

A man with glasses, wearing a white shirt and a dark tie, is shown in profile, talking on a mobile phone. The background is a bright, slightly blurred office setting with vertical blinds.

▶ **KASPERSKY
VERKSAMHETS-
PRODUKTER 2013**

SEE IT. CONTROL IT.

PROTECT IT.

► OM KASPERSKY LAB

Kaspersky Lab är världens största oberoende säkerhetsprogramföretag. Vi erbjuder bästa möjliga IT-säkerhet för din organisation genom en kombination av kraftfulla skydd mot skadlig programvara, flexibla kontrollverktyg, krypteringsteknik och systemhanteringsverktyg. Kaspersky Security sträcker sig från klienten till dina servrar och gatewayer och vår unika integrerade design betyder att du kan skydda och kontrollera alla dina fysiska, virtuella och mobila enheter från en central hanteringskonsol, oberoende av hur stor din infrastruktur är. Kaspersky-tekniken används över hela världen i produkter och tjänster från ledande IT-tillverkare och utgivare.

Mer information finns på www.kaspersky.com.

Om du vill ha den senaste informationen om antivirusprogram, antispionprogram, skydd mot skräppost och andra IT-säkerhetsproblem och trender går du till www.securelist.com.

► BRANSCHENS ENDA HELT INTEGRERADE SÄKERHETSPLATTFORM

EN KONSOL

Kaspersky-produkterna har utformats så att du från ett "fönster" kan visa och hantera hela säkerhetslösningen, såväl virtuella datorer som fysiska och mobila enheter.

EN PLATTFORM

Vid Kaspersky Lab har vi utvecklat konsolen, säkerhetsmodulerna och verktygen i egen regi i stället för att köpa in från andra företag. Detta innebär att samma programmerare utifrån samma kodbas har utvecklat tekniker som fungerar tillsammans. Resultatet är stabilitet, integrerade policyer, praktisk rapportering och intuitiva verktyg.

EN KOSTNAD

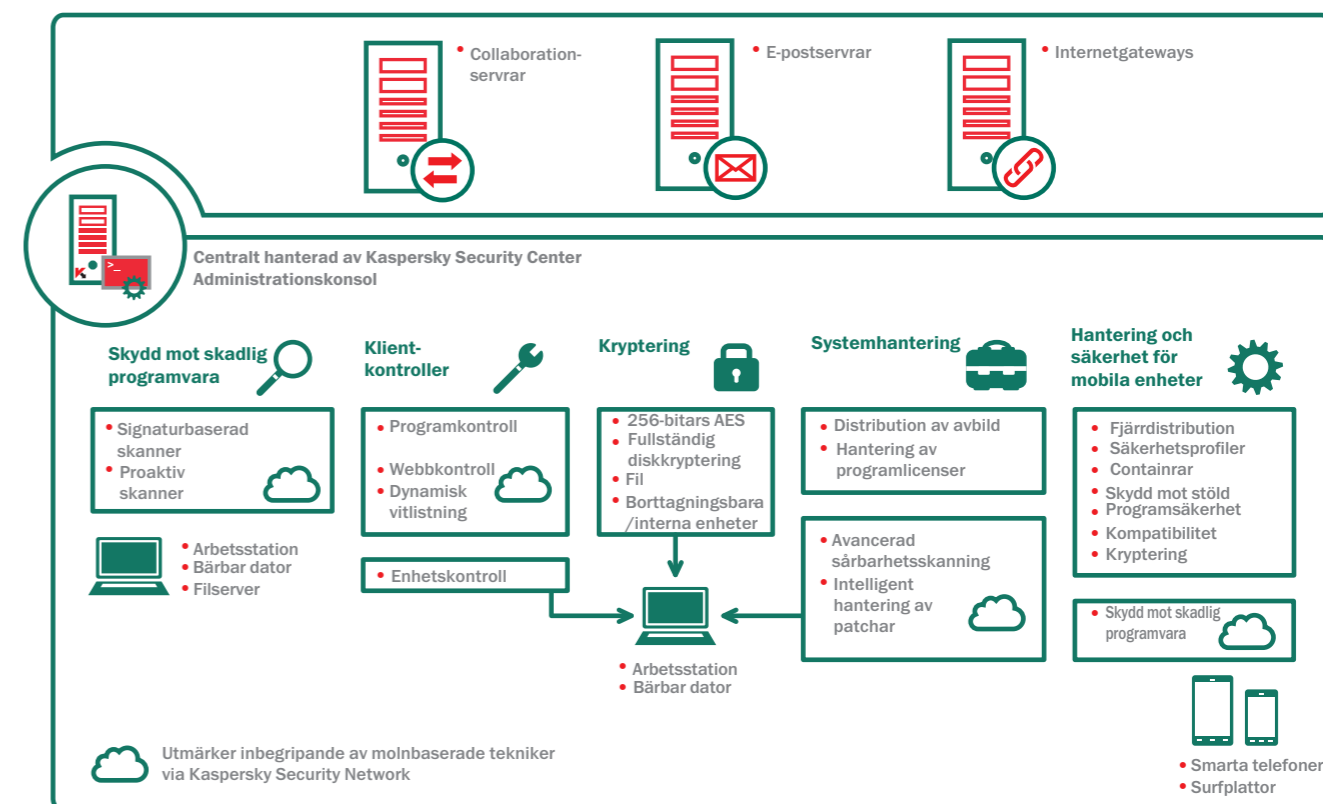
Alla Kaspersky-produkter och verktyg kommer från samma leverantör och levereras som en installation. Du behöver inte gå igenom en ny budget- och motiveringsprocess varje gång för att få säkerhetsriskerna i linje med företagets mål.

► DEN RÄTTA LÖSNINGEN FÖR DIG

Kaspersky Security for Business ger den rätta lösningen för ditt företag, oberoende av om du letar efter något för att skydda och kontrollera klienterna (från arbetsstationer till smarta telefoner och virtuella datorer) för att skydda dina servrar och gatewayer, eller för att fjärrhantera hela säkerhetsmiljön.

Kaspersky kan erbjuda en omfattande lista med olika tekniker, från kryptering och hantering av mobila enheter till patchhantering och licensregister. Allt fungerar friktionsfritt och stöds av det molnbaserade Kaspersky Security Network för att ge kunderna det förstklassiga skydd som de behöver för att motverka de allt mer sofistikerade och diversifierade cyberhoten.

Kort sagt så har vi levererat branschens första säkerhetsplattform som skapad från grunden, vilket underlättar för administratörer att visa, kontrollera och skydda sin värld.

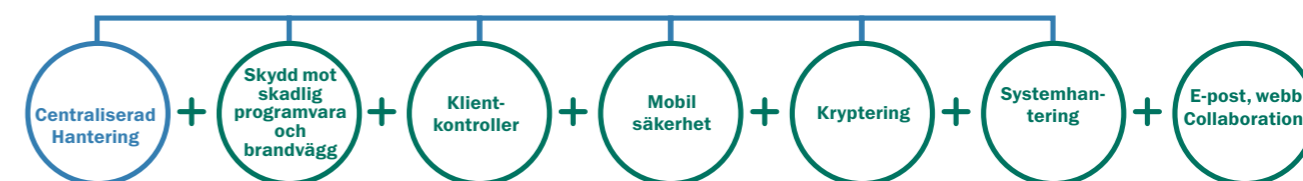


► KASPERSKY SECURITY FOR BUSINESS

Våra olika tekniker och hur de samverkar för att skydda dig

	Core	Select	Advanced	Total	Hanteras av Security Center	Tillgängligt i en riktad lösning
Skydd mot skadlig programvara	•	•	•	•	•	
Brandvägg	•	•	•	•	•	
Programkontroll		•	•	•	•	
Enhetskontroll		•	•	•	•	
Webbkontroll		•	•	•	•	
Filservrar		•	•	•	•	•
Agent för mobil klient		•	•	•	•	•
Hantering av mobila enheter		•	•	•	•	•
Krypteringsteknik			•	•	•	
OS Image Management			•	•	•	•
Licenshantering			•	•	•	•
Sårbarhetshantering			•	•	•	•
Hantering av patchar			•	•	•	•
Kontroll av nätverksåtkomst			•	•	•	•
Collaboration				•		•
E-postservrar				•		•
Internetgateways				•		•
Virtualisering					•	•
Lagring					•	•

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS



NIVÅN CORE

Vi har kompletterat Kasperskys prisvinnande och kraftfulla icke-serverbaserade teknik för skydd mot skadlig programvara och en skyddande brandvägg, med Kaspersky Security Center – vår intuitiva administrationskonsol. För kunder som bara kräver skydd mot skadlig programvara är detta lösningen.

NIVÅN SELECT

CORE-nivån är utbyggd med skyddstjänster för **filserversäkerhet, programvitlistor och -kontroll, enhetskontroll samt webbkontroll**. Den innehåller också en **lösning för mobilskydd** som består av en **agent för klientssäkerhet** och **MDM (Mobile Device Management)**. Om behoven inkluderar skydd av mobil arbetsstyrka och genomdrivande av IT-policyer kan SELECT vara den rätta nivån för er.

