



► **PODNIKOVÉ
PRODUKTY
SPOLEČNOSTI
KASPERSKY 2013**

Vidět. Kontrolovat. Chránit.

► O SPOLEČNOSTI KASPERSKY LAB

Společnost Kaspersky Lab je největší nezávislou softwarovou společností na světě. Dodáváme nejlepší možné zabezpečení IT pro vaši organizaci pomocí kombinace výkonné ochrany proti malwaru, flexibilních nástrojů pro kontroly, technologie šifrování a nástrojů pro správu systémů. Zabezpečení společnosti sahá od koncových zařízení vašich serverů a bran, a naše jedinečná integrovaná koncepce znamená, že můžete zabezpečit a kontrolovat všechna svá fyzická zařízení z jediné centrální konzole pro správu bez ohledu na velikost vaší infrastruktury. Technologie společnosti Kaspersky se také používá po celém světě a je integrovaná do produktů a služeb předních výrobců a vydavatelů IT.

Další informace získáte na adrese www.kaspersky.com.

Pro nejnovější záležitosti ohledně antivirů, antispýwaru a další problematiky a trendů v oblasti IT bezpečnosti navštivte www.securelist.com.

▶ JEDINÁ SKUTEČNĚ INTEGROVANÁ BEZPEČNOSTNÍ PLATFORMA NA TRHU

JEDNA KONSOLE

Produkty společnosti Kaspersky jsou navrženy tak, aby administrátor mohl na jednom místě zobrazovat a provádět správu celé bezpečnostní scény — virtuálních i fyzických strojů, stejně jako mobilních zařízení.

JEDNA PLATFORMA

V Kaspersky Lab jsme vlastními silami vyvinuli vlastní konsoli, bezpečnostní moduly a nástroje, místo abychom je pořizovali od jiných společností. Stejní programátoři, kteří vycházeli ze stejného základu kódu, vyvinuli technologie, které si spolu rozumějí — a dobře spolupracují. Výsledkem je stabilita, integrovaná pravidla, praktický reporting a intuitivní nástroje.

JEDNA CENA

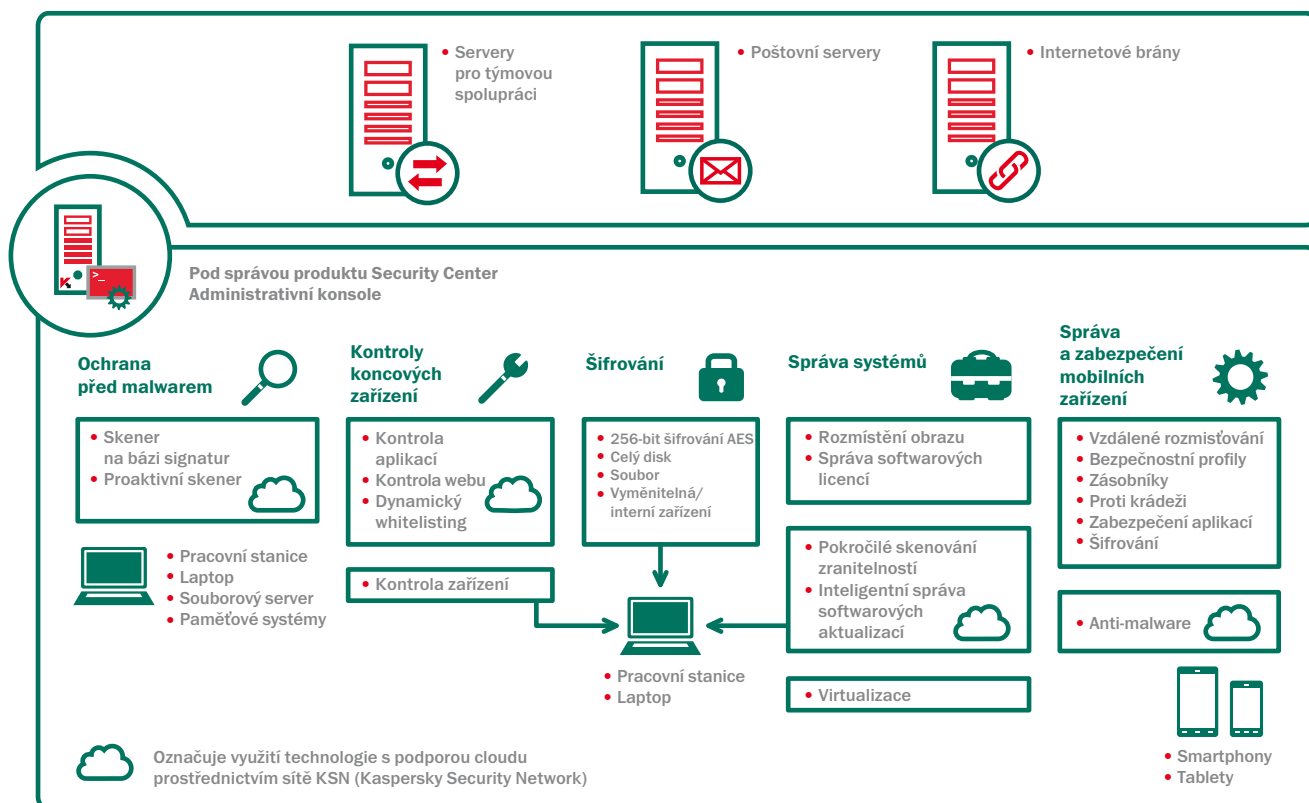
Všechny produkty a nástroje Kaspersky pocházejí od jednoho dodavatele a dodávají se v rámci jedné instalace; nemusíte tak opakovaně procházet proces rozpočtování a zdůvodňování vždy, když chcete zajistit soulad mezi bezpečnostními riziky a vašimi podnikovými cíli.

▶ NEJVHODNĚJŠÍ ŘEŠENÍ PRO VÁS

Produkt Kaspersky Security for Business představuje nejvhodnější řešení pro vaši organizaci bez ohledu na to, zda usilujete o ochranu a kontrolu svých koncových zařízení (počínaje pracovními stanicemi až po smartphony a virtuální stroje) a zabezpečení svých serverů a bran, nebo zda chcete provádět vzdálenou správu celého vašeho bezpečnostního prostředí.

Společnost Kaspersky je právem hrdá na svůj komplexní seznam technologií od šifrování a správy mobilních zařízení až po správu softwarových aktualizací a inventární seznamy licencí. To vše bezpřechodově spolupracuje s podporou sítě KSN (Kaspersky Security Network) na bázi cloudu, aby zákazníkům mohla být poskytnuta ochrana nejvyšší třídy, jakou potřebují pro boj se stále sofistikovanějšími a rozmanitějšími počítačovými hrozbami.

