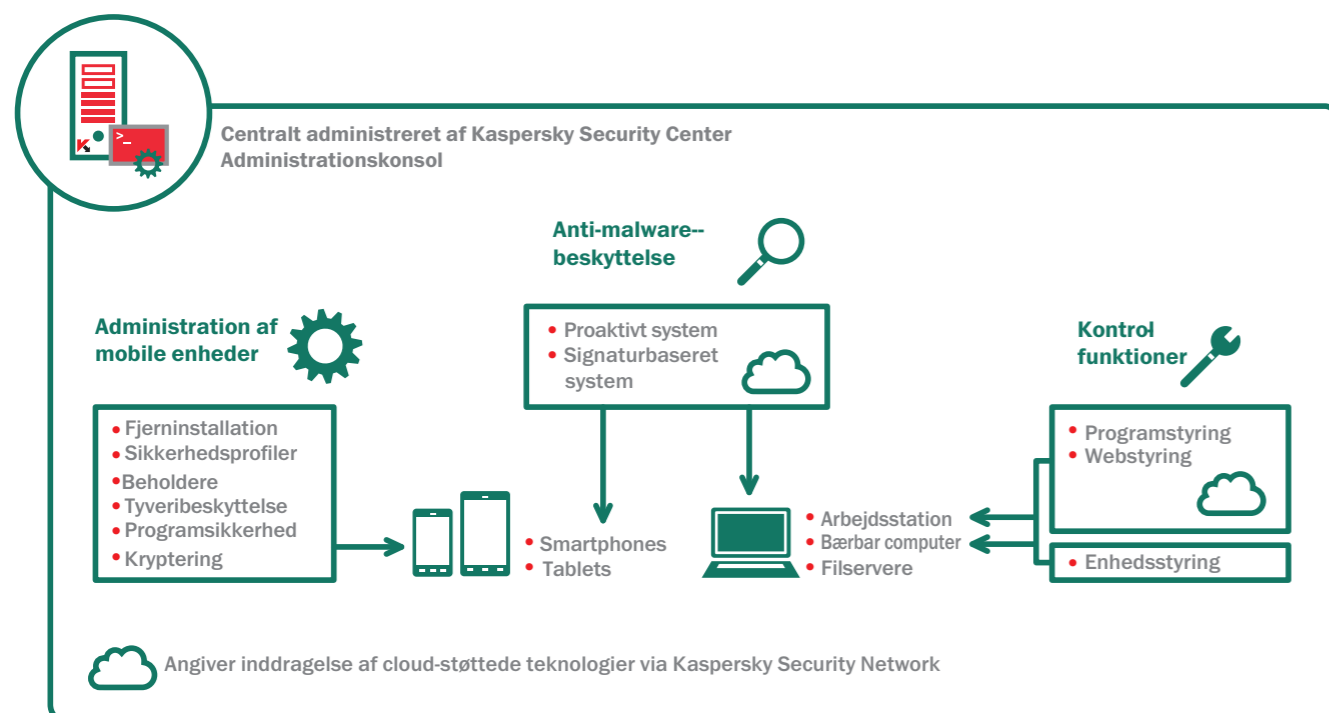
Overvåger eksternt beskyttelsesstatus og rapporterer om de vigtigste begivenheder fra en tilgængelig brugergrænseflade.

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS Select



Værktøjer til at aktivere en mobil arbejdsstyrke, sikre en konsekvent it-sikkerhedspolitik og blokere malware.

Kasperskys 'Select'-niveau inkluderer installation af mobile enheder og beskyttelse via Mobile Device Management (MDM) og mobil anti-malware. Værktøjer til styring af klienter (web, enhed og program) hjælper din organisation med at håndhæve en it-politik, der sikrer de væsentlige elementer i dit it-miljø.



Kaspersky Endpoint Security for Business - vælg niveau. Med kontrolværktøjer og mobilsikkerhed.

HOVEDFUNKTIONER:

EFFEKTIV BESKYTTELSE AF KLIENTER MOD MALWARE

Kasperskys bedste scanningssystem fungerer på flere niveauer i operativsystemet og udrydder malware. Det cloud-baserede Kaspersky Security Network (KSN) beskytter brugerne i realtid mod nye trusler.

FLEKSIBEL, GRANULÆRE STYRINGSVÆRKTØJER

En cloud-baseret, kategoriseret database over sikre og usikre programmer og websteder hjælper administratoren med at håndhæve politikker for programmer og websurfing, mens granulær styring sikrer, at kun bestemte enheder kan sluttes til maskiner på netværket.

PÅ DETTE NIVEAU INTRODUCERES:

STYRING AF KLIENTER:

PROGRAMSTYRING

Gør det muligt for it-administratører at oprette politikker, der tillader, blokerer eller regulerer programmer (eller kategorier af applikationer).

ENHEDSSTYRING

Gør det muligt for brugerne at indstille, planlægge og gennemføre politikker for data med flytbare lagermedier og andre perifere enheder - tilsluttet til USB eller enhver anden type bus.

EFFEKTIV, MOBIL OPSÆTNING OG SIKKERHED FOR SMARTPHONES OG TABLET-PC'ER

Agent-baseret mobilsikkerhed findes til mobile enheder fra Android™, BlackBerry®, Symbian og Windows®. Politikker og programmer på mobile enheder kan via Kaspersky MDM installeres forsvarligt trådløst til disse og iOS-enheder.

WEBSTYRING

Betyder, at klientbaseret styring af surfing følger brugeren - uanset om det er fra virksomhedens netværk eller roaming.

DYNAMISK GODKENDELSE

Filers omdømme leveres i realtid af Kaspersky Security Network, hvorved det sikres, at dine godkendte programmer er fri for malware, og det er med til at maksimere brugernes produktivitet.

KASPERSKY SECURITY FOR MOBILE:

INNOVATIVE ANTI-MALWARE-TEKNOLOGIER

Kombineret signaturbaseret, proaktiv og cloud-baseret opdagelse giver beskyttelse i realtid. En sikker browser og anti-spam øger sikkerheden.

INSTALLATION MED OVER THE AIR (OTA) FORSYNING

Kan forudkonfigurere og installere programmer centralt via SMS, e-mail og pc.

FJERNVÆRKTØJER TIL ANTI-TYVERI

SIM-Watch rRemote Lock, Wipe og Find forhindrer al uautoriseret adgang til virksomhedens data, hvis en mobil enhed mistes eller bliver stjålet.