NIVÅN ADVANCED

På nivån ADVANCED har Kaspersky även lagt till **dataskydd** i form av **kryptering** av filer eller hela diskar. Ytterligare ett nytt erbjudande är **Kaspersky Systems Management** som kombinerar säkerhet med IT-effektivitet. Den här breda uppsättningen funktioner inkluderar viktiga verktyg så att administratören kan:

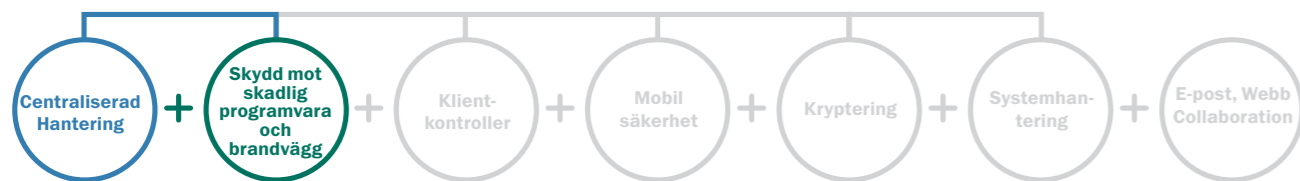
- Skapa utbildnings- och distribueringsystem med modulen Image Management.
- Prioritera behandling av sårbarheter i maskinvara och programvara med en kraftfull kombination av avancerad sårbarhetsskanning och intelligent patchhantering.
- Spåra licensanvändning och efterlevnad med hjälp av Software License Management (hantering av programlicenser).
- Ställa in åtkomstpolicyer till data och infrastruktur för användare och gäster med Network Admission Control (åtkomstkontroll för nätverk).
- Distribuera och fjärrinstallera uppdateringar och ny programvara till användare från centralkonsolen.

KASPERSKY TOTAL SECURITY FOR BUSINESS

Vårt flaggskepp Kaspersky Total Security for Business kombinerar de tre tidigare nivåerna och förbättrar säkerheten med ytterligare skydd av webb-, e-post och collaborationservrar. Detta är den perfekta lösningen för organisationer som har stora säkerhetskrav och kräver bästa möjliga skydd för varje nätverk.

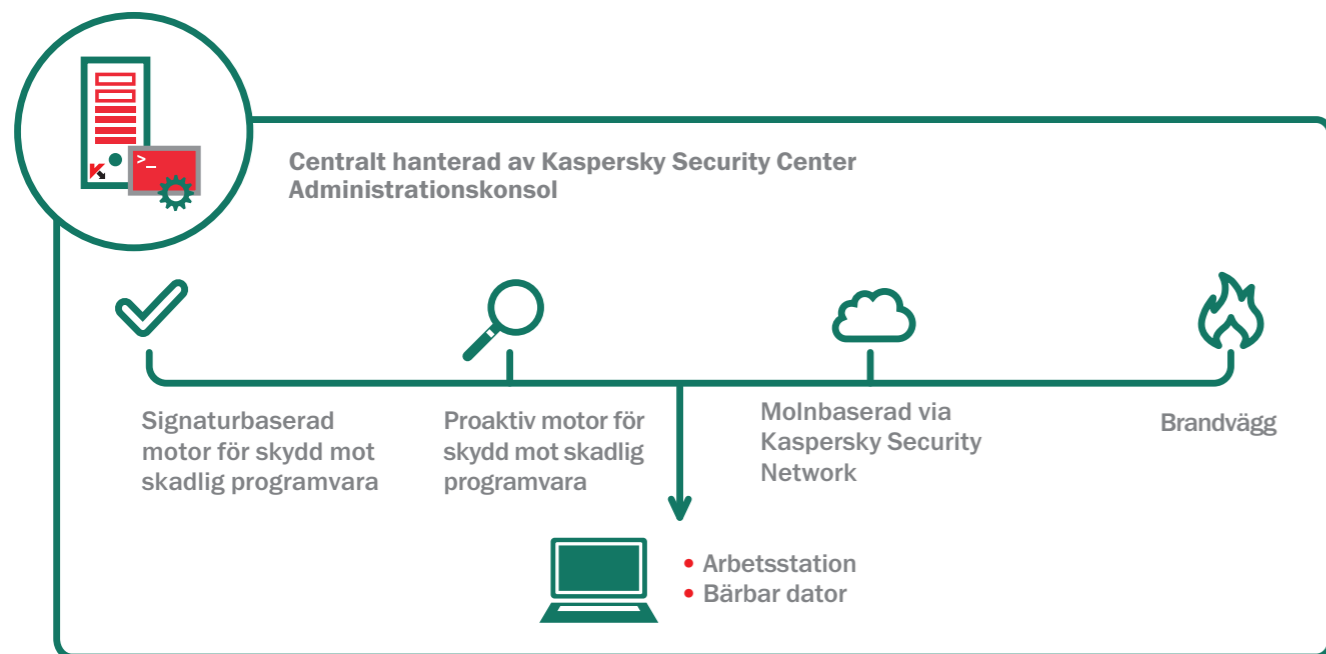
► KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Core



Prisbelönt skydd mot skadlig programvara med centraliserad distribution, hantering och rapportering.

En säkerhetsmodell i flera lager börjar med det bästa skyddet mot skadlig programvara. Eftersom Kaspersky länge har varit känt som ledande inom identifiering och borttagning av skadlig programvara, finns det ingen bättre grund. Nivån Core i Kaspersky Endpoint Security for Business hanteras centralt i Kaspersky Security Center med stöd av det molnbaserade Kaspersky Security Network.



Core-nivån i Kaspersky Endpoint Security for Business – kraftfullt skydd mot skadlig programvara med molnbaserat skydd.

HUVUDFUNKTIONER:

KRAFTFULLT SKYDD MOT SKADLIG PROGRAMVARA FÖR KLIENTER

Kasperskys sökmotorer arbetar på flera nivåer i operativsystemet och tar effektivt bort skadlig programvara.

MOLNBASERAT SKYDD

Med det molnbaserade Kaspersky Security Network är användarna skyddade mot nya hot i realtid.

CENTRAL HANTERING

Administratörer kan centralt ta bort befintlig antivirusprogramvara, konfigurera och distribuera Kaspersky samt utföra rapportering – allt från samma konsol.

FUNKTIONER I SKYDD MOT SKADLIG PROGRAMVARA FÖR KLIENTER:

FREKVENTA UPPDATERINGAR OCH SIGNATURBASERAT SKYDD

Branschbeprövad, traditionell signaturbaserad metod för identifiering av hot från skadlig programvara.

VÄRDBASERAT SYSTEM FÖR INTRÅNGSSKYDD (HIPS) MED PERSONLIG BRANDVÄGG

Fördefinierade policyer för hundratals av de mest använda programmen minskar tiden för konfiguration av brandväggen.

BETEENDEANALYS UTFÖRD AV SYSTEM WATCHER

Kaspersky Security Network (KSN) svarar på misstänkta hot, mycket snabbare än traditionella skyddsmetoder. Svarstiden för KSN kan vara så kort som 0,02 sekunder!

BRETT PLATTFORMSSTÖD

Kaspersky erbjuder klientssäkerhet för Windows®, Macintosh® och Linux®, vilket gör det enklare för administratörer som hanterar olika nätverk.

FUNKTIONER I KASPERSKY SECURITY CENTER:

EN CENTRAL KONSOL

För fjärrhantering av alla företagets Kaspersky-skyddade klienter.

WEBBGRÄNSSNITT

Fjärrövervakar skyddsstatus och rapporterar om nyckelhändelser från ett tillgängligt gränssnitt.

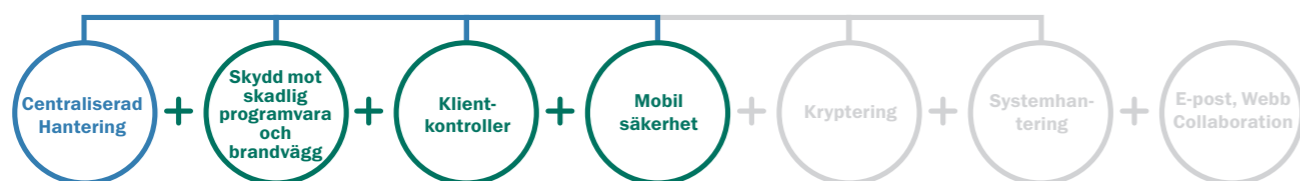
INTUITIVT ANVÄNDARGRÄNSSNITT

Tydlig, interagerbar information på en ren instrumentpanel ger administratörer möjlighet att visa skyddsstatus i realtid, ange policyer, hantera system och få rapporter.