Zkrátka: představili jsme první Bezpečnostní platformu v oboru, kterou jsme od základu vytvořili tak, aby IT administrátorům usnadňovala zobrazování, kontrolu a ochranu celého prostředí.





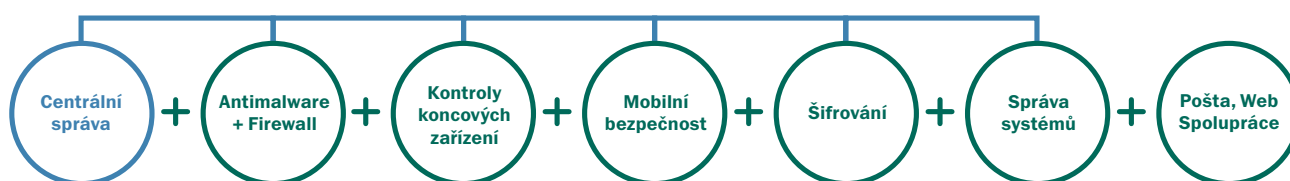


► KASPERSKY SECURITY FOR BUSINESS

Naše technologie a jak
spolupracují ve váš prospěch

	Core	Select	Advanced	Total	Pod správou produktu Security Center	K dispozici v Cíleném řešení
Anti-Malware	•	•	•	•	•	
Firewall	•	•	•	•	•	
Kontrola aplikací		•	•	•	•	
Kontrola zařízení		•	•	•	•	
Kontrola webu		•	•	•	•	
Souborové servery		•	•	•	•	•
Agent pro mobilní koncová zařízení		•	•	•	•	•
Správa mobilních zařízení		•	•	•	•	•
Technologie šifrování			•	•	•	
Správa obrazu operačního systému			•	•	•	•
Správa licencí			•	•	•	•
Řízení zranitelnosti			•	•	•	•
Správa softwarových aktualizací			•	•	•	•
Kontrola přístupu k síti			•	•	•	•
Týmová spolupráce				•		•
Poštovní servery				•		•
Internetové brány				•		•
Virtualizace					•	•
Paměťové systémy					•	•

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS



ÚROVEŇ CORE

K základu, tedy k efektivní a oceňované, jiné než serverové, antimalware technologii a ochrannému firewallu společnosti Kaspersky přidáváme Kaspersky Security Center — naši intuitivní administrativní konsoli. Je to řešení pro zákazníky, kteří chtějí pouze antimalware.

ÚROVEŇ SELECT

Za základ jsme vzali úroveň CORE, kde jsme ochrany rozšířili o **zabezpečení souborového serveru, whitelisting a kontrolu aplikací, kontrolu zařízení a kontrolu webu**. Tato úroveň zahrnuje i řešení pro ochranu mobilních zařízení, které je tvořeno agentem pro kontrolu koncových zařízení a modulem MDM (Mobile Device Management, tj. správa mobilních zařízení). Pokud vaše potřeby zahrnují i ochranu mobilních pracovníků a uplatňování IT pravidel, může být SELECT tou správnou úrovní pro vás.

ÚROVEŇ ADVANCED

Úroveň ADVANCED rozšířila firma Kaspersky o ochranu dat formou **šifrování** souboru nebo celého disku. Další nová nabídka, Kaspersky Systems Management, kombinuje bezpečnost s efektivitou IT. Široká škála funkcí obsahuje základní nástroje, které administrátorovi umožňují:

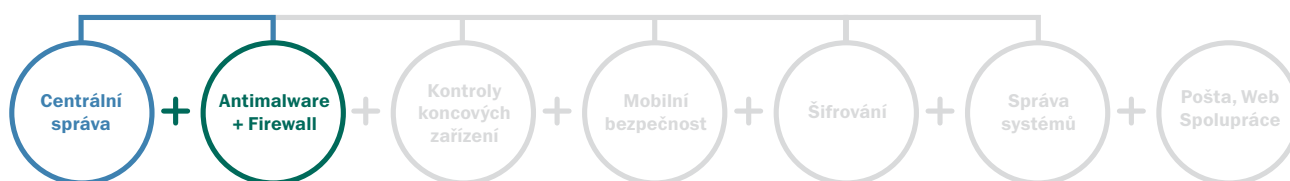
- Rozmísťovat systémy a vytvářet jejich obrazy s použitím modulu Image Management.
- Přidělovat priority ošetření softwarových i hardwarových zranitelností efektivní kombinací pokročilé funkce Vulnerability Scanning (tj. skenování zranitelností) a inteligentní Patch Management (tj. správa softwarových aktualizací).
- Sledovat použití licencí a dodržování předepsaných podmínek s funkcí Software License Management (tj. správa softwarových licencí).
- Nastavovat pravidla pro přístup k datům a infrastrukturám pro uživatele a hosty pomocí funkce NAC (Network Admission Control, tj. kontrola přístupu do sítě).
- Vzdáleně rozmísťovat a instalovat uživatelům aktualizace a nové softwarové produkty z centrální konsoly.

KASPERSKY TOTAL SECURITY FOR BUSINESS

Naše nejvýznamnější nabídka, Kaspersky Total Security for Business, spojuje všechny tři předcházející úrovně a dále rozšiřuje vaši bezpečnostní situaci o další ochranu webu, pošty a Collaboration serveru. Je to perfektní řešení pro organizace s nejvyššími bezpečnostními nároky, které vyžadují nejlepší ochranu pro každou síť.