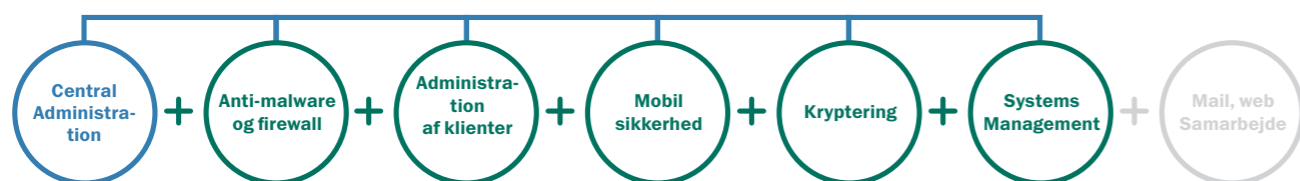
PROGRAMSTYRING FOR MOBILE ENHEDER

Overvåger programmer installeret på en mobil enhed i henhold til de foruddefinerede gruppepolitikker. Inkluderer en "obligatorisk program"-gruppe.

UNDERSTØTTER ENHEDER EJET AF MEDARBEJDERE

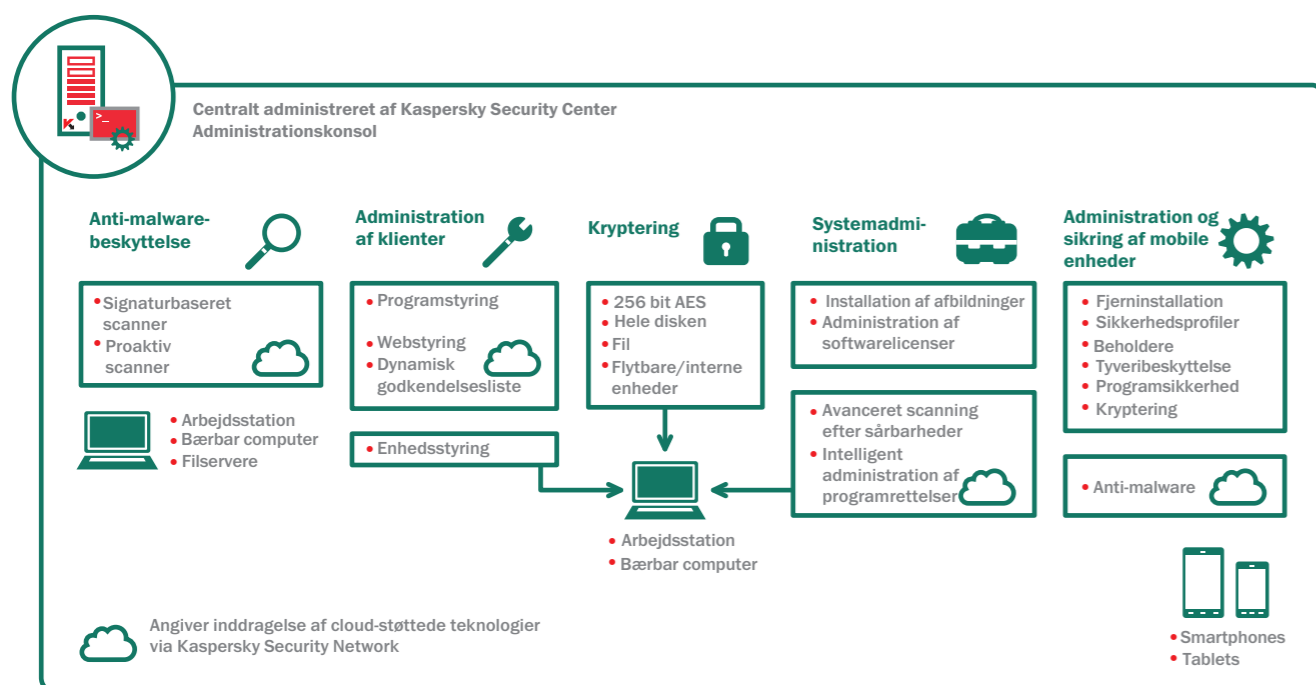
Virksomhedens data og programmer er isolerede i krypterede beholdere, som er gennemsigtige for brugeren. Disse data kan slettes separat.

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS Advanced



Der findes et væld af sikkerhedsværktøjer kombineret med it-optimering i denne værdifulde vifte af løsninger fra Kaspersky Lab.

Kasperskys Advanced niveau leverer de beskyttelses- og administrationsløsninger, din virksomhed behøver for at gennemføre it-politikken, holder brugerne fri for malware, forhindrer datatab og forbedrer it-effektiviteten.



Kaspersky Endpoint Security for Business - avanceret niveau. Med krypteringsteknologi og systemadministration af sikkerhed.

HOVEDFUNKTIONER:

EFFEKTIV KRYPTERINGSTEKNOLOGI

Kryptering med AES 256-bit af hele disken og på mappeniveau beskytter mistede eller stjålne data og tillader sikker datadeling via flytbare enheder, e-mail, netværk eller internettet, alle med gennemsigtighed for brugeren.

SYSTEMKONFIGURATION OG ADMINISTRATION AF PROGRAMRETTELSER

Kombinationen af oprettelse og installation af systemafbildningen, scanning for sårbarheder, automatiseret administration af programrettelser, Network Admission Control, fortegnelser og administration af licenser giver et fuldt integreret sæt værktøjer, der administreres via en enkel, brugervenlig, central konsol.

PÅ DETTE NIVEAU INTRODUCERES:

KRYPTERING OG DATABESKYTTELSE:

OMFATTENDE KRYPTERING

Vælg mellem hele disken eller filniveau, der understøttes af AES (Advanced Encryption Standard) med 256-bit kryptering for at sikre vigtige oplysninger i tilfælde af tab eller tyveri af enheden.

SIKKER DELING AF DATA

Opret krypterede og selvudpakkende pakker for at sikre, at data er beskyttet ved deling via flytbare enheder, e-mail, netværk eller internettet.

MOBIL INSTALLATION OG SIKKERHED TIL SMARTPHONES OG TABLET-PC'ER

Agent-baseret sikkerhed for mobile klienter og administration af fjerne enheder og stoftwarepolitikker via Kaspersky MDM.

EFFEKTIV OG FLEKSIBEL STYRING AF ANTI-MALWARE PÅ KLIENTER

Kasperskys cloud-baserede "best of breed", anti-malware og granulære programmer og værktøjer til styring af internet og enheder.

UNDERSTØTTELSE AF FLYTBARE ENHEDER

Øger din sikkerhed gennem politikker, der skal håndhæve kryptering af data på flytbare enheder.

GENNEMSIGTIGHED FOR SLUTBRUGERE

Kasperskys krypteringsløsning er problemfri og usynlig for brugerne og har ingen negativ indflydelse på produktiviteten. Ingen påvirkning af programindstillinger eller opdateringer.

SYSTEMKONFIGURATION OG ADMINISTRATION AF PROGRAMRETTELSER:

ADMINISTRATION AF PROGRAMRETTELSER

Avanceret, dybdegående scanning for sårbarheder kombineret med automatiseret distribution af programrettelser.

OPERATIVSYSTEM OG PROGRAM TIL AFBILDNINGSIINSTALLATION

Nem oprettelse, lagring og installation af systemafbildninger fra et centralt sted. Perfekt til en migrering til Microsoft® Windows® 8.