SKALBART STÖD

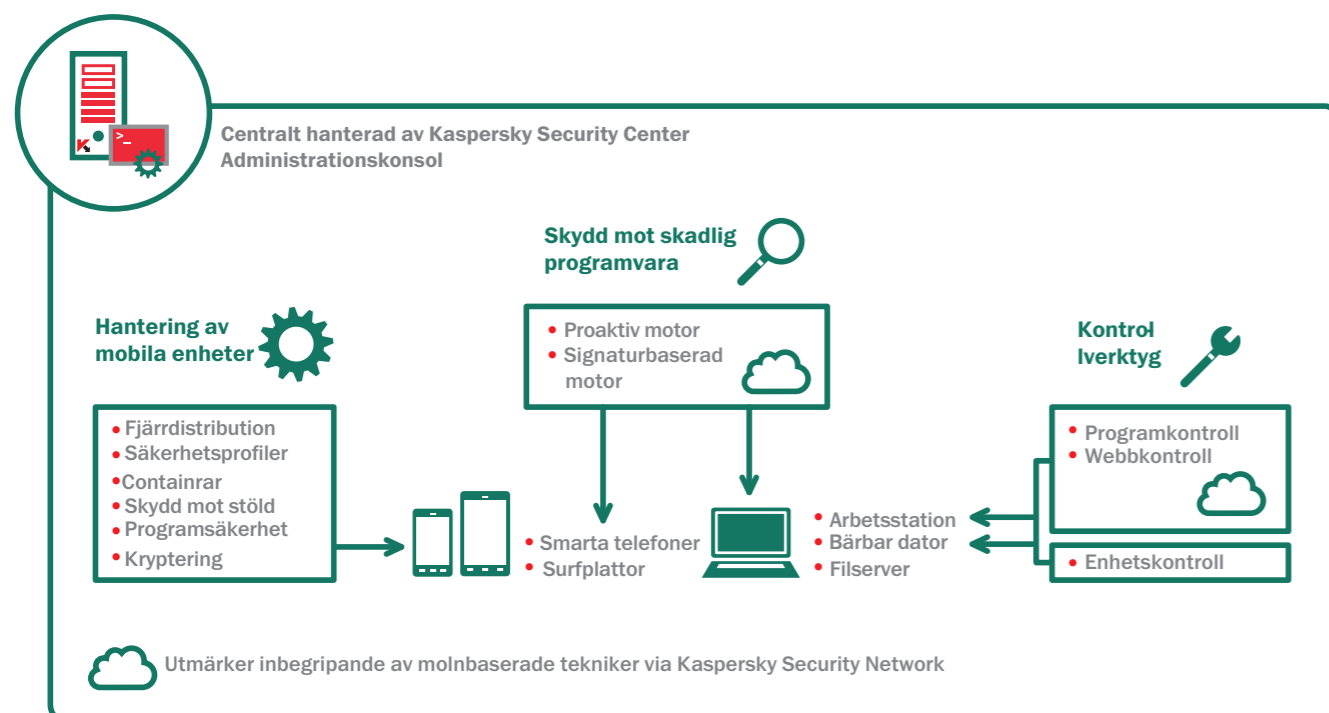
Oavsett infrastrukturens storlek erbjuder Kaspersky Security Center verktyg för distribution och hantering, flexibla policyalternativ och stabil rapportering för att uppfylla dina växande behov.

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS Select



Verktyg som möjliggör mobil arbetsstyrka, säkerställer överensstämmande IT-säkerhetspolicyer och blockerar skadlig programvara.

Kasperskys Select-nivå omfattar distribution och skydd av mobila enheter via Mobile Device Management (MDM) och skydd mot skadlig programvara för mobila enheter. Verktyg för klientkontroll (webb, enheter och program) hjälper företaget att upprätthålla IT-policyer och skyddar därmed viktiga element i IT-miljön.



Kaspersky Endpoint Security for Business – nivån Select. Med kontrollverktyg och mobil säkerhet.

HUVUDFUNKTIONER:

KRAFTFULLT SKYDD MOT SKADLIG PROGRAMVARA FÖR KLIENTER

Kasperskys bästa sökmotor arbetar på flera nivåer i operativsystemet och tar effektivt bort skadlig programvara. Det molnbaserade Kaspersky Security Network (KSN) skyddar användarna i realtid mot nya hot.

FLEXIBLA, GRANULÄRA KONTROLLVERKTYG

En molnbaserad, kategoriserad databas över säkra och osäkra program och webbplatser hjälper administratören att skapa och upprätthålla policyer för program och webbsurfning, medan granulära kontroller säkerställer att bara specifika enheter kan anslutas till datorer i nätverket.

EFFEKTIV DISTRIBUTION OCH SÄKERHET FÖR MOBILA ENHETER SOM SMARTA TELEFONER OCH SURFPLATTOR

Agentbaserad mobilsäkerhet är tillgänglig för enheter som har Android™, Blackberry®, Symbian och Windows® Mobile. Policyer och programvara för mobila enheter kan säkert fjärrdistribueras via Kaspersky MDM till dessa enheter och till iOS-enheter.

DEN HÄR NIVÅN INNEHÅLLER:

KLIENTKONTROLLER:

PROGRAMKONTROLL

Ger IT-administratörer möjlighet att skapa policyer för att tillåta, blockera eller policyera program (eller programkategorier).

WEBBKONTROLL

Innebär att klientbaserade kontroller vid surfning följer användaren, både i företagsnätverket och vid roaming.

ENHETSKONTROLL

Ger användare möjlighet att ange, schemalägga och upprätthålla datapolicyer för kontroll av borttagningsbara lagringsenheter och annan kringutrustning – anslutna via USB eller någon annan busstyp.

DYNAMISK VITLISTNING

Filryktesdata i realtid från Kaspersky Security Network säkerställer att godkända program är fria från skadlig programvara vilket bidrar till att maximera användarproduktiviteten.

KASPERSKY SECURITY FOR MOBILE:

INNOVATIVA TEKNIKER FÖR SKYDD MOT SKADLIG PROGRAMVARA

Kombinerad signaturbaserad, förebyggande och molnbaserad identifiering ger realtidsskydd. En säker webbläsare och skydd mot skräppost ökar säkerheten.

PROGRAMKONTROLL FÖR MOBILA ENHETER

Övervakar program som är installerade på en mobil enhet enligt fördefinierade gruppolicyer. Omfattar en grupp med obligatoriska program.

DISTRIBUTION VIA FJÄRRANSLUTNING (OTA)

Möjlighet att förkonfigurera och distribuera program centralt med hjälp av SMS, e-post och dator.

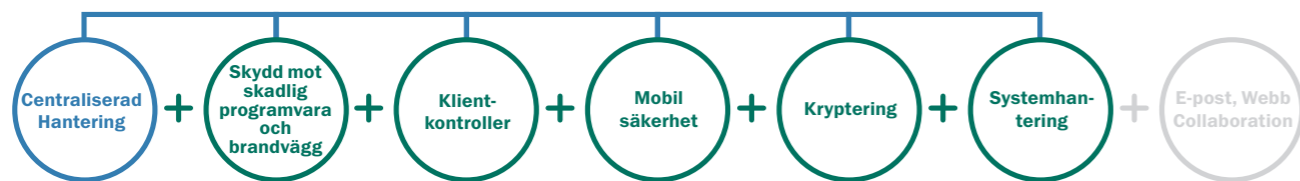
STÖD FÖR ANSTÄLLDAS PRIVATA ENHETER

Företagets data och program är isolerade i krypterade behållare som är transparenta för användaren. Den här informationen kan rensas separat.

FJÄRRVERKTYG FÖR STÖLDSKYDD

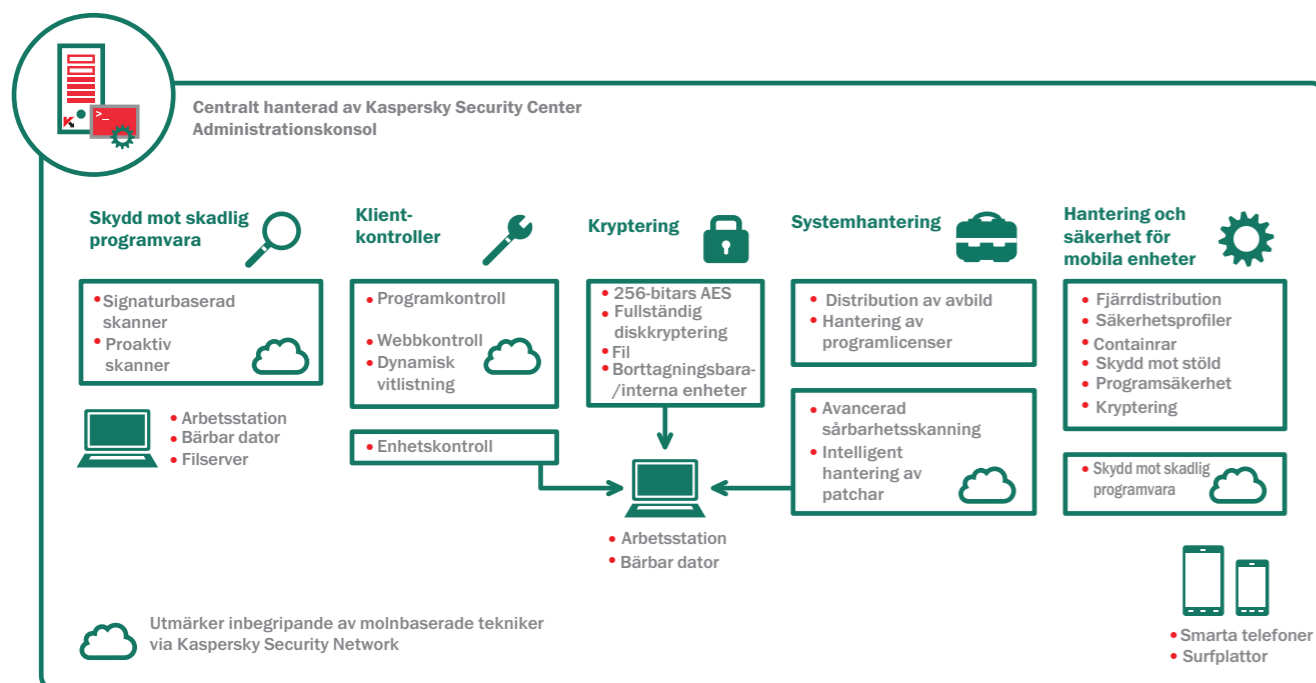
Funktionerna för SIM-Watch, fjärrlåsning, rensning och sökning förhindrar obehöriga att få åtkomst till företagsdata om en mobil enhet förloras eller stjäls.