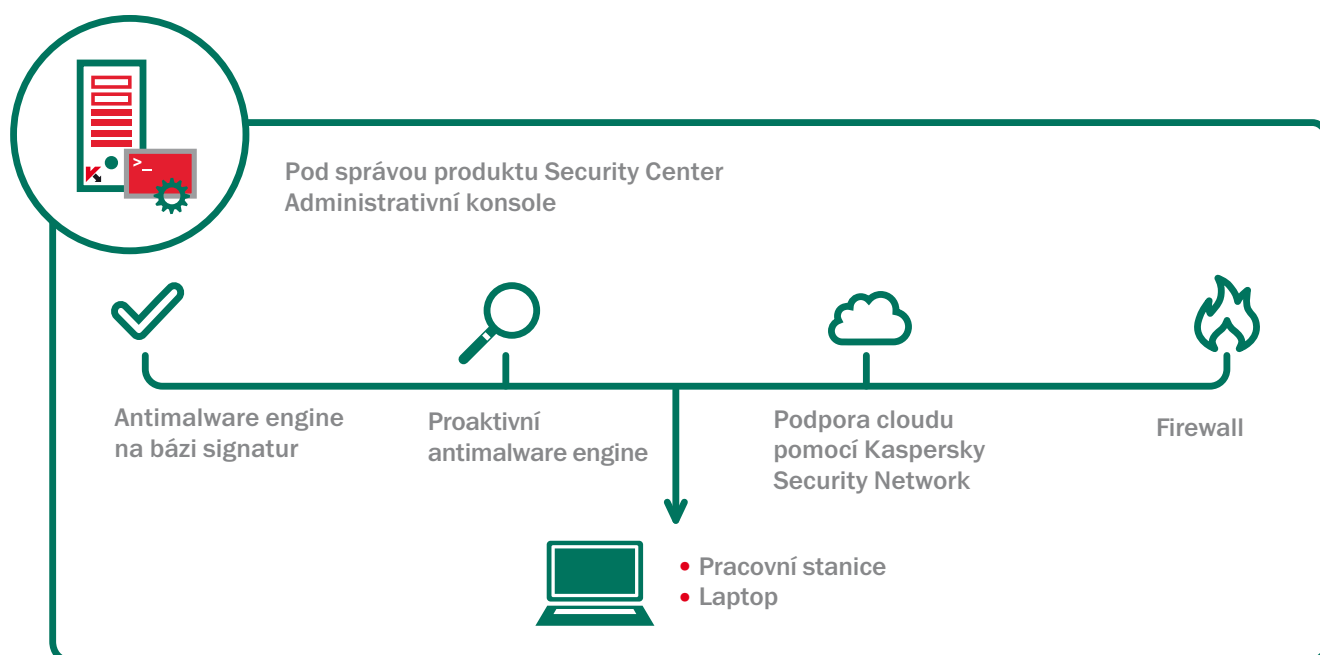
► KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Core



Vysoce hodnocený antimalware s centrálním rozmístováním, správou a reportingem.

Základem vrstveného bezpečnostního modelu je nejlepší antimalware ve své kategorii. A protože společnost Kaspersky je již dlouho uznávaným lídrem v detekci a odstraňování škodlivého softwaru, lepší základ neexistuje. Zabezpečení koncových zařízení (Endpoint Security for Business) úroveň 'Core' od firmy Kaspersky je centrálně spravované pomocí bezpečnostního centra Kaspersky s podporou cloudové sítě KSN.



Kaspersky Endpoint Security for Business úroveň Core — Výkonný antimalware disponující ochranou na bázi cloudu.

HLAVNÍ RYSY:

VÝKONNÝ ANTIMALWARE PRO KONCOVÁ ZAŘÍZENÍ

Skenovací enginy společnosti Kaspersky pracují v operačním systému na více úrovních, aby odstraňovaly malware.

CLOUDEM ZPŘÍSTUPNĚNÁ OCHRANA

Se sítí KSN na bázi cloudu jsou uživatelé chráněni v reálném čase před novými hrozbami.

CENTRÁLNÍ SPRÁVA

Administrátoři mohou centrálně odstraňovat stávající antivirový software, konfigurovat a rozmisťovat produkty Kaspersky a provádět reporting — to vše z jediné konsole.

FUNKCE ANTIMALWARE PRO KONCOVÁ ZAŘÍZENÍ:

ČASTÉ AKTUALIZACE A OCHRANA NA BÁZI SIGNATUR

Praxí ověřená metoda detekování malwarových hrozeb na bázi signatur.

ANALÝZA CHOVÁNÍ PROGRAMŮ POMOCÍ KOMPONENTY SYSTEM WATCHER

Síť KSN (Kaspersky Security Network) představuje daleko rychlejší reakci na podezřelé hrozby než tradiční metody ochrany. Doba odezvy KSN může být pouhých 0,02 sekundy!

SYSTÉM HIPS (HOST-BASED INTRUSION PREVENTION SYSTEM) S OSOBNÍM FIREWALLEM

Předdefinovaná pravidla pro stovky nejběžnější používaných aplikací zkracují dobu nutnou ke konfiguraci firewallu.

PODPORA ŠIROKÉHO SPEKTRA PLATFORM

Firma Kaspersky nabízí ochranu koncových zařízení pro platformy Windows®, Macintosh® a Linux® a snižuje tak pracovní zatížení administrátorů, kteří podporují různé sítě.

FUNKCE KASPERSKY SECURITY CENTER:

JEDNA CENTRÁLNÍ KONSOLE

Pro vzdálenou správu všech koncových zařízení pod ochranou produktů Kaspersky.

INTUITIVNÍ UŽIVATELSKÉ ROZHRANÍ

Zřetelné, prakticky použitelné informace na úsporném dashboardu umožňují administrátorům sledovat status ochrany v reálném čase, nastavovat pravidla, provádět správu systémů a získávat reporty.

ROZHRANÍ WEBOVÉHO PROHLÍZEČE

Vzdáleně monitoruje status ochrany a z dostupného rozhraní informuje o nejvýznamnějších událostech.