FJERNINSTALLATION AF SOFTWARE

Central installation af software til klientmaskiner, selv til afdelingskontorer.

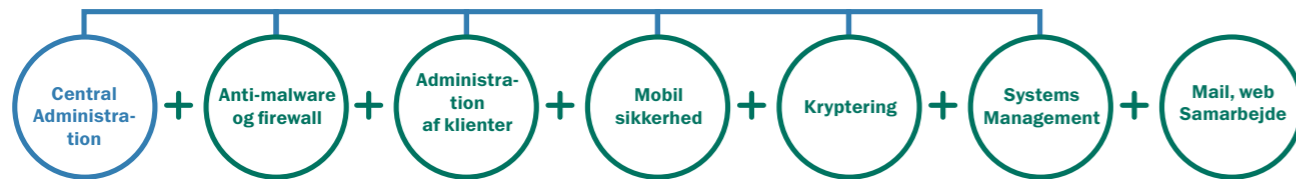
NETWORK ADMISSION CONTROL (NAC)

Med Network Admission Control (NAC), kan du oprette en politik for "gæster" på netværket. Gæste-enheder (herunder mobile enheder) genkendes automatisk og sendes til en virksomhedsportal, hvor en korrekt identificeret adgangskode gør det muligt for dem at benytte de ressourcer, som du har godkendt.

HARDWARE, SOFTWARE OG LICENSSTYRING

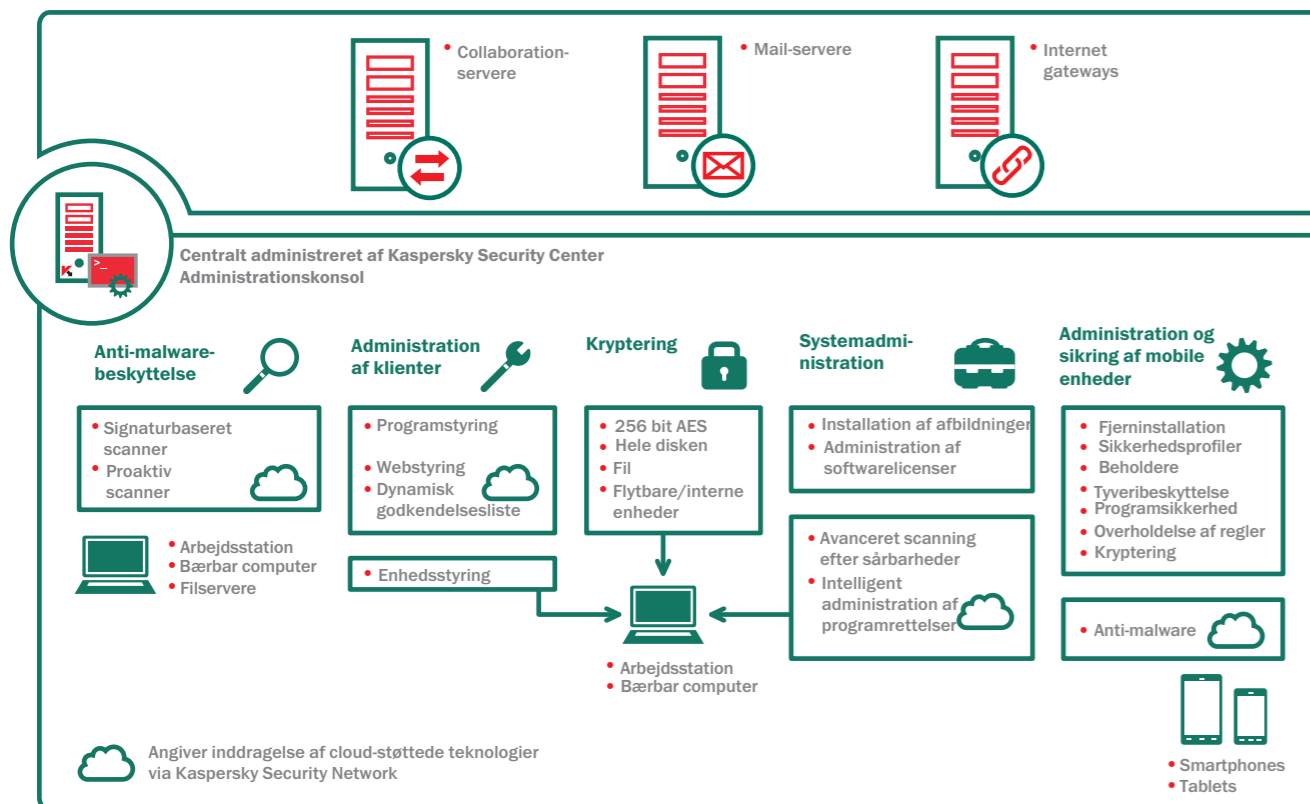
Lagerrapporter om hardware og software hjælper med at styre softwarens licensforpligtelser. Så du kan spare på omkostningerne ved central tildeling af softwarerettigheder.

▶ KASPERSKY TOTAL SECURITY FOR BUSINESS



Komplette værktøjer til beskyttelse mod malware, kryptering, omfattende it-effektivitet og håndhævelse af politikker.

Kaspersky Total Security for Business leverer den mest komplette platform for beskyttelse og administration, som branchen tilbyder i dag. Total Security for Business sikrer hvert lag af dit netværk og indeholder effektive konfigurationsværktøjer til at sikre, at dine brugere er produktive og fri for trusler fra malware, uanset enhed eller placering.



HOVEDFUNKTIONER:

Alle funktionerne fra tre de foregående niveauer, plus:

BESKYTTELSE AF E-MAIL-SERVER

Anti-malware- og anti-spam-beskyttelse af e-mail-trafik til alle populære e-mail-systemer

SECURITY FOR INTERNET GATEWAY

Giver sikker internet-adgang i hele organisationen ved automatisk at fjerne skadelige og potentielt fjendtlige programmer i HTTP(s) /FTP/SMTP og POP3-trafik.

SAMARBEJDSSIKKERHED

Kaspersky beskytter dine SharePoint®-servere mod malware, mens funktioner til filtrering af indhold og filer hjælper med at forhindre lagring af upassende indhold.

PÅ DETTE NIVEAU INTRODUCERES:

MAIL-SERVERE:

BESKYTTELSE AF E-MAIL-TRAFIK

Beskyttelse af mail på de nyeste versioner af de vigtigste platforme til mails og samarbejde: Microsoft Exchange, IBM Lotus Domino og Linux-baserede mailservere.

REDUCERET TRAFIK-BELASTNING

Cloud-aktiveret, intelligent spam filtrering reducerer markant trafikbelastning.

KSN INTEGRATION FOR ANTI-SPAM

Øger spamregistreringsprocent takket være integration med Kaspersky Labs cloud-baserede system til identifikation af trusler (KSN).

OPTIMERING AF SYSTEMRESSOURCER

Et ny antivirusprogram, belastningsjustering af serverressourcer og scanningsbaserede udelukkelse reducerer alle belastningen af dit system.