▶ KASPERSKY ENDPOINT SECURITY FOR BUSINESS Advanced



Säkerhetsverktyg kombinerade med IT-optimeringsfunktioner gör dessa lösningar från Kaspersky Lab oslagbara.

Kasperskys Advanced-nivå erbjuder den skydds- och hanteringslösning som din organisation behöver för att upprätthålla IT-policyer, skydda användarna mot skadlig programvara, förhindra dataförluster och förbättra IT-effektiviteten.



Kaspersky Endpoint Security for Business – nivån Advanced. Med krypteringsteknik och hantering av säkerhetssystem.

HUVUDFUNKTIONER:

KRAFTFULL KRYPTERINGSTEKNIK

Kryptering av hel disk eller på mappnivå AES 256-bitars skyddar förlorade eller stulna data och medger dessutom säker datadelning via borttagningsbara diskar, nätverk eller webb, helt transparent för användaren.

SYSTEMKONFIGURATION OCH PATCHHANTERING

Skapande av avbildningar av operativsystem och distribution, skanning efter sårbarheter, automatisk patchhantering, NAC (Network Admission Control), lager- och licenshantering – kombinerat i en komplett verktygslåda som administreras via en användarvänlig, central konsol.

MOBIL DISTRIBUTION OCH SÄKERHET FÖR SMARTA TELEFONER OCH SURFPLATTOR

Agentbaserad mobil klientssäkerhet samt fjärrhantering av enheter och programvarupolicy via Kaspersky MDM.

KRAFTFULLT SKYDD MOT SKADLIG PROGRAMVARA FÖR KLIENTER OCH FLEXIBLA KONTROLLER

Kasperskys bästa molnbaserade skydd mot skadlig programvara och avancerade kontrollverktyg för skydd av program, webben och enheter.

DEN HÄR NIVÅN INNEHÅLLER:

KRYPTERING OCH DATASKYDD

OMFATTANDE KRYPTERING

Välj mellan kryptering av hel disk eller på filnivå enligt AES (Advanced Encryption Standard) med 256-bitars kryptering för skydd av viktig företagsinformation vid stöld eller förlust av enhet.

SÄKER DATADELNING

Skapa krypterade och självextraherande paket som säkerställer att data skyddas vid delning via borttagningsbara enheter, e-post, nätverk eller webben.

STÖD FÖR BORTTAGNINGSBARA ENHETER

Ökad säkerhet tack vare policyer som upprätthåller kryptering av data på borttagningsbara enheter.

TRANSPARENS FÖR SLUTANVÄNDARE

Kasperskys krypteringslösning är sömlös och osynlig för användarna, och har ingen negativ påverkan på produktiviteten. Påverkar inte heller programinställningar eller uppdateringar.

SYSTEMKONFIGURATION OCH PATCHHANTERING:

HANTERING AV PATCHAR

Avancerad, djupgående skanning efter sårbarheter i kombination med automatiserad distribution av patchar.

DISTRIBUTION AV OPERATIVSYSTEMS- OCH PROGRAMAVBILDNINGAR

Enkelt att skapa, lagra och distribuera systemavbildningar från en central plats. Perfekt för migrering till Microsoft® Windows® 8.

FJÄRRDISTRIBUTION AV PROGRAMVARA

Central distribution av programvara till klientdatorer, även till lokalkontor.

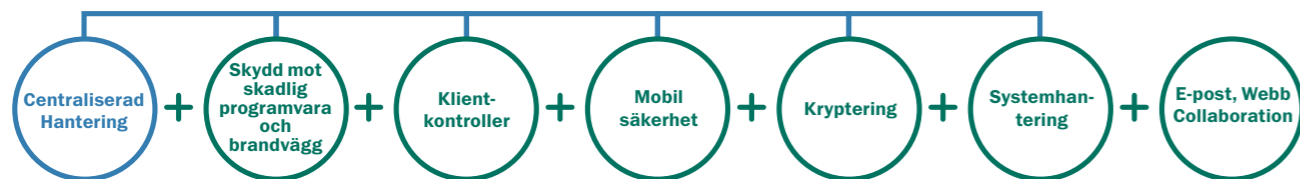
NETWORK ADMISSION CONTROL (NAC)

Med Network Admission Control (NAC) kan du skapa en gästpolicy för nätverket. Gästenheter (inklusive mobila enheter) identifieras automatiskt och skickas till en företagsportal där korrekt identifieringslösenord gör att de kan använda de resurser som du har godkänt.

HANTERING AV MASKINVARA, PROGRAMVARA OCH LICENSER

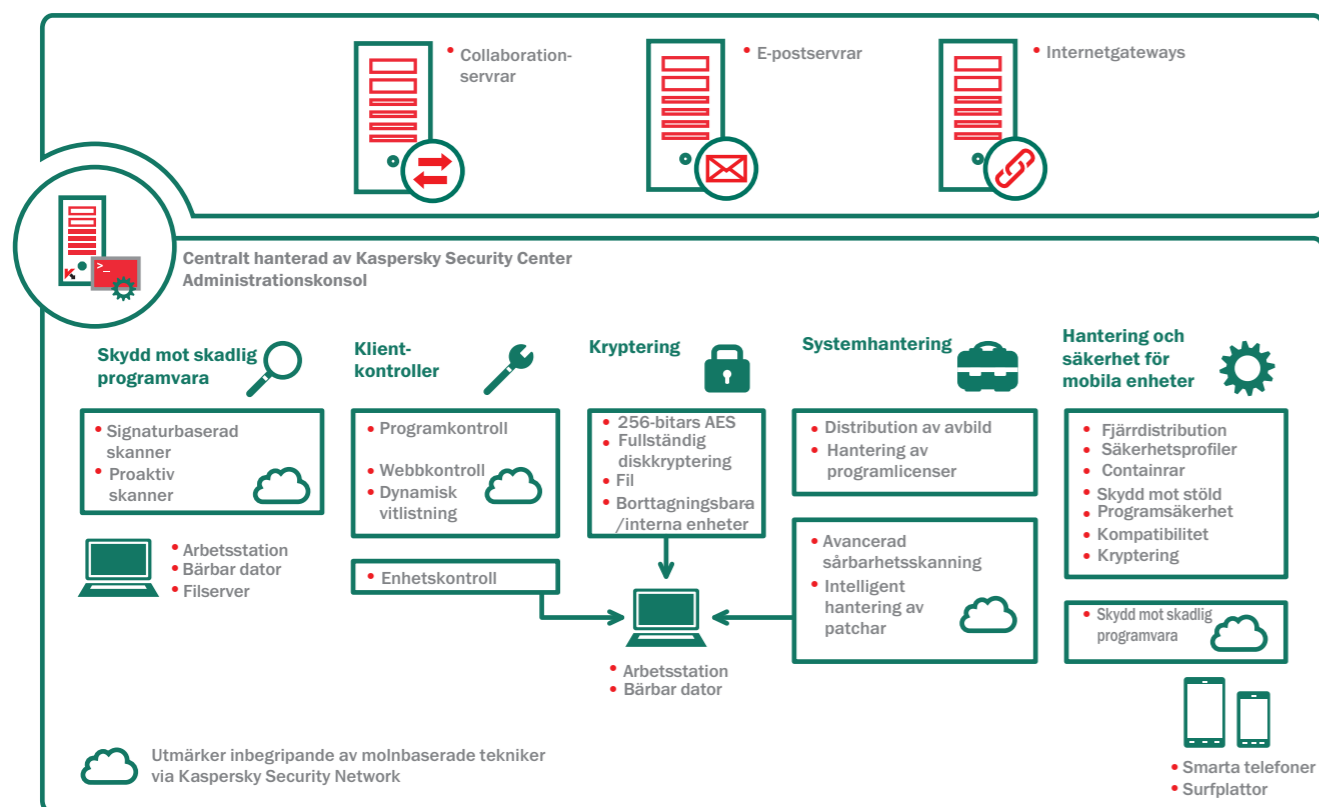
Med hjälp av inventeringsrapporter för maskinvara och programvara har du kontroll över programvarulicenskrav. Du kan därmed spara kostnader genom centralt installerade programvarurättigheter.