ŠKÁLOVATELNÁ PODPORA

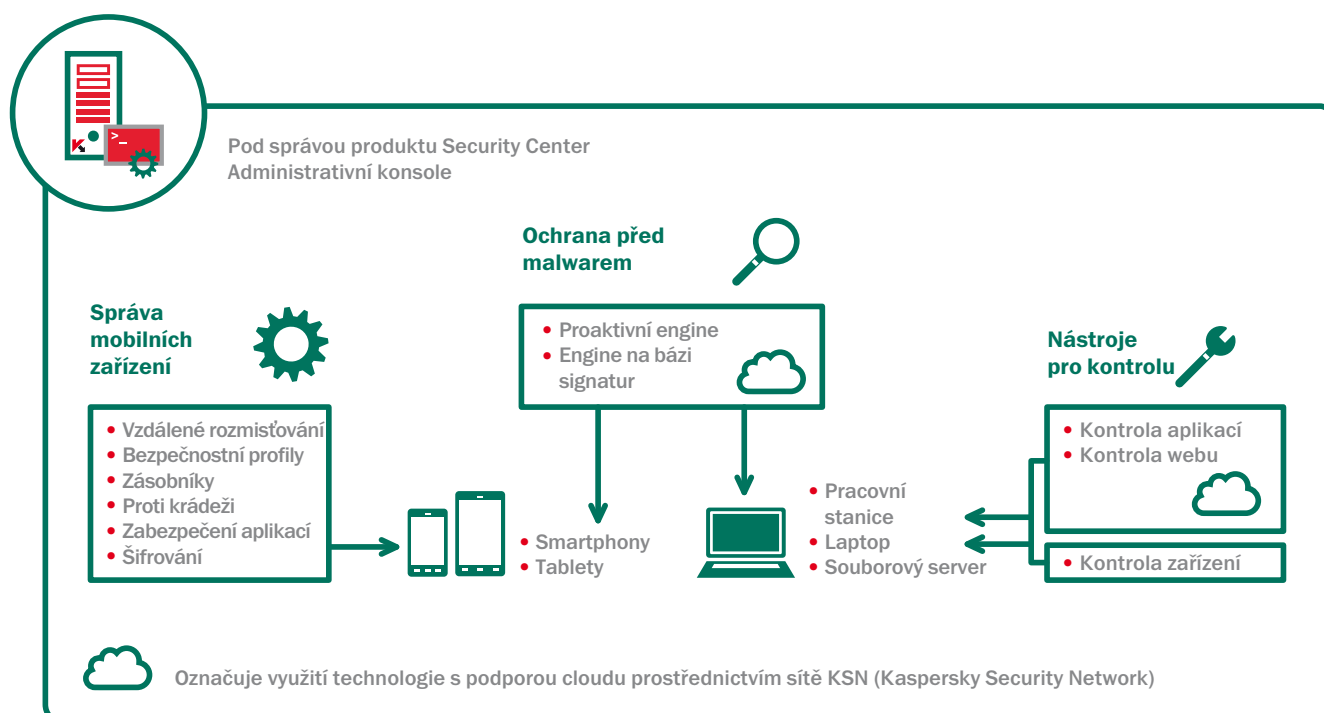
Bez ohledu na rozsah vaší infrastruktury nabízí Kaspersky Security Center nástroje pro konfiguraci, rozmisťování a správu, možnosti flexibilních pravidel a robustní reporting, které uspokojí vaše rostoucí potřeby.

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS Select



Nástroje pro zajištění mobilních pracovníků, zabezpečení conformity pravidel pro IT bezpečnost a blokování malwaru.

Úroveň “Select” zahrnuje nasazení a ochranu mobilních zařízení prostřednictvím komponenty MDM (Mobile Device Management, tj. správa mobilních zařízení) a mobilního antimalwaru. Nástroje pro kontrolu koncových bodů (web, zařízení a aplikace) pomáhají vaší organizaci uplatňovat IT pravidla, a tak zajišťovat bezpečnost základních prvků vašeho IT prostředí.



Kaspersky Endpoint Security for Business — úroveň Select. Představujeme nástroje pro kontrolu a mobilní bezpečnost

HLAVNÍ RYSY:

VÝKONNÝ ANTIMALWARE PRO KONCOVÁ ZAŘÍZENÍ

Skenovací engine firmy Kaspersky - nejlepší ve svém oboru - pracuje na více úrovních operačního systému, odstraňuje malware; cloudová KSN (Kaspersky Security Network) chrání uživatele v reálném čase před novými hrozbami.

FLEXIBILNÍ, GRANULÁRNÍ KONTROLNÍ NÁSTROJE

Cloudová, kategorizovaná databáze bezpečných a nebezpečných aplikací a webů pomáhá administrátorům vytvářet a uplatňovat pravidla pro aplikace a používání webu, zatímco granulární kontroly zajišťují, aby se k počítači na síti směla připojovat pouze určitá zařízení.

EFEKTIVNÍ MOBILNÍ ROZMISŤOVÁNÍ A ZABEZPEČENÍ PRO SMARTPHONY A TABLETY

Pro mobilní zařízení na platformách Android™, BlackBerry®, Symbian a Windows® je k dispozici mobilní zabezpečení na bázi agentů. Pravidla a software pro mobilní zařízení lze na tato zařízení a zařízení se systémem iOS bezdrátově rozmisťovat s pomocí komponenty Kaspersky MDM

V TÉTO ÚROVNI PŘEDSTAVUJEME:

KONTROLY KONCOVÝCH ZAŘÍZENÍ:

KONTROLA APLIKACÍ

Administrátorům IT umožňuje nastavení pravidel, která povolují, blokují nebo regulují aplikace (nebo kategorie aplikací).

KONTROLA ZAŘÍZENÍ

Uživatelům umožňuje plánovat a uplatňovat datová pravidla s vyměnitelnými úložnými zařízeními a kontroly dalších periférií — připojených přes USB nebo jinou sběrnici.

KONTROLA WEBU

Znamená, že plovoucí kontroly koncového zařízení následují uživatele, a to jak v podnikové síti, tak mimo ni.

DYNAMICKÝ WHITELISTING

Reputace souboru poskytované v reálném čase prostřednictvím sítě KSN zajišťují, aby vaše schválené aplikace neobsahovaly malware a tak umožnily maximální produktivitu uživatelů.

KASPERSKY SECURITY FOR MOBILE:

INOVATIVNÍ ANTIMALWAROVÉ TECHNOLOGIE

Výsledkem kombinace cloudu, proaktivní detekce a detekce na bázi signatur je efektivní ochrana v reálném čase. Bezpečný webový prohlížeč a anti-spam zvyšují bezpečnost.

ROZMISŤOVÁNÍ BEZDRÁTOVÝM (OTA, OVER THE AIR) ZAJIŠŤOVÁNÍM

Schopnost centrálně předkonfigurovat a rozmístit aplikace s použitím SMS, e-mailu a PC.

VZDÁLENÉ NÁSTROJE PROTI KRÁDEŽI

Moduly SIM-Watch, rRemote Lock, Wipe a Find zabraňují neoprávněnému přístupu k podnikovým datům v případě ztráty nebo krádeže mobilního zařízení.

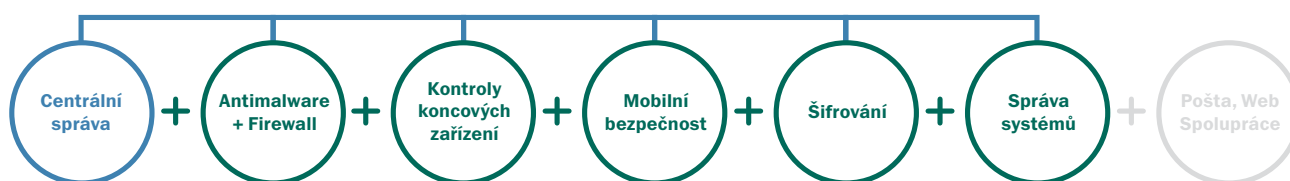
KONTROLA APLIKACÍ PRO MOBILNÍ ZAŘÍZENÍ

Monitoruje aplikace instalované v mobilním zařízení podle předem definovaných skupinových pravidel. Obsahuje skupinu "Povinná aplikace".