INTERNET GATEWAYS:

HØJ YDELSE

Et effektivt antivirusprogram plus optimeret, intelligent scanningsteknologi og belastningsjustering øger ydeevnen og reducerer de ressourcer, der er nødvendige til virusscanning.

UNDERSTØTTER FORSKELLIGE PLATFORME

Kaspersky Security for Internet Gateway understøtter de mest populære gateways på Windows- og Linux-platforme.

SAMARBEJDE

ANTI-MALWARE-BARRIERE FOR SHAREPOINT-MILJØER

Anvender nyskabende teknologi, der er udviklet til at identificere og blokere malware fra forsøg på upload eller download i realtid.

INDHOLDSFILTRERING

Hjælper med at forhindre upassende, eksterne overførsler, at håndhæve politikker for intern kommunikation og blokerende lagring af upassende filer efter filtype eller tekstindhold.

KASPERSKY SECURITY FOR MOBILE

Komplet mobilsikkerhed kombinerer Mobile Device Management (MDM) og Endpoint Security for mobile enheder.

Kaspersky MDM gør sikker konfiguration af mobile enheder smertefri og enkel, mens Kaspersky Endpoint Security for Mobile Devices giver den beskyttelse, du behøver mod nutidens trusler - selv på medarbejdernes egne enheder.

NÆRMERE OPLYSNINGER OM FUNKTIONER I KASPERSKY SECURITY FOR MOBILE:

FUNKTIONER I IT EFFICIENCY:

NEM KONFIGURATION VIA EN ENKELT KONSOL

I modsætning til andre løsninger giver Kaspersky Lab administratorer mulighed for at bruge en enkelt konsol til styring af sikkerhed for mobile enheder, fysiske klienter, virtuelle systemer, kryptering og værktøjer til håndhævelse af politikker.

PRIVAT PROGRAMPORTAL

Administratorer offentliggør en virksomhedsportal, der indeholder links til godkendte programmer. Brugere kan begrænses til kun disse programmer.

TRÅDLØS TILDELING

Sikrer fjerne telefoner ved at sende enten en e-mail eller SMS med et link til virksomhedsportalen,

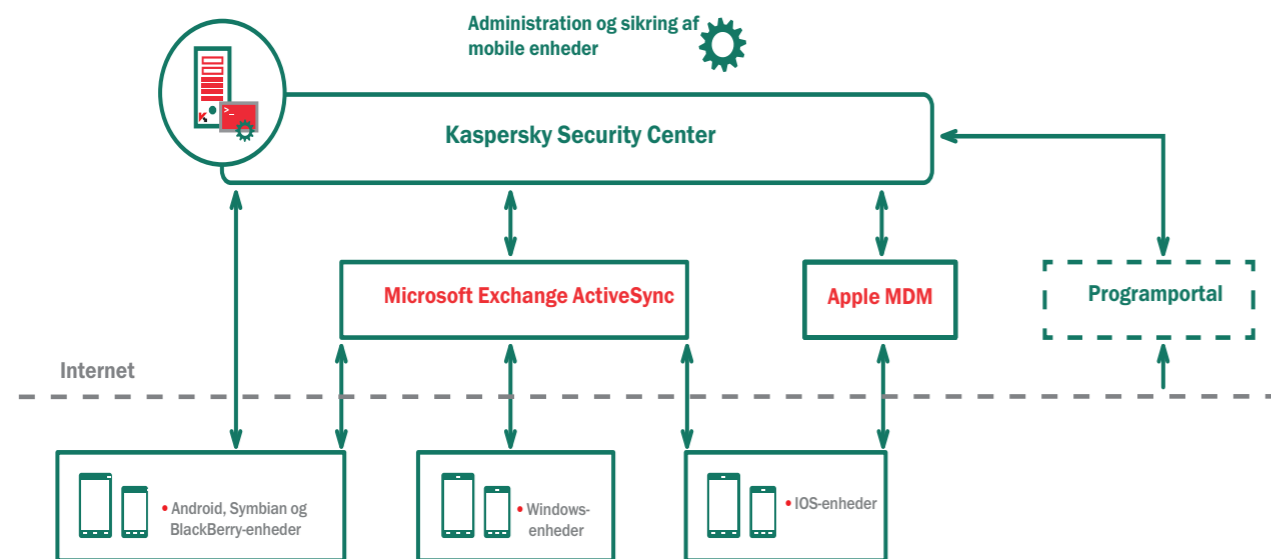
hvorfra brugerne kan downloade den profil og de programmer, du har godkendt. Brugeren har ikke adgang til data, før brugeren har accepteret.

SIKKER KONFIGURATION

Sikrer integritet for hardware og software ved at aktivere rooting og jailbreak-sporing. Andre sikkerhedsindstillinger omfatter "deaktivering af kamera", tvungen adgangskode mv.

OVERHOLDELSE OG HÅNDHÆVELSE AF POLITIKKER

Programstyring giver mulighed for overvågning og kontrol med brugen af enheden, herunder "Afvis som standard" og "Tillad som standard".



HÅNTERING AF SIKKERHEDSRISICI:

KRYPTERING

Data er beskyttet via transparent datakryptering af hele disken og på filniveau og kan også anvendes på en beholder.

TYVERIBESKYTTELSE

Administratorer kan fjernstyre en fuld eller selektiv sletning af en enhed, lokalisere en mistet enhed ved hjælp af GPS-"Find" og få besked, hvis et SIM-kort fjernes eller udskiftes.

MOBIL ANTI-MALWARE

Kaspersky Labs anti-malware-system indeholder flere detekteringslag inkl. cloud-assisteret beskyttelse og kombineres med en sikker browser og effektiv anti-spam for at sikre, at enheden ikke er kompromitteret af skadelig software.

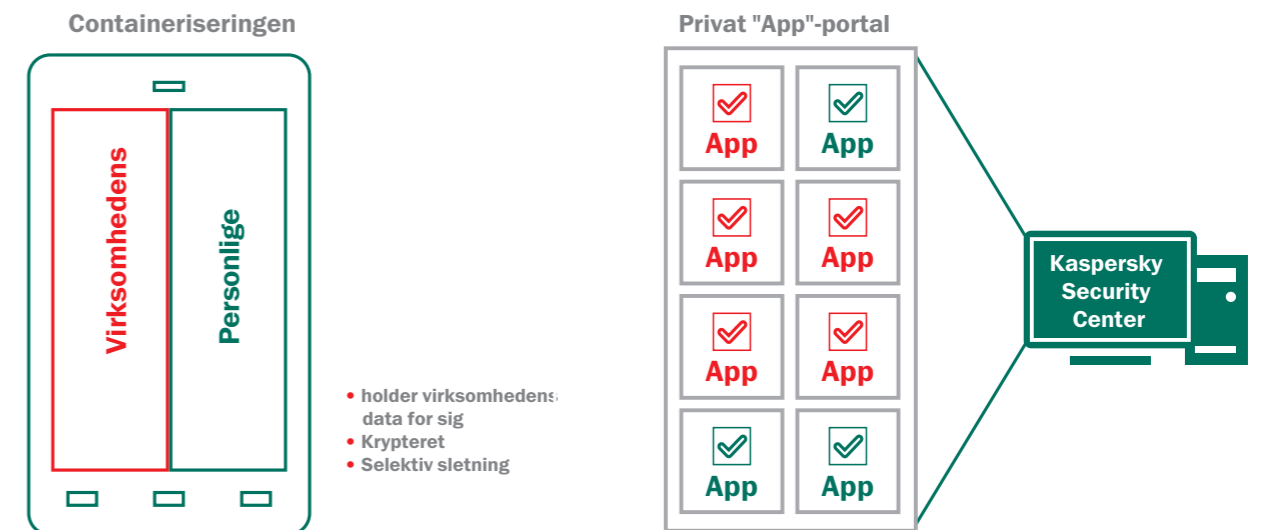
INTEGRITET FOR VIRKSOMHEDENS OG PERSONLIGE DATA:

BEHOLDERE

Til hjælp for enheder, der er ejet af medarbejdere, kan virksomhedens data og programmer placeres i isolerede "beholdere". Dette giver maksimal sikkerhed for virksomhedens data og optimal integritet for personligt indhold.

VÆRKTØJER TIL FJERNSTYRING AF DATASIKKERHED

Hvis en enhed bliver forlagt, kan Fjernlås aktiveres. Virksomhedens data i en beholder på enheden kan sikres, krypteres, fjernadministreres og slettes uafhængigt af personlige data på enheden.



PERFEKT TIL "TAG DIN EGEN ENHED MED" (BYOD) INITIATIVER

Mange medarbejdere anvender deres egne enheder til både personlige og virksomhedens opgaver. Nogle virksomheder tilskynder faktisk medarbejderne til at vælge deres foretrukne smartphone eller tablet fra en forhandler, og it-afdelingen tilføjer e-mail og virksomhedsadgang til den medarbejderejede enhed.

Der er besparelser og produktivetsmæssige fordele, men BYOD (tag din egen enhed med) kan også åbne organisationen for sikkerhedsrisici. Virksomhedens data kan nemt misbruges pga. utilstrækkelig beskyttelse og potentiel sammenblanding med personlige ting. Ofte anvendes disse enheder også af familiemedlemmer, som ikke tager hensyn til programmernes sikkerhed. Nogle udsættes endda for rooting eller jailbreak.

Kaspersky Security for Mobile løser disse problemer ved at muliggøre sikker konfiguration og installation af smartphones og tablet-pc'er ved hjælp af samme konsol som din netværkssikkerhed. IT-administratorer kan trygt regne med, at brugernes enheder er konfigureret med de korrekte indstillinger og kan sikres i tilfælde af tab, tyveri eller misbrug.

► KASPERSKY SYSTEMS MANAGEMENT

Vi præsenterer Kaspersky Systems Management. Denne løsning indeholder en bred vifte af effektive og produktivitetsfremmende it-værktøjer skrevet i samme kode og styret fra en enkelt konsol. Det giver en platform med den enkelhed og automatisering, du ønsker - og den sikkerhed og kontrol, du har brug for.

FORSKELLIGE IT-VÆRKTØJER SKABER KOMPLEKSITET - OG KOMPLEKSITET ER EN TRUSSEL MOD SIKKERHEDEN.

Undgå gentagelse

Eliminer dobbeltarbejde i forbindelse med etablering af individuelle systemer for nye og eksisterende brugere. Ved hjælp af teknologi til tildeling af system kan diskafbildninger oprettes, administreres og installeres fra en central placering.

Øg sikkerhed

Administratorer fortæller os, at deres dage ofte går med at sikre, at programrettelser er opdateret.. Kaspersky hjælper med at fjerne kompleksitet ved at identificere sårbarheder, der kan udnyttes straks, og hvilke løsninger, der kan udskydes til efter arbejdstid. Denne prioritering hjælper administratorer med at planlægge deres arbejdsdag og forbedre sikkerheden.

Arbejd effektivt

Administratorer kan fjerninstallere afbildninger, opdateringer, programrettelser og programmer. Hvis en bruger har et problem, kan it-afdelingen logge på maskinen og fjernstyre fejlfinding på systemet. Det betyder, at administratoren ikke spilder sin tid ved at gå fra skrivebord til skrivebord eller bruge frustrerende timer på at yde mindre produktiv telefonsupport.

Disse funktioner og mere til er en del af Kaspersky Systems Management og tilgås via administrationskonsollen i Kaspersky Security Center. Eftersom hvert værktøj ikke kræver sin egen konsol, er kommandoer ensartede, intuitive og kræver ingen yderligere uddannelse.

FUNKTIONER TIL SYSTEMADMINISTRATION:

OPERATIVSYSTEM OG PROGRAMTILDELING

Nem oprettelse, lagring, kloning og installation af systemafbildninger fra en central placering. Sørg for, at systemer leveres til brugeren uden problemer og med optimale sikkerhedsindstillinger. Dette værktøj er velegnet til migrering til Microsoft Windows 8.

VÆR PÅ FORKANT MED SÅRBARHEDER

Et klik på hardware- og software-scanning sammenligner resultater på tværs af flere sårbarhedsdatabaser, så du kan prioritere hvilke sårbarheder, som kræver øjeblikkelig opmærksomhed, og hvilke, som du kan udskyde til efter arbejdstid.

FJERNBETJENT, FLEKSIBEL SOFTWAREINSTALLATION

Minimer netværksbelastningen ved at benytte enten manuelle eller planlagte installationer.

FJERNAGENTER

Tildel en arbejdsstation i et fjern- eller afdelingskontor som en central opdateringsagent. Spar båndbredde ved at sende én opdatering til et fjernkontor - og brug den pågældende arbejdsstation til distribution af opdateringen på det pågældende sted.

UNDERSTØTTELSE AF WAKE-ON-LAN-TEKNOLOGI

Ved installation og support uden for arbejdstiden kan Kaspersky Systems Management fjernstyre start af en arbejdsstation.

FEJLFINDINGSVÆRKTØJER

Fjernbetjent og sikker forbindelse til et klientsystem for at løse problemer - fra samme, administrative konsol.

UNDERSTØTTER MICROSOFT WINDOWS SERVER UPDATE SERVICES (WSUS)

Kaspersky Systems Management synkroniserer jævnlige data med tilgængelige opdateringer og programrettelser til servere, herunder Microsoft Windows Update, downloader dem via Windows Update Services og distribuerer dem effektivt .

NETWORK ADMISSION CONTROL (NAC)

Med Network Admission Control (NAC) kan du oprette en netværkspolitik for "gæster". Gæsteenheder (herunder mobile enheder) genkendes automatisk og sendes til virksomhedens portal, hvor de korrekte legitimationsoplysninger gør det muligt for dem at udnytte de ressourcer, du har godkendt.