KASPERSKY TOTAL SECURITY FOR BUSINESS



Skydd mot skadlig programvara mellan klienter, kryptering samt omfattande verktyg för IT-effektivitet och policyefterlevnad.

Kaspersky Total Security for Business är den mest kompletta plattformen för skydd och hantering som branschen erbjuder idag. Med Total Security for Business skyddas varje lager i nätverket, det innehåller kraftfulla konfigurationsverktyg som ser till att användarna kan vara produktiva och skyddade mot hot från skadlig programvara oavsett enhet och plats.



HUVUDFUNKTIONER:

Alla funktioner i föregående tre nivåer och:

SKYDD FÖR E-POSTSERVER

Skydd mot skadlig programvara och skräppost i e-posttrafik för alla populära e-postsystem

SÄKERHET FÖR INTERNETGATEWAYS

Garanterar säker internetåtkomst i hela företaget genom att automatiskt ta bort skadlig och potentiellt fientlig programvara i HTTP(S)-, FTP-, SMTP- och POP3-trafik.

COLLABORATIONSÄKERHET

Kaspersky skyddar dina SharePoint®-servrar mot skadlig programvara, medan funktioner för innehålls- och filfiltrering bidrar till att förhindra lagring av olämpligt innehåll.

DEN HÄR NIVÅN INNEHÅLLER:

E-POSTSERVERAR:

SKYDD FÖR E-POSTTRAFIK

Skydda e-post på de senaste versionerna av större plattformar för e-post och collaboration: Microsoft Exchange, IBM Lotus Domino och Linux-baserade e-postserverar.

KSN-INTEGRERING FÖR SKYDD MOT SKRÄPPOST
Ökar antalet upptäckta skräppostmeddelanden tack vare integrering med Kaspersky Labs molnbaserade motor för identifiering av hot (KSN).

MINSKAD TRAFIKBELASTNING

Molnbaserad och intelligent skräppostfiltrering minskar trafikbelastningen.

OPTIMERING AV SYSTEMRESURSER

En ny antivirusmotor, belastningsbalansering av serverresurser och skanningsexkluderingar minskar belastningen på systemet.

INTERNETGATEWAYER

HÖGA PRESTANDA

En kraftfull antivirusmotor och optimerad, intelligent skanningsteknik samt belastningsbalansering ökar prestandan och minskar behovet av resurser för viruskanning.

STÖD FÖR FLERA PLATTFORMAR

Kaspersky Security for Internet Gateway har stöd för de flesta populära gatewayer som baseras på Windows- och Linux-plattformar.

COLLABORATION

SPÄRR FÖR SKYDD MOT SKADLIG PROGRAMVARA FÖR SHAREPOINT-SERVERGRUPPER

Här används en ny identifieringsteknik som är utvecklad för att identifiera och blockera skadlig programvara från försök att överföra eller ladda ned filer i realtid.

INNEHÅLLSFILTRERING

Hjälper till att förhindra olämpliga externa överföringar, upprätthåller interna kommunikationspolicyer och blockerar lagring av olämpliga filer per filtyp eller textinnehåll.

KASPERSKY SECURITY FOR MOBILE

Fullständig mobil säkerhet med MDM (Mobile Device Management) och Endpoint Security för mobila enheter.

Med Kaspersky MDM blir säkerhetskonfiguration av mobila enheter smidig och enkel, medan Kaspersky Endpoint Security för mobila enheter har det skydd som behövs mot dagens hot, även på enheter som ägs av den anställde.

DETALJERAD INFORMATION OM FUNKTIONER I KASPERSKY SECURITY FOR MOBILE:

FUNKTIONER FÖR IT-EFFEKTIVITET:

ENKEL KONFIGURATION VIA EN ENDA KONSOL

Till skillnad från andra lösningar har Kaspersky Lab bara en konsol som administratörerna använder för att hantera säkerheten för mobila enheter, fysiska klienter, virtuella system, kryptering och verktyg för policyefterlevnad.

PRIVAT PROGRAMPORTAL

Administratörerna publicerar en företagsportal som innehåller länkar till godkända program. Användare kan begränsas till enbart dessa program.

FJÄRRINSTALLATION (OTA)

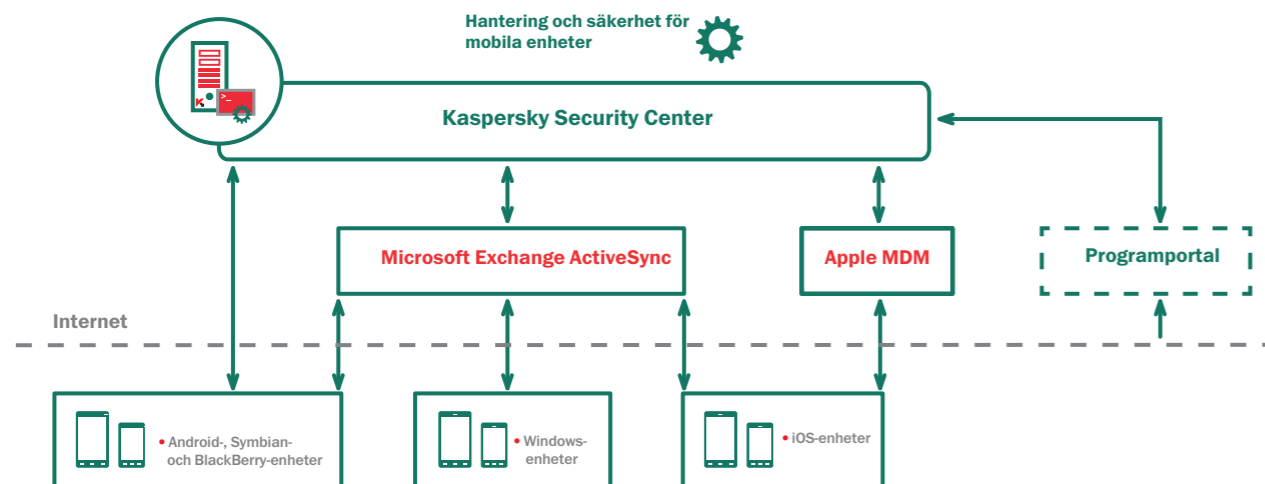
Skyddar fjärranslutna telefoner genom att skicka ett e-postmeddelande eller SMS med en länk till företagsportalen, där användarna kan hämta den profil och godkända program. Åtkomst till data beviljas inte förrän användaren har accepterat.

SÄKER KONFIGURATION

Säkerställer integriteten för maskinvara och programvara genom att aktivera identifiering av rotåtkomst och modifiering. Andra säkerhetsinställningar omfattar bland annat inaktivering av kamera och lösenordstvång.

PROGRAMANVÄNDNING OCH POLICYEFTERLEVAD

Med programkontroll kan programanvändningen övervakas och styras på enheten, bland annat stöd för "Neka som standard" och "Tillåt som standard".



KONTROLL AV SÄKERHETSRISKER:

KRYPTERING

Dataöverföringar skyddas via transparent datakryptering av hel disk och på filnivå, vilken även kan tillämpas på en behållare.

STÖLDSKYDD

Administratörer kan via fjärranslutning utföra en fullständig eller selektiv rensning av en enhet, lokalisera en saknad enhet med hjälp av GPS-sökfunktionen och även få meddelanden när ett SIM-kort tas ur eller byts ut.

SKYDD MOT SKADLIG PROGRAMVARA FÖR MOBILA ENHETER

Kaspersky Labs sökmotor för skydd mot skadlig programvara arbetar med identifiering på flera nivåer och med molnbaserade skyddstekniker. Detta i kombination med en säker webbläsare och ett kraftfullt skräppostskydd säkerställer att enheten inte utsätts för skadlig programvara.