PODPORA ZAŘÍZENÍ VE VLASTNICTVÍ ZAMĚSTNANCŮ

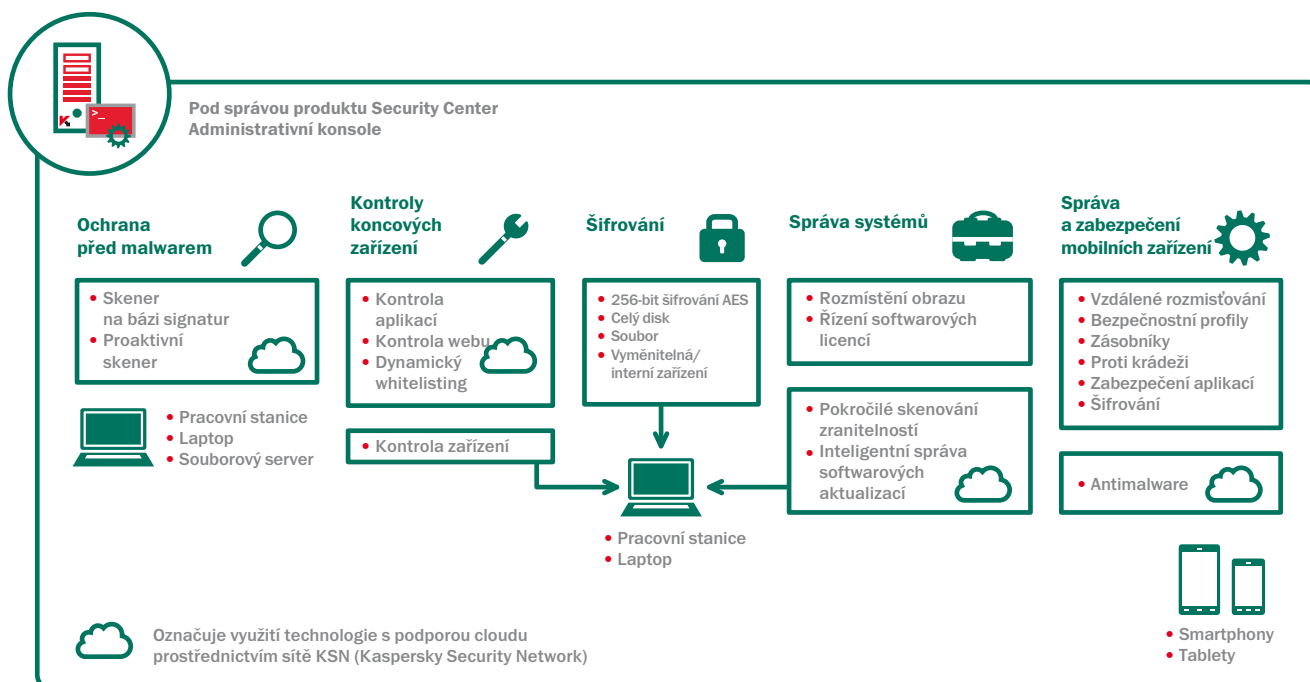
Podniková data a aplikace jsou oddělené v šifrovaných složkách, které jsou pro uživatele transparentní. Tato data lze vymazat samostatně.

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS Advanced



Tento balíček řešení společnosti Kaspersky Lab kombinuje bezpečnostní nástroje s bohatými funkcemi pro optimalizaci IT.

Úroveň Advanced představuje řešení ochrany a správy, jaké vaše organizace potřebuje pro uplatňování IT pravidel a chrání uživatele před malwarem, zabraňuje ztrátám dat a zvyšuje efektivitu IT.



Kaspersky Endpoint Security for Business — úroveň Advanced. Představujeme technologii šifrování a správu zabezpečení systémů.

HLAVNÍ RYSY:

VÝKONNÁ TECHNOLOGIE ŠIFROVÁNÍ

AES 256-bitové šifrování celého disku nebo složky chrání ztracená nebo ukradená data a současně umožňuje sdílení dat prostřednictvím vyměnitelných zařízení, e-mailem, po síti nebo přes web - to vše plně transparentně pro uživatele sítí.

KONFIGURACE SYSTÉMU A SPRÁVA SOFTWAREVÝCH AKTUALIZACÍ

Vytváření a rozmisťování obrazu operačního systému, skenování zranitelností, automatická správa softwarových aktualizací, kontrola přístupu k síti, správa licencí a inventárních seznamů dohromady poskytují plně integrovanou sadu nástrojů ovládanou přes jedinou konsoli s vysokým uživatelským pohodlím.

MOBILNÍ ROZMISŤOVÁNÍ A ZABEZPEČENÍ SMARTPHONŮ A TABLETŮ

Zabezpečení koncových mobilních zařízení s pomocí agentů a vzdálená správa zařízení a softwaru prostřednictvím komponenty Kaspersky MDM.

VÝKONNÝ ANTIMALWARE PRO KONCOVÁ ZAŘÍZENÍ A FLEXIBILNÍ KONTROLY

Antimalware firmy Kaspersky - nejlepší svého druhu - a granulární aplikace s nástroji pro kontrolu zařízení a webů.

V TÉTO ÚROVNI PŘEDSTAVUJEME:

ŠIFROVÁNÍ A OCHRANA DAT:

KOMPLEXNÍ ŠIFROVÁNÍ

Pro zabezpečení životně důležitých obchodních informací v případě ztráty nebo krádeže zařízení se můžete rozhodnout mezi šifrováním celého disku nebo jednotlivých souborů; 256-bitové šifrování podporuje standard AES (Advanced Encryption Standard, tj. standard pokročilého šifrování).

BEZPEČNÉ SDÍLENÍ DAT

Vytvořením šifrovaných a samorozbalovacích balíčků zajistíte ochranu dat při sdílení prostřednictvím výměnných zařízení, pomocí e-mailů, po síti nebo na webu.

PODPORA VÝMĚNNÝCH ZAŘÍZENÍ

Zvyšuje vaši bezpečnost prostřednictvím pravidel, které uplatňují šifrování dat na výměnných zařízeních.

TRANSPARENTNOST PRO KONCOVÉ UŽIVATELE

Řešení šifrování společnosti Kaspersky je zcela bezpřechodové a pro uživatele neviditelné, navíc nemá nepříznivý dopad na produktivitu, ani na nastavení aplikací nebo aktualizací.