FORTEGNELSER OVER HARDWARE OG SOFTWARE

Computere, harddiske og endog flytbare enheder findes automatisk og tages med i fortegnelsen. Indførelsen af en ny enhed udløser en meddelelse til administratoren. Denne funktion gør det muligt for administratoren at spore status og brug af hardware på netværket.

TILDELING OG ADMINISTRATION AF LICENSER

Kaspersky Systems Management rapporterer præcis hvilken software, der er i brug i dit miljø. Derved kan du tilpasse dine licensomkostninger og identificere brugere, der ikke er i overensstemmelse med reglerne. Ved installation sammen med Kaspersky Labs klientværktøjer kan du begrænse brugen til kun godkendte programmer og versioner - og begrænse antallet af licenser i brug ad gangen.

► KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server giver pålidelig beskyttelse af servere, der kører Microsoft® Windows®, Novell NetWare og Linux mod alle typer af ondsindede programmer.

Antivirusbeskyttelse af delt fillagring er afgørende, da en enkelt inficeret fil på en server kan inficere arbejdsstationerne hos alle brugere af ressourcen. En ordentlig beskyttelse af filserveren sikrer ikke kun, at brugere og deres data er beskyttet, men eliminerer også risikoen for, at ondsindede programmer finder vej til sikkerhedskopier af filer, hvilket kan medføre gentagne malware-udbrud og andre hændelser.

PRODUCT HIGHLIGHTS*

- Understøttelse af de nyeste versioner af Microsoft® Windows® og Linux-platforme
- Optimeret brug af systemressourcerne
- Understøtter Hierarchical Storage Management-systemer (HSM)
- Beskyttelse af terminalservere og servere i klynger
- Certificeret forberedt til VMware
- Understøttelse af NSS-filsystemet
- Gratis BSD-understøttelse

FUNKTIONER

- Beskyttelse af fil-servere, der kører Windows® (herunder Windows Server® 2008 R2), Linux (herunder Samba) og Novell NetWare
- Forbedret proaktiv beskyttelse mod nye, ondsindede programmer
- Antivirusbeskyttelse i realtid
- Behandling af aktive infektioner
- Planlagt scanning af lagrede filer
- Scanning af systemets kritiske områder
- Isolation af smittede arbejdsstationer
- Skalerbarhed
- Sikkerhedskopiering af data før desinfektion eller sletning
- Centraliseret installation, administration og opdateringer
- Valg af metoder til installation og administration
- Fleksibelt system til scanning og scenarier for reaktion på hændelser
- Meddelelsessystem for status for programmer
- Omfattende rapporter over status for nettets beskyttelse

PROGRAMMER

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

* Produktfunktioner kan variere afhængigt af kombinationen af anvendte komponenter. Se beskrivelse af komponenterne på: www.kaspersky.com for yderligere oplysninger om de enkelte komponenters funktioner.

► KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server beskytter mail- og groupware-servere mod ondsindede programmer og spam.

Produktet indeholder programmer, der beskytter e-mail-trafik på alle populære servere, herunder Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim og CommuniGate Pro. Løsningen kan også bruges til at oprette en dedikeret e-mail-gateway.

PRODUCT HIGHLIGHTS*

BESKYTTELSE AF MAILSERVER

Anti-malware- og anti-spam-beskyttelse af mails til alle populære e-mail-systemer.

OPTIMERING AF SYSTEMRESSOURCER

Et ny anti-virusprogram, belastningsjustering af serverressourcer og scanningbaserede reducerer alle belastningen af dit system.

KSN-INTEGRATION AF ANTI-SPAM

Øger spamregistreringsprocent takket være integration med Kaspersky Labs cloud-baserede system til identifikation af trusler (KSN).

REDUCERET TRAFIKBELASTNING

Cloud-aktiveret, intelligent spamfiltrering reducerer markant trafikbelastning.

FUNKTIONER

- Integreret beskyttelse af mail-servere mod alle former for ondsindede programmer
- Effektiv beskyttelse mod spam
- Antivirusbeskyttelse i realtid
- Planlagt scanning af e-mails og databaser
- Beskyttelse af Sendmail, qmail, Postfix, Exim og CommuniGate Pro mail-serverne
- Scanning af meddelelser, databaser og andet på Lotus® Domino® serverne
- Scanning af alle meddelelser på Microsoft® Exchange-serveren, herunder offentlige mapper
- Filtrering af meddelelser efter vedhæftet filtype
- Skalerbarhed
- Understøttelse af Microsoft® Exchange Server 2007-klynger og DAG for Microsoft® Exchange Server 2010
- Sikkerhedskopiering af data før desinfektion eller sletning
- Isolation af smittede objekter
- Annullering af gentagne mail-scanninger
- Bekvem værktøj til installation, administration og opdateringer
- Omfattende rapporter om beskyttelsesstatus
- Fleksibelt system til scanning og scenarier for reaktion på hændelser
- Meddelelsessystem for status for programmer

PROGRAMMER

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

* Produktfunktioner kan variere afhængigt af kombinationen af anvendte komponenter. Se beskrivelse af komponenterne på: www.kaspersky.com for yderligere oplysninger om de enkelte komponenters funktioner.

► KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway giver sikker adgang til Internettet for alle medarbejdere i en organisation.

Kaspersky Security for Internet Gateway understøtter de mest populære gateways på Windows- og Linux-platforme. Kendte, skadelige og potentielt farlige programmer, der kører via HTTP, HTTPS og FTP, POP3 og SMTP-protokoller, slettes automatisk fra datastrømmen. Optimeringsteknologi, skalerbarhed og understøttelse af de nyeste platforme gør det til det ideelle produkt til store organisationer med store trafikmængder.

PRODUCT HIGHLIGHTS*

- Beskyttelse af Microsoft® Forefront® TMG
- Bredt udvalg af værktøjer til administration af politikker og konfiguration
- Scanning af VPN-forbindelser
- Beskyttelse af e-mail-trafik (via POP3- og SMTP-protokoller)
- Scanning af HTTP- og FTP-trafik fra offentliggjorte servere
- Certificeret forberedt til VMware

FUNKTIONER

- Scanning i realtid af internettrafik via HTTP-, HTTPS-, FTP-, POP3- og SMTP-protokoller
- Integreret beskyttelse mod alle former for ondsindede programmer
- Understøttelse af Squid, Blue Coat og Cisco® proxyservere
- Lagring af sikkerhedskopier
- Belastningsjustering af server-processorer
- Skalerbarhed
- Bekvemme værktøjer til installation, administration og opdateringer
- Flexibelt system til scanning og scenarier for reaktion på hændelser
- Omfattende rapporter om nettets beskyttelsesstatus

PROGRAMMER

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

* Produktfunktioner kan variere afhængigt af kombinationen af anvendte komponenter. Se beskrivelse af komponenterne på: www.kaspersky.com for yderligere oplysninger om de enkelte komponenter.