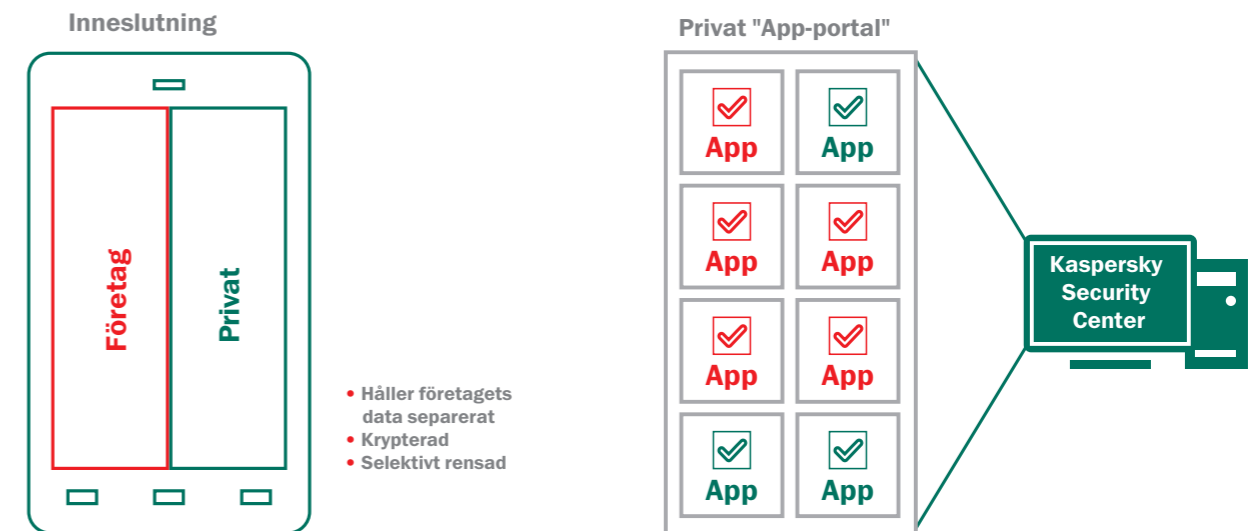
INTEGRITET FÖR FÖRETAGSDATA OCH PRIVATA UPPGIFTER:

CONTAINRAR

I de fall anställda använder egna enheter kan företagsdata och program placeras i isolerade "behållare". Detta ger maximal säkerhet för företagets data och optimal integritet för personligt innehåll.

FJÄRRVERKTYG FÖR DATASÄKERHET

Om en enhet förloras kan fjärrlåset aktiveras. Företagsdata i en behållare på enheten kan säkras och krypteras samt hanteras och rensas via fjärranslutning oberoende av personlig information som finns på enheten.



PERFEKT FÖR LÖSNINGAR DÄR ANSTÄLLDA SKA KUNNA ANVÄNDA PRIVATA ENHETER (BYOD, BRING YOUR OWN DEVICE)

Många anställda använder sina privata enheter för både personliga och arbetsrelaterade ändamål. Vissa företag uppmanar till och med sina anställda att välja en smart telefon eller surfplatta hos en återförsäljare, och därefter förbereder IT-personalen den privatägda enheten för åtkomst till e-post och företagsnätverket.

BYOD ger besparingar och produktivitetsfördelar men kan också innebära att organisationen utsätts för säkerhetsrisker. Företagsdata som inte är korrekt skyddade och som potentiellt lagras tillsammans med privat material kan lätt utnyttjas. Dessa enheter används också ofta av familjemedlemmar som inte tänker på säkerheten vid programanvändning. Vissa enheters säkerhetssystem har rotats eller modifierats.

Kaspersky Security for Mobile löser dessa problem med hjälp av säker konfiguration och distribution för smarta telefoner och surfplattor via samma konsol som företagets nätverkssäkerhetssystem. IT-administratörer kan vara säkra på att användarnas enheter har konfigurerats med de korrekta inställningarna och är skyddade i händelse av förlust, stöld eller oförsiktig användning.

▶ KASPERSKY SYSTEMS MANAGEMENT

Vi introducerar här Kaspersky Systems Management. Den här lösningen erbjuder ett brett utbud av kraftfulla IT-produktionsverktyg som är skrivna i samma kod och hanteras från en enda konsol. Den resulterande plattformen har den önskvärda enkelhet och automatisering du vill ha och uppfyller dina krav på säkerhet och kontroll.

OLIKA IT-VERKTYG SKAPAR KOMPLEXITET OCH KOMPLEXITET ÄR SÄKERHETENS FIENDE.

Undvik duplicering

Eliminera det extra arbete det innebär att konfigurera individuella system för nya och befintliga användare. Med hjälp av tekniker för systeminstallation kan diskavbildningar skapas, hanteras och distribueras från en central plats.

Förbättra säkerheten

Administratörer har berättat för oss att de ägnar mycket tid åt att se till att patchar är aktuella. Kaspersky förenklar arbetet genom att identifiera sårbarheter som skulle kunna utnyttjas omedelbart och vilka patchar som kan skjutas upp till efter kontorstid. Denna prioritering hjälper administratörerna att planera dagen och öka säkerheten.

Arbeta effektivt

Administratörer kan fjärrinstallera avbildningar, uppdateringar, patchar och program. Om en användare har ett problem kan IT-personalen logga in på datorn via fjärranslutning och felsöka systemet. Detta innebär att administratören inte behöver slösa tid på att gå från skrivbord till skrivbord eller ägna frustrerande timmar på telefonsupport.

Dessa funktioner och mycket mer ingår i Kaspersky Systems Management och du får tillgång till dem genom administrationskonsolen Kaspersky Security Center. Eftersom varje verktyg inte kräver en egen konsol är alla kommandon konsekventa och intuitiva, och kräver ingen ytterligare utbildning.

SYSTEMHANTERINGSFUNKTIONER:

INSTALLATION AV OPERATIVSYSTEM OCH PROGRAM

Enkelt att skapa, lagra, kлона och distribuera systemavbildningar från en central plats. Se till att systemen levereras till användaren utan problem och med optimala säkerhetsinställningar. Det här verktyget lämpar sig väl för migrering till Microsoft Windows 8.

BEHÅLL KONTROLLEN ÖVER SÅRBARHETER

Med ett enda klick genomsöker du maskinvara och programvara och resultatet från flera olika sårbarhetsdatabaser jämförs. Du kan därmed prioritera vilka sårbarheter som behöver åtgärdas omedelbart och vilka du kan skjuta upp till efter kontorstid.

FLEXIBEL FJÄRRINSTALLATION AV PROGRAMVARA

Minimera nätverksbelastningen genom att använda antingen manuell eller schemalagd distribution.

FJÄRRAGENTER

Utse en arbetsstation på en extern plats eller ett lokalkontor till central uppdateringsagent. Spara bandbredd genom att skicka en uppdatering till ett fjärrkontor, och använd den tilldelade lokala arbetsstationen för att distribuera uppdateringen på den platsen.

STÖD FÖR WAKE-ON-LAN-TEKNIK

Om distribution eller support ska ske efter arbetstid kan Kaspersky Systems Management fjärrstarta en arbetsstation.

FELSÖKNINGSVERKTYG

Säker fjärranslutning till ett klientsystem för att åtgärda problem – från samma administrationskonsol.

STÖD FÖR MICROSOFT WINDOWS SERVER UPDATE SERVICES (WSUS)

Kaspersky Systems Management synkroniserar regelbundet data för tillgängliga uppdateringar och snabbpatchar med servrar (inklusive Microsoft Windows Update), hämtar dem via Windows Update Services och distribuerar dem effektivt.

NETWORK ADMISSION CONTROL (NAC)

Med Network Admission Control (NAC) kan du skapa en gästpolicy för nätverket. Gästenheter (inklusive mobila enheter) identifieras automatiskt och skickas till en företagsportal där de med hjälp av korrekta inloggningsuppgifter kan användas för godkända resurser.

INVENTERINGAR AV MASKINVARA OCH PROGRAMVARA

Datorer, hårddiskar och även borttagningsbara enheter identifieras automatiskt och inventeras. Om en ny enhet identifieras utlöses ett meddelande till administratören. Den här funktionen gör det möjligt för administratören att följa upp status och användning för maskinvara i nätverket.

INSTALLATION AV LICENSER OCH KONTROLL

Kaspersky Systems Management rapporterar exakt vilka program som används i din miljö. På så sätt kan du justera licenskostnaderna och identifiera användare som inte följer standard. Vid distribution med Kaspersky Labs verktyg för klientskontroll kan du begränsa användningen till endast godkända program och versioner. Du kan när som helst begränsa hur många licenser som används.

► KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server skyddar effektivt servrar med Microsoft® Windows®, Novell NetWare och Linux från alla typer av skadliga program.

Antiviruskydd vid delad fillagring är viktigt eftersom en smittad fil på en server kan smitta arbetsstationerna för alla som använder den resursen. Rätt skydd av filservern skyddar inte bara användare och deras data utan eliminerar även faran med att skadliga program infekterar säkerhetskopior vilket i sin tur kan orsaka upprepade utbrott av infekterad programvara och andra incidenter.