KONFIGURACE SYSTÉMU A SPRÁVA SOFTWAREVÝCH AKTUALIZACÍ:

SPRÁVA SOFTWAREVÝCH AKTUALIZACÍ

Pokročilé hloubkové skenování zranitelností kombinované s automatickou distribucí softwarových aktualizací.

ROZMISŤOVÁNÍ OBRAZŮ OPERAČNÍHO SYSTÉMU A APLIKACÍ

Snadné vytváření, ukládání a rozmisťování obrazů systému z centrálního úložiště. Skvělé pro migraci na Microsoft® Windows® 8.

VZDÁLENÉ ROZMISŤOVÁNÍ SOFTWARE

Centrální rozmisťování softwaru na klientské stroje, dokonce i na pobočkách.

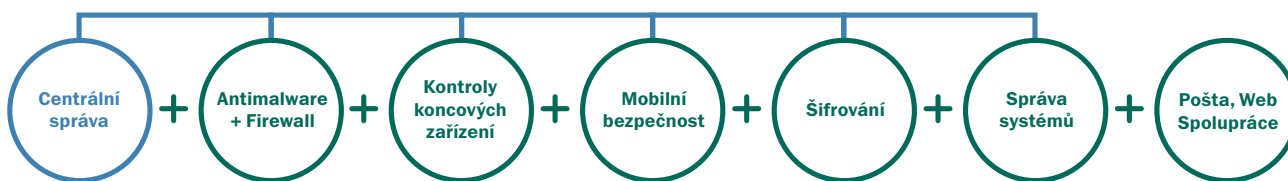
KONTROLA PŘÍSTUPU K SÍTI (NAC)

S kontrolou přístupu k síti (Network Admission Control, NAC) můžete vytvářet pravidla pro 'hosty' v síti. Zařízení hostů (včetně mobilních zařízení) jsou automaticky rozpoznána a odeslána na podnikový portál, odkud jim správné identifikační heslo umožní využívat zdroje, které jste povolili.

KONTROLY HARDWARU, SOFTWARE A LICENCÍ

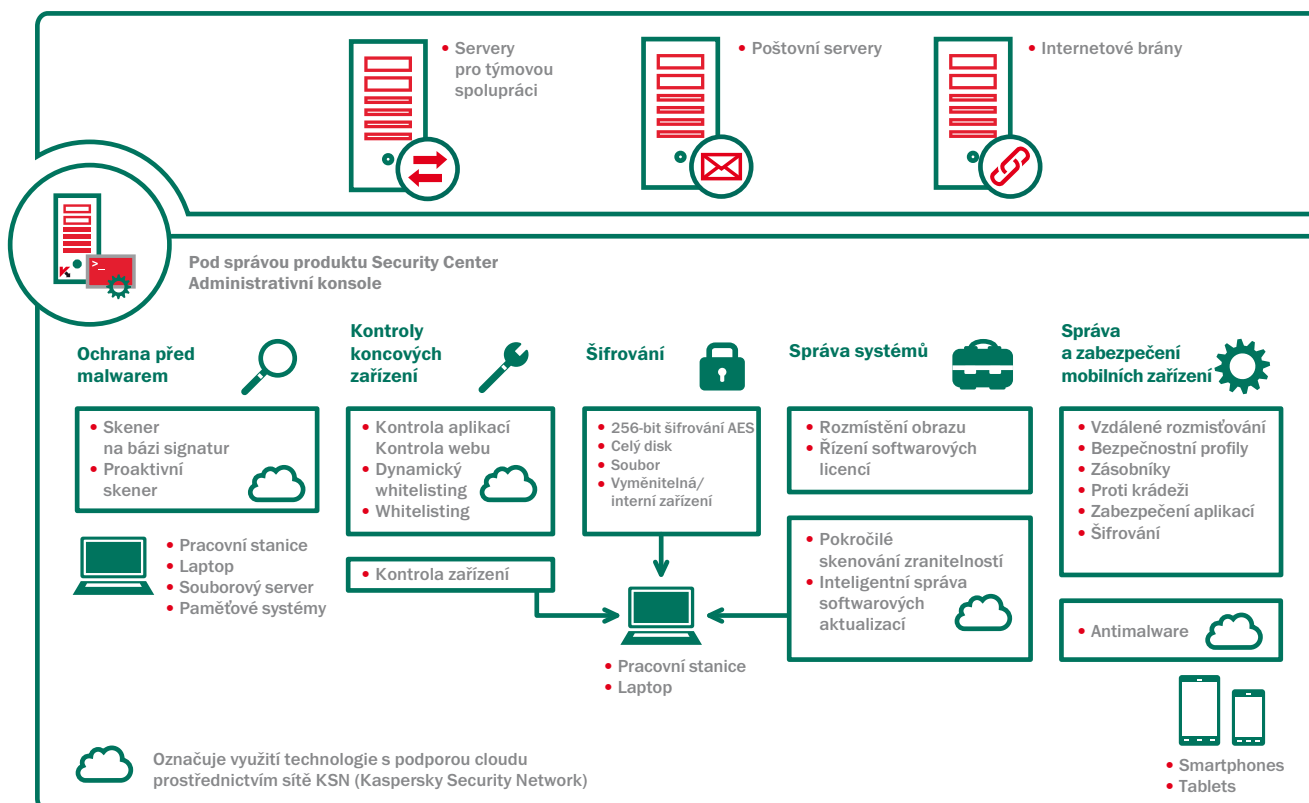
Inventární seznamy hardwaru a softwaru pomáhají k udržení kontroly nad povinnostmi, které vyplývají ze závazků softwarových licencí. Tak můžete centrálním zajišťováním práv k softwaru výrazně ušetřit na nákladech.

► KASPERSKY TOTAL SECURITY FOR BUSINESS



Komplexní ochrana před malwarem; nástroje pro šifrování, zvýšení efektivity IT a uplatnění pravidel.

Kaspersky Total Security for Business představuje nejkompletnější platformu pro ochranu a správu, která je v současné době na trhu. Total Security for Business zajišťuje bezpečnost každé vrstvy vaší sítě a zahrnuje efektivní nástroje pro konfiguraci. Tím zajišťuje produktivitu vašich zaměstnanců a zbavuje je hrozeb malwaru bez ohledu na použité zařízení nebo umístění.



HLAVNÍ RYSY:

Všechny funkce předcházející úrovně plus:

OCHRANA POŠTOVNÍHO SERVERU.