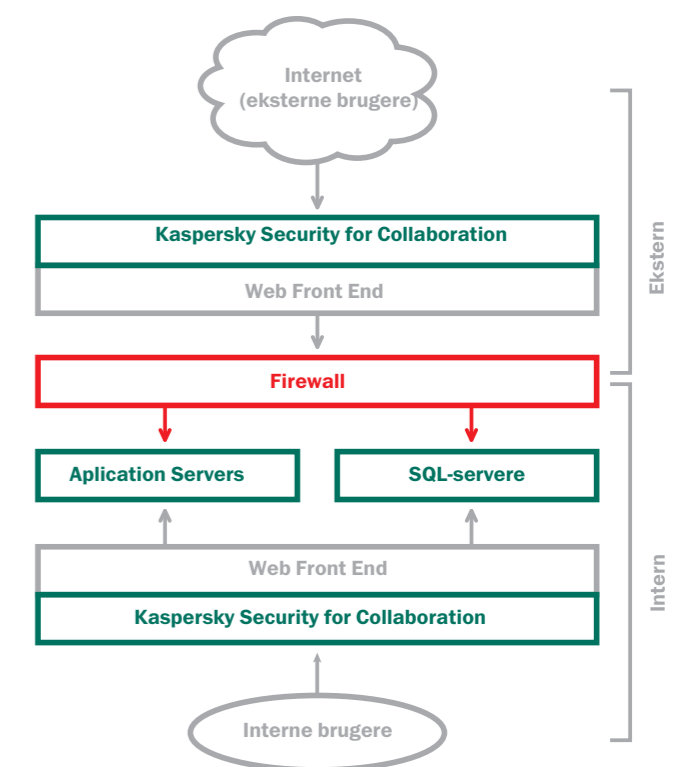
► KASPERSKY SECURITY FOR COLLABORATION

Kaspersky Security for Collaboration benytter de nyeste teknologier til beskyttelse af din samarbejdsplatform og kombinerer brugervenlig administration med høj malwaresporingsrate.

Kaspersky Security for Collaboration bruger Kaspersky's prisbelønnede antivirusprogram til beskyttelse af Microsoft® SharePoint®-miljøer. Med prisbelønnet teknologi til opdagelse af malware beskytter produktet en enkelt server eller hele SharePoint-miljøer - mens dens indhold og funktioner til filtrering af filer hjælper med at forhindre lagring af upassende indhold.

FUNKTIONER

- Innovativ teknologi til opdagelse af malware er designet til at identificere og blokere trusler mod forsøg på overførsel i realtid
- Forhindrer slutbrugere i at lagre bestemte filtyper (f.eks. musik, video, eksekverbare filer) eller filer med upassende tekst
- Globale administrationsindstillinger kan konfigureres på alle beskyttede servere fra en enkelt skærm
- Enkel, intuitiv administration - kræver ingen særlig uddannelse
- Integration med Active Directory strømliner opsætning og brugergodkendelse
- Detaljerede logfiler og backup af ændrede filer hjælper administratorer med at reagere på krænkelser eller sikkerhedsproblemer
- Detaljeret, fleksibel rapportering



* Produktfunktioner kan variere afhængigt af kombinationen af anvendte komponenter. Se beskrivelse af komponenterne på: www.kaspersky.com for yderligere oplysninger om de enkelte komponenter.

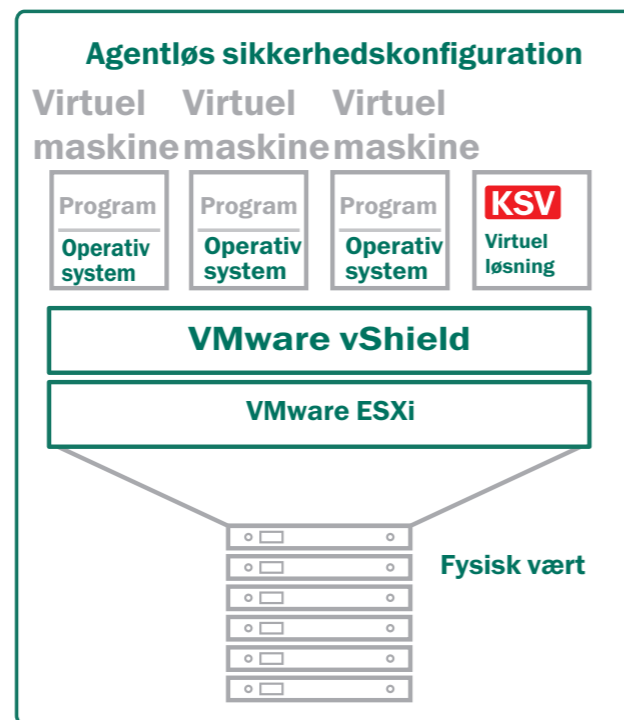
▶ KASPERSKY SECURITY FOR VIRTUALIZATION

Med Kaspersky Security for Virtualization – som er konstrueret til de unikke krav fra virtualiserede it-miljøer – får du prisbelønnet anti-malware-beskyttelse til virtualiserede servere, desktop-computere og datacentre.

Kaspersky Security for Virtualization er en agentløs anti-malware-løsning, som giver en mere effektiv måde at beskytte den virtualiserede infrastruktur på – med bedre ydelse og mindre påvirkning af tætheden af virtualiseringen. Programmet er nemt at installere og har avancerede administrationsfunktioner, som forenkler en lang række sikkerhedsopgaver – på både de fysiske og virtuelle maskiner.

BESKYTTELSES- OG YDELSESFUNKTIONER

- **Centraliseret sikkerhed.** Kaspersky Security for Virtualization er en virtuel løsning, som fungerer sammen med VMwares vShield Endpoint – så der leveres funktioner til anti-malware-scanning. Der leveres et enkelt, centraliseret anti-malware-system og en database til hver af de fysiske værtsmaskiner.
- **Avanceret anti-virus-system** Med Kasperskys prisbelønnede anti-malware-teknologier – kombineret med Kasperskys hyppige opdateringer, som er branchens bedste – får du hjælp til at beskytte systemet mod nye og fremspirende trusler. En heuristisk analysefunktion bekæmper polymorfisk malware.
- **Automatisk beskyttelse** Nye virtuelle maskiner beskyttes automatisk vha. anti-malware-løsningen – så man undgår huller i sikkerheden og fejlkonfigurationer. Enhver gæst-VM er altid beskyttet med den nyeste signaturdatabase, uanset om en VM tidligere var offline.
- **Større tæthed for virtualiseringen** Da Kaspersky Security for Virtualization er en agentløs løsning, hjælper den med at eliminere pres fra opdateringer og scanninger, opnår større tæthed for virtualiseringen, reducerer påvirkning af ydelsen og undgår de huller i sikkerheden, som kan være forbundet med visse agentbaserede produkter.