PRODUKTFÖRDELAR*

- Stöd för de senaste versionerna av Microsoft® Windows®- och Linux-plattformarna
- Optimerad användning av systemresurser
- Stöd för HSM (Hierarchical Storage Management)
- Skydd av terminal- och klusterservrar
- VMware Ready-certifiering
- Stöd för NSS-filsystem
- Gratis BSD-stöd

FUNKTIONER

- Skydd av filservrar med Windows® (inklusive Windows Server® 2008 R2), Linux (inklusive Samba) och Novell NetWare
- Utökat förebyggande skydd mot nya skadliga program
- Realtidsskydd mot virus
- Behandling av aktiva infektioner
- Schemalagd skanning av fillager
- Skanning av viktiga systemområden
- Isolering av smittade arbetsstationer
- Skalbarhet
- Säkerhetskopiering av data före desinficering eller radering
- Central installation, hantering och uppdatering
- Val av metoder för installation och hantering
- Flexibelt system för olika scenarier för skanning och incidentsvar
- Meddelandesystem för programstatus
- Omfattande rapporter över status för nätverksskydd

PROGRAM

- 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 variera beroende på vilken kombination av komponenter som används. Mer information om komponentbeskrivningarna och enskilda komponentfunktioner finns på www.kaspersky.com.

► KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server skyddar e-post- och groupware-servrar från skadliga program och skräppost.

Produkten innehåller program som skyddar e-posttrafiken i de vanligaste servrarna, bland annat Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim och CommuniGate Pro. Lösningen kan också användas för att ställa in en speciell gateway för e-post.

PRODUKTFÖRDELAR*

SKYDD FÖR E-POSTSERVER
Skydd mot skadlig programvara och skräppost i e-posttrafik för alla vanliga e-postsystem.

OPTIMERING AV SYSTEMRESURSER
En ny antivirusmotor, belastningsbalansering av serverresurser och skanningexkluderingar minskar belastningen på systemet.

KSN-INTEGRERING FÖR SKYDD MOT SKRÄPPOST
Ökar antalet upptäckta skräppostmeddelanden tack vare integrering med Kaspersky Labs molnbaserade hotidentifieringsmotor (KSN).

MINSKAD TRAFIKBELASTNING
Molnbaserad och intelligent skräppostfiltrering minskar trafikbelastningen.

FUNKTIONER

- Integrerat skydd av e-postservrar från alla typer av skadliga program
- Effektivt skydd mot skräppost
- Realtidsskydd mot virus
- Schemalagd skanning av e-post och databaser
- Skydd för e-postservrarna Sendmail, qmail, Postfix, Exim och CommuniGate Pro
- Skanning av meddelanden, databaser och andra objekt på Lotus® Domino®-servrar
- Skanning av alla meddelanden på Microsoft® Exchange-servrar, bland annat offentliga mappar
- Filtrering av meddelanden efter bilagetyp
- Skalbarhet
- Stöd för Microsoft® Exchange Server 2007-kluster och DAG för Microsoft® Exchange Server 2010
- Säkerhetskopiering av data före desinficering eller radering
- Isolering av smittade objekt
- Annullering av upprepade e-postskanning
- Lättanvända verktyg för installation, hantering och uppdatering
- Omfattande rapporter över skyddsstatus
- Flexibelt system för scenarier för skanning och incidentsvar
- Meddelandesystem för programstatus

PROGRAM

- 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 variera beroende på vilken komponentkombination som används. Mer information om komponentbeskrivningarna och enskilda komponentfunktioner finns på www.kaspersky.com.

► KASPERSKY SECURITY FOR INTERNET GATEWAY

Kaspersky Security for Internet Gateway erbjuder säker internetåtkomst för alla anställda i en organisation.

Kaspersky Security for Internet Gateway har stöd för de flesta populära gatewayer som baseras på Windows- och Linux-plattformar. Kända skadliga och potentiellt farliga program som körs via protokollen HTTP, HTTPS, FTP, POP3 och SMTP tas automatiskt bort från dataflödet. Optimeringsteknik, skalbarhet och stöd för de senaste plattformarna gör den till den perfekta produkten för stora organisationer med mycket stora trafikvolymer.

PRODUKTFÖRDELAR*

- Skydd av Microsoft® Forefront® TMG
- Stort utbud av verktyg för policyhantering och konfiguration
- Skanning av VPN-anslutningar
- Skydd av e-posttrafik (via protokollen POP3 och SMTP)
- Skanning av HTTP- och FTP-trafik från publicerade servrar
- VMware Ready-certifiering

FUNKTIONER

- Skanning i realtid av internettrafiken där protokollen HTTP, HTTPS, FTP, POP3 och SMTP används
- Integrerat skydd mot alla typer av skadlig programvara
- Stöd för proxyservrarna Squid, Blue Coat och Cisco®
- Förvaring av säkerhetskopior
- Belastningsbalansering av serverprocesser
- Skalbarhet
- Lättanvända verktyg för installation, hantering och uppdatering
- Flexibelt system för scenarier för skanning och incidentsvar
- Omfattande rapporter över status för nätverksskydd

PROGRAM

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

*Produktfunktioner kan variera beroende på vilken komponentkombination som används. Mer information om komponentbeskrivningarna och enskilda komponentfunktioner finns på www.kaspersky.com.

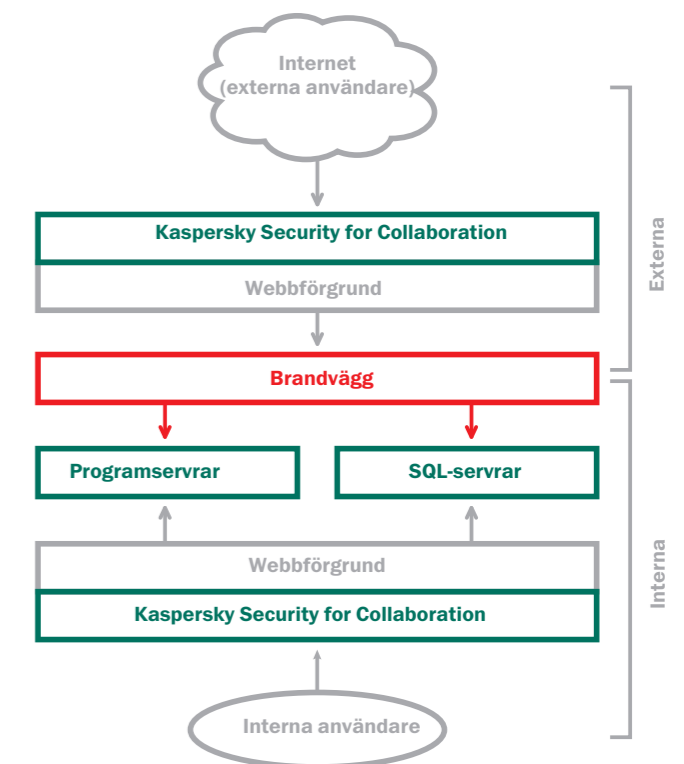
► KASPERSKY SECURITY FOR COLLABORATION

Kaspersky Security for Collaboration använder den senaste skyddstekniken för collaborationplattformar genom att kombinera enkel hantering och höga upptäcktsfrekvenser av skadlig programvara.

I Kaspersky Security for Collaboration används Kasperskys prisbelönta antivirusmotor för att skydda Microsoft® SharePoint®-miljöer. Tack vare den prisbelönta tekniken för identifiering av skadlig programvara kan produkten skydda en enskild server eller hela SharePoint-servergrupper, medan dess funktioner för innehåll och filfiltrering hjälper till att förhindra lagring av olämpligt innehåll.

FUNKTIONER

- Ny identifieringsteknik som är utvecklad för att identifiera och blockera skadlig programvara från att överföra eller ladda ned filer i realtid
- Förhindrar att slutanvändare lagrar speciella filtyper (t.ex. musik, video och körbara filer) eller filer med olämplig text
- Globala hanteringsinställningar kan konfigureras på alla skyddade servrar från en enda infopanel
- Enkel och intuitiv hantering, ingen speciell utbildning krävs
- Integrering med Active Directory effektiviserar installation och användarautentisering
- Detaljerade loggar och säkerhetskopiering av ändrade filer hjälper supportadministratörer att åtgärda störande intrång och säkerhetsproblem
- Detaljerade och flexibla rapporter



*Produktfunktioner kan variera beroende på vilken komponentkombination som används. Mer information om komponentbeskrivningarna och enskilda komponentfunktioner finns på www.kaspersky.com.

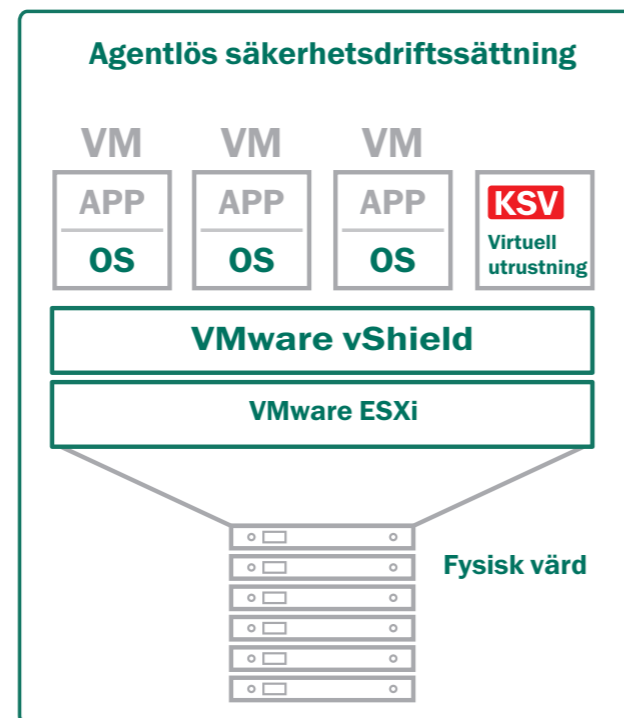
▶ KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization är skapat för de unika kraven som förekommer i virtualiserade IT-miljöer. Det tillhandahåller ett prisbelönt skydd mot skadlig programvara för virtualiserade servrar, stationära datorer och datacenter.