Anti-malware and anti-spam protection of mail traffic for all popular mail systems

ZABEZPEČENÍ INTERNETOVÝCH BRAN

Zajišťuje bezpečný přístup k internetu v rámci celé organizace tím, že automaticky odstraňuje škodlivé a potenciálně nepřátelské programy v provozu HTTP(S)/FTP/SMTP a POP3.

ZABEZPEČENÍ TÝMOVÉ SPOLUPRÁCE

Firma Kaspersky chrání vaše servery SharePoint® před malwarem, zatímco funkce pro filtrování obsahu a souborů pomáhají zabránit ukládání nevhodného obsahu.

TATO ÚROVEŇ OBSAHUJE:

POŠTOVNÍ SERVERY:

OCHRANA POŠTOVNÍHO PROVOZU

Ochrana pošty na nejnovějších verzích hlavních platforem pro poštu a týmovou spolupráci: Microsoft Exchange, IBM Lotus Domino a poštovní servery na Linuxu.

INTEGRACE KSN PRO ANTISPAM

Zvyšuje míru rozpoznání spamu díky integraci s cloudovým enginem firmy Kaspersky Lab pro identifikaci spamových hrozeb (KSN).

SNIŽUJE PROVOZNÍ ZATÍŽENÍ

Inteligentní filtrování spamu s podporou cloudu významně snižuje provozní zatížení.

OPTIMALIZACE SYSTÉMOVÝCH ZDROJŮ

Nový antivirový engine, vyvznávání zátěže na procesorech serveru a skenování výjimek snižují provozní zatížení systému.

INTERNETOVÉ BRÁNY:

VYSOKÝ VÝKON

Výkonný antivirový engine plus optimalizovaná skenovací technologie a vyvažování pracovní zátěže zvyšují výkon a snižují zdroje nutné pro skenování virů.

PODPORA VÍCE PLATFOREM

Produkt Kaspersky Security for Internet Gateway podporuje nejoblíbenější brány na platformách Windows a Linux.

TÝMOVÁ SPOLUPRÁCE:

ZÁBRANA PROTI MALWARU PRO FARMY SHAREPOINT SERVERŮ

Využívá inovativní technologie rozpoznání pro identifikaci a blokování malwaru v reálném čase při pokusech o stahování nebo uploadování.

FILTROVÁNÍ OBSAHU

Pomáhá zabránit nevhodným externím uploadům, uplatňuje interní pravidla pro komunikaci a blokuje ukládání nevhodných souborů podle obsahu nebo typu souboru.



► KASPERSKY ANTI-VIRUS FOR STORAGE

Produkt Kaspersky Anti-Virus for Storage zajišťuje ochranu produktů síťových úložných systémů řady EMC Celerra před všemi typy malwaru.

Síťové systémy pro ukládání dat poskytují pracovníkům organizací všech velikostí rychlý přístup k informacím a jejich snadné sdílení. Pokud však podniková síť není chráněna, přístup ke sdíleným souborům může vést k některým zcela nežádoucím následkům. Jediný infikovaný soubor uložený v systému může ohrozit celou síť a potenciálně způsobit závažné obchodní a finanční škody, nehledě na poškození důvěryhodnosti podniku. Proto je komplexní ochrana síťových úložných systémů absolutně nevyhnutelná.

Produkt Kaspersky Anti-Virus for Storage je plně kompatibilní s produkty řady EMC Celerra. Byl odborně navržen tak, aby jim poskytoval nejvyšší úroveň ochrany, detekoval a neutralizoval malware ze souborů a archivů uložených v systémech Celerra. Toto řešení umožňuje administrátorům konfigurovat systém tak, aby prováděl skenování v reálném čase, kdy jsou objekty ukládány a upravovány, nebo v případě potřeby na požádání.

FUNKCE

- Ochrana systémů pro ukládání dat EMC Celerra
- Podpora pro Windows Server® 2008 R2
- Podpora pro systémy správy hierarchických úložišť (Hierarchical Storage Management, HSM)
- Rozšířená proaktivní ochrana před novými škodlivými programy
- Antivirová ochrana v reálném čase
- Plánované skenování datového úložiště
- Skenování kritických systémových oblastí
- Optimalizované využívání systémových zdrojů
- Zálohování úložného prostoru před desinfekcí nebo odstraněním dat
- Škálovatelnost
- Certifikace VMware Ready
- Centrální instalace, správa a aktualizace pomocí Kaspersky Security Center
- Plná slučitelnost s platformou Kaspersky Endpoint Security for Business a dalšími produkty společnosti Kaspersky
- Systém notifikací o statusu aplikací
- Komplexní reporty o statusu ochrany sítě

► KASPERSKY SECURITY FOR MOBILE

Kompletní mobilní zabezpečení kombinující komponenty Mobile Device Management (MDM) a Endpoint Security for Mobile Devices.

Díky Kaspersky MDM je bezpečná konfigurace mobilních zařízení jednoduchá a bezproblémová, přičemž Kaspersky Endpoint Security for Mobile Devices zajišťuje ochranu, kterou před současnými hrozbami potřebujete, a to dokonce i na vlastních zařízeních zaměstnanců.

SEZNAM FUNKCÍ PRODUKTU KASPERSKY SECURITY FOR MOBILE:

FUNKCE PRO ZAJIŠTĚNÍ IT EFEKTIVITU:

JEDNODUCHÁ KONFIGURACE PROSTŘEDNICTVÍM JEDNÉ KONSOLE

Na rozdíl od dalších řešení Kaspersky Lab umožňuje administrátorům používat pouze jednu konsoli pro správu zabezpečení mobilních zařízení, fyzických koncových zařízení, virtuálních systémů, šifrování a nástrojů pro uplatňování pravidel.

PRIVÁTNÍ PORTÁL APLIKACÍ

Administrátoři publikují podnikový portál, který obsahuje odkazy na schválené aplikace. Uživatelé lze omezit na použití pouze těchto aplikací.