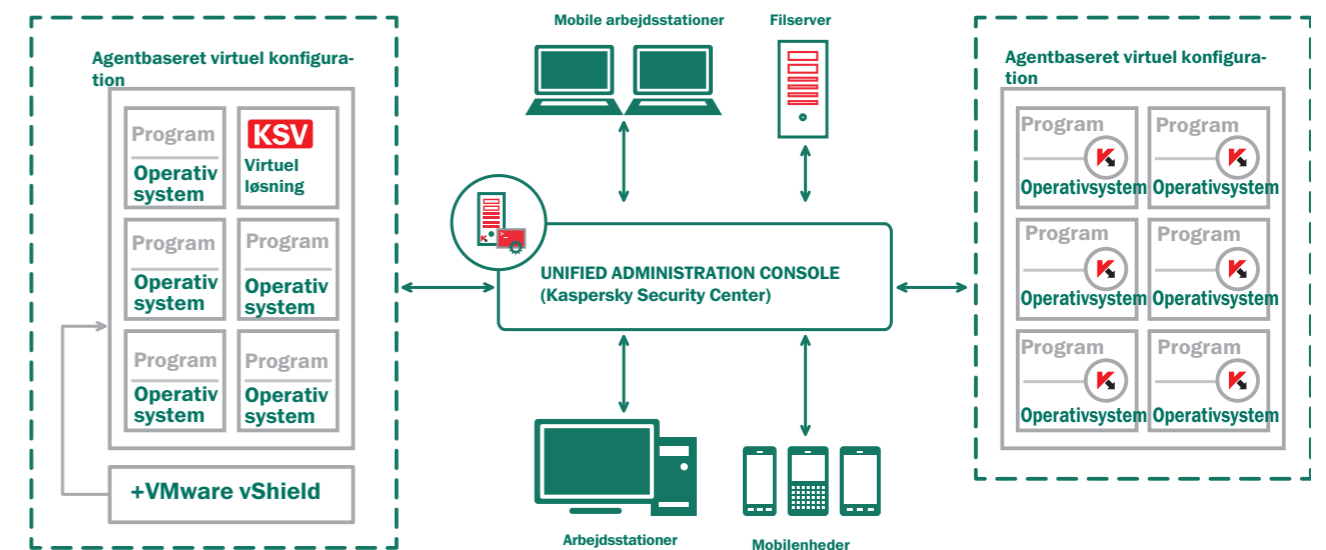
Kaspersky Security for Virtualization giver agentløs antivirusbeskyttelse af VMware-konfigurationer.

ADMINISTRATIONSFUNKTIONER:

ÉN ENKELT ADMINISTRATIONSKONSOL
Kaspersky Security Center – som følger gratis med – er en enkelt, samlet administrationskonsol, hvorfra du kan administrere sikkerheden for virtuelle maskiner, fysiske maskiner og mobile enheder.

UNDERSTØTTER VMWARE VMOTION
Idet Kaspersky Security for Virtualization understøtter VMware vMotion fuldt ud, sikres det, at beskyttelsen ikke afbrydes, når en arbejdsbelastning flyttes fra den ene ESXi-vært til den anden. Forudsat at den nye værtsmaskine har de nødvendige licenser, følger beskyttelsen arbejdsbelastningen, og alle sikkerhedsindstillingerne vil forblive de samme.

INTEGRERET MED VMWARE VCENTER
Kaspersky Security for Virtualization modtager oplysninger om virtuelle maskiner fra vCenter – herunder en liste over alle de virtuelle maskiner og relevante parametre. Ud over at it-medarbejderne opnår større overblik, sikrer denne integration med vCenter, at der automatisk leveres beskyttelse, når en ny virtuel maskine konfigureres.



▶ KASPERSKY ANTI-VIRUS FOR STORAGE

Kaspersky Anti-Virus for Storage beskytter EMC Celerra-familien af netværkslagringsprodukter mod alle typer malware.

Datalagringsystemer på et netværk giver medarbejdere i organisationer af enhver størrelse hurtig og nem delt adgang til oplysninger. Men hvis et virksomhedsnetværk ikke er beskyttet, kan adgang til delte filer have nogle meget uheldige konsekvenser. En enkelt inficeret fil gemt på et system kan kompromittere hele netværket og medføre betydelige forretningsmæssige, finansielle og omdømmemæssige skader. Derfor er omfattende beskyttelse af netværkslagringsystemer en absolut nødvendighed.

Kaspersky Anti-Virus for Storage er fuldt ud kompatibel med EMC Celerra-produktsortimentet. Det er specielt udviklet til at forsyne dem med de højeste niveauer af beskyttelse, afsløring og uskadeliggørelse af malware i filer og arkiver, der er lagret i Celerra-systemer. Løsningen giver administratorer mulighed for at konfigurere systemet til at udføre scanningsopgaver i realtid, da objekter gemmes og modificeres, eller on-demand, hvis det ønskes.

FUNKTIONER

- Beskyttelse af EMC Celerra-datalagringsystemer
- Understøttelse af Windows Server® 2008 R2
- Understøtter Hierarchical Storage Management-systemer (HSM)
- Forbedret, proaktiv beskyttelse mod nye, ondsindede programmer
- Antivirusbeskyttelse i realtid
- Planlagte scanninger af lagrede filer
- Scanning af systemets kritiske områder
- Optimeret brug af systemressourcerne
- Sikkerhedskopiering af data før desinfektion eller sletning
- Skalerbarhed
- Certificeret forberedt til VMware
- Centraliseret installation, administration og opdatering via Kaspersky Security Center
- Integreres fuldt med Kaspersky Endpoint Security for Business Platform og andre Kaspersky-produkter
- Meddelelsessystem for status for programmer
- Omfattende rapporter om nettets beskyttelsesstatus

Kaspersky Lab AB
Jan Stenbecks Torg 17
164 40 Kista
Sverige

corporatesales@kaspersky.dk
www.kaspersky.dk

Alt om internetsikkerhed:
www.securelist.com

Find en partner i nærheden af dig:
www.kaspersky.com/buyoffline

© 2013 Kaspersky Lab ZAO. Alle rettigheder forbeholdes. Registrerede varemærker og servicemærker tilhører deres respektive ejere. Mac og Mac OS® er registrerede varemærker tilhørende Apple Inc. Cisco er et registreret varemærke eller varemærke tilhørende Cisco Systems, Inc. og/eller dets associerede selskaber i USA og visse andre lande. IBM, Lotus, Notes og Domino er varemærker tilhørende International Business Machines Corporation, registreret i mange retskredse over hele verden. Linux er et registreret varemærke tilhørende Linus Torvalds i USA og andre lande. Microsoft, Windows, Windows Server og Forefront er registrerede varemærker tilhørende Microsoft Corporation i USA og andre lande. Android™ er et varemærke tilhørende Google, Inc. Varemærket BlackBerry ejes af Research In Motion Limited og er registreret i USA og kan være under behandling eller registreret i andre lande.