Kaspersky Security for Virtualization är en agentlös lösning som på ett effektivare sätt skyddar virtualiserad infrastruktur mot skadlig programvara med bättre prestanda och mindre påverkan på virtualiseringstäthet. Tillämpningen är lätt att distribuera och innehåller avancerade hanteringsfunktioner som förenklar många olika säkerhetsåtgärder, både när det gäller fysiska och virtuella datortillgångar.

FUNKTIONER FÖR SKYDD OCH PRESTANDA

- **Centraliserad säkerhet.** Kaspersky Security for Virtualization är en virtuell funktion som ansluts till VMwares vShield Endpoint – för att leverera funktioner för sökning efter skadlig programvara. Den tillhandahåller en centraliserad databas och motor för skydd mot skadlig programvara för varje fysisk värd.
- **Avancerad antivirusmotor.** Kasperskys prisbelönta tekniker mot skadlig programvara och Kasperskys branschledande uppdateringsfrekvens, ger bättre skydd mot nya och kommande hot. En heuristisk analysfunktion används för att bekämpa skadliga polymorfa program.
- **Automatiskt skydd.** Nya virtuella datorer skyddas automatiskt mot skadlig programvara, vilket eliminerar säkerhetsluckor och felaktiga konfigurationer. Eventuella gäst-VM:er är alltid skyddade med den senaste signaturdatabasen, oavsett om ett VM tidigare var offline eller inte.
- **Högre täthetsvirtualisering.** Eftersom Kaspersky Security for Virtualization är en agentlös lösning bidrar den till att eliminera "uppdateringsstormar" och "skanningsstormar", ger högre virtualiseringstäthet, minskar påverkan på prestanda och fokuserar på säkerhetsbrister som kan uppstå vid användning av vissa agentbaserade produkter.



Kaspersky Security for Virtualization ger agentlöst antivirusprogram för VMware-distribueringar.

HANTERINGSFUNKTIONER:

EN HANTERINGSKONSOL.

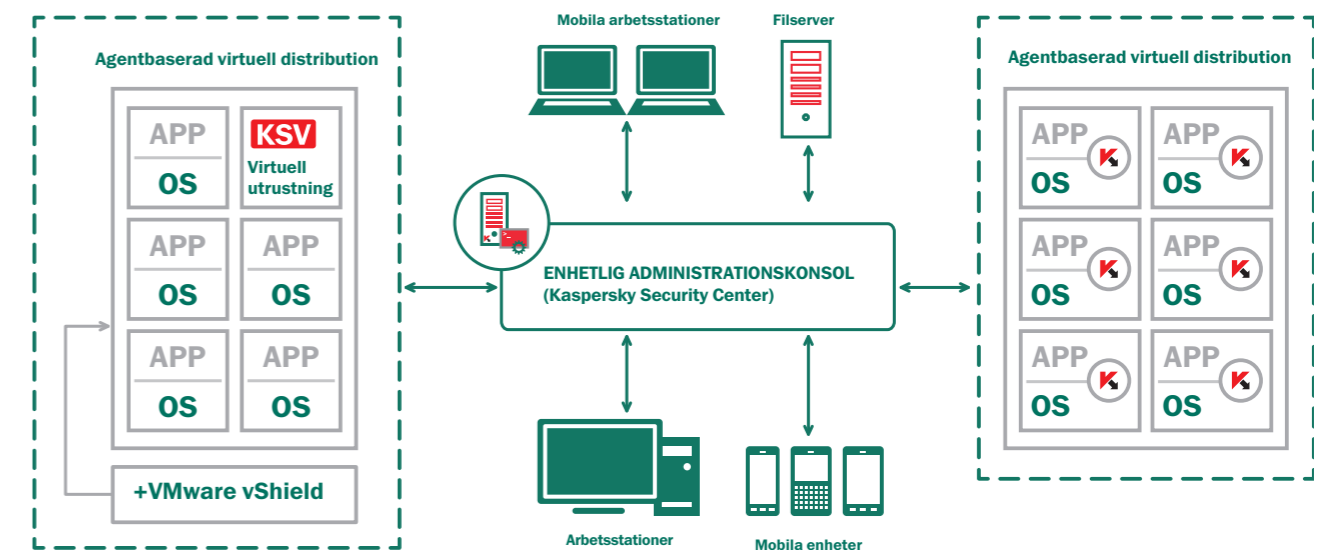
Kaspersky Security Center, som är tillgängligt utan extra kostnad, är en enhetlig hanteringskonsol för hantering av säkerhet i virtuella datorer, fysiska datorer och mobila enheter.

HAR STÖD FÖR VMWARE VMOTION.

Kaspersky Security for Virtualization stöder VMware vMotion fullt ut så att skyddet inte avbryts när en arbetsuppgift flyttas från en ESXi-värd till en annan. Så länge den nya värden har nödvändiga licenser följer skyddet arbetsbelastningen och alla säkerhetsinställningar förblir desamma.

INTEGRERAT MED VMWARE VCENTER.

Kaspersky Security for Virtualization får information om virtuella datorer från vCenter, bland annat en lista över alla virtuella datorer och relevanta parametrar. Förutom att ge IT-gruppen en bättre överblick säkerställer den här integreringen med vCenter att skyddet aktiveras automatiskt när en ny virtuell dator konfigureras.



▶ KASPERSKY ANTI-VIRUS FOR STORAGE

Kaspersky Anti-Virus for Storage skyddar produkter i EMC Celerra-serien av produkter för nätverkslagring från alla typer av skadlig programvara.

Datalagringsystem i ett nätverk ger anställda i organisationer, oavsett organisationsstorlek, snabb och enkel delning av information. Om ett företagsnätverk däremot är oskyddat kan åtkomst till delade filer leda till vissa mycket oönskade konsekvenser. En enskild infekterad fil i ett system kan äventyra hela nätverket och allvarligt skada företaget, dess ekonomi och rykte. Detta är anledningen till att ett omfattande skydd av lagringssystem i nätverk är av yttersta vikt.

Kaspersky Anti-Virus for Storage är helt kompatibelt med hela produktsortimentet för EMC Celerra. Det har speciellt utformats för att ge högsta tänkbara nivå av skydd mot, upptäckt och neutralisering av skadliga program från filer och arkiv som finns lagrade i Celerra-systemen. Lösningen gör det möjligt för administratörer att konfigurera systemet så att skanninguppgifterna utförs i realtid när objekt sparas eller ändras, eller på begäran.

FUNKTIONER

- Skydd för datalagringsystemet EMC Celerra
- Stöd för Windows Server® 2008 R2
- Stöd för HSM (Hierarchical Storage Management)
- Utökat förebyggande skydd mot nya skadliga program
- Realtidsskydd mot virus
- Schemalagd skanning av fillager
- Skanning av viktiga systemområden
- Optimerad användning av systemresurser
- Säkerhetskopiering av data före desinficering eller radering
- Skalbarhet
- VMware Ready-certifiering
- Central installation, hantering och uppdatering med Kaspersky Security Center
- Fullständig integration med Kaspersky Endpoint Security for Business Platform och andra Kaspersky-produkter
- Meddelandesystem för programstatus
- Omfattande rapporter över status för nätverksskydd

Kaspersky Lab AB
Jan Stenbecks Torg 17
164 40 Kista
Sverige
corporatesales@kaspersky.se
www.kaspersky.se

Allt om internetsäkerhet:
www.securelist.com

Hitta en collaborationpartner nära dig:
www.kaspersky.com/buyoffline

© 2013 Kaspersky Lab ZAO. Med ensamrätt. Registrerade varumärken och servicemärken tillhör sina respektive ägare. Mac och Mac OS är registrerade varumärken som tillhör Apple Inc. Cisco är ett registrerat varumärke eller varumärke som tillhör Cisco Systems, Inc. och/eller dess dotterbolag i USA och vissa andra länder. IBM, Lotus och Domino är varumärken som tillhör International Business Machines Corporation, registrerade i många jurisdiktioner världen över. Linux är ett registrerat varumärke som tillhör Linus Torvalds i USA och i andra länder. Microsoft, Windows, Windows Server och Forefront är registrerade varumärken som tillhör Microsoft Corporation i USA och andra länder. Android™ är ett varumärke som tillhör Google, Inc. Varumärket BlackBerry tillhör Research In Motion Limited och är registrerat i USA och kan vara pågående eller registrerat i andra länder.