BEZDRÁTOVÉ POSKYTOVÁNÍ OTA (“OVER THE AIR”)

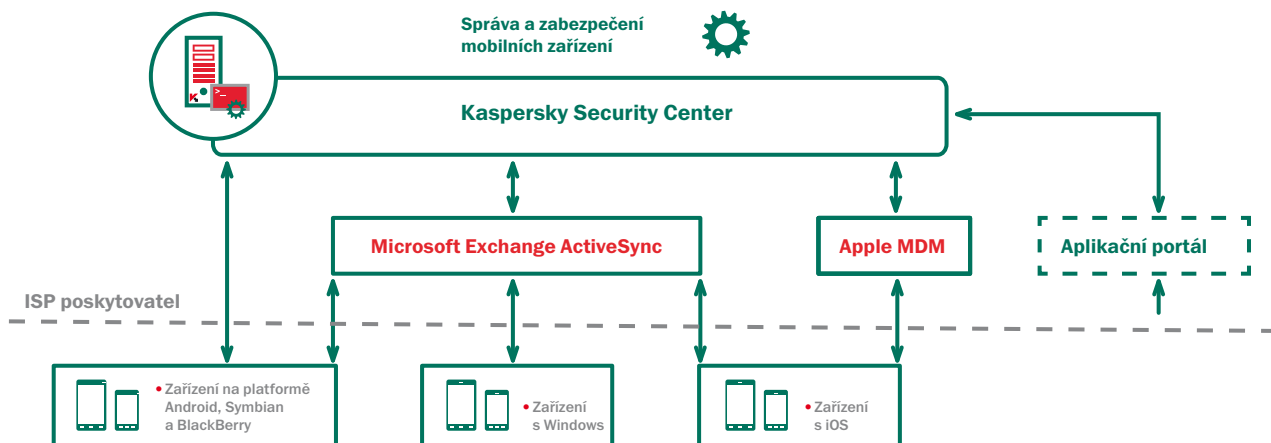
Vzdáleně zabezpečuje telefony buď odesláním e-mailu nebo SMS s odkazem na podnikový portál, kde uživatelé mohou stahovat profil a vámi schválené aplikace. Přístup k datům nebude udělen, dokud je uživatel nepřijme.

BEZPEČNÁ KONFIGURACE

Zajišťuje softwarovou i hardwarovou integritu tím, že umožňuje detekci rootingu a jailbreaku. Mezi další bezpečnostní nastavení patří deaktivace kamery ('camera disable'), vynucené heslo a další.

UPLATŇOVÁNÍ DODRŽOVÁNÍ PRAVIDEL A PŘEDEPSANÝCH NÁLEŽITOSTÍ

Kontrola aplikací umožňuje monitorování a kontrolu používání aplikací na zařízení včetně podpory 'Default Deny' (tj. implicitně odmítnout) a 'Default Allow' (tj. implicitně povolit).



KONTROLA BEZPEČNOSTNÍCH RIZIK:

ŠIFROVÁNÍ

Mobilní data jsou chráněna buď jako celý disk nebo na úrovni souborů prostřednictvím transparentního šifrování, které lze také použít na zásobník.

PROTI KRÁDEŽI

Administrátoři mohou vzdáleně provádět plné nebo selektivní čištění zařízení, označit umístění chybějícího zařízení s hledáním pomocí GPS a získat informaci, zda došlo k odstranění nebo výměně SIM karty.

MOBILNÍ ANTIMALWARE

Antimalware engine společnosti Kaspersky Lab disponuje více úrovněmi detekce včetně ochrany s podporou cloudu a v kombinaci s bezpečným prohlížečem a výkonným antispamem zajišťuje, aby nedošlo k ohrožení zařízení škodlivým softwarem.

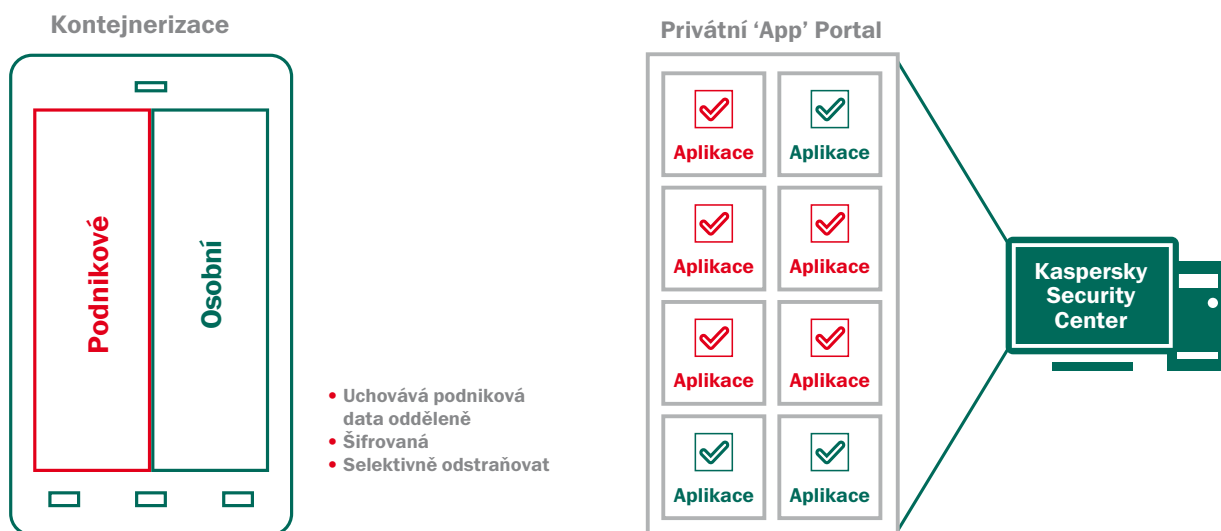
INTEGRITA PODNIKOVÝCH A OSOBNÍCH DAT:

ZÁSOBNÍKY

Pro podporu scénářů vlastních zařízení zaměstnanců lze podniková data a data aplikací umístit do samostatných zásobníků. Tím je zajištěna maximální bezpečnost pro podniková data a optimální integrita pro osobní obsah.

NÁSTROJE PRO BEZPEČNOST VZDÁLENÝCH DAT

V případě ztráty zařízení lze použít funkci Remote Lock (tj. vzdálený zámek). Podniková data v zásobníku na zařízení lze zabezpečit, šifrovat, provádět vzdáleně jejich správu a odstraňovat je nezávisle na osobních datech na daném zařízení.



SKVĚLÉ PRO INICIATIVY BYOD (“BRING YOUR OWN DEVICE”, TJ. PŘINESTE SI VLASTNÍ ZAŘÍZENÍ)

Řada zaměstnanců používá vlastní zařízení pro osobní i podnikové úkoly. Některé organizace dokonce podporují, aby si jejich zaměstnanci vybrali jimi preferované smartphony nebo tablety v obchodě a IT oddělení zajistí přístup k e-mailům a podnikovým datům z tohoto zařízení pracovníka.

Představuje to úspory a přínosy produktivity, ale tento přístup také může vystavit podnik bezpečnostním rizikům. Podniková data, nevhodně zabezpečená a potenciálně promíchaná s osobními položkami, lze snadno zneužít. Taková zařízení také bývají často používána členy rodiny, kteří nemají ponětí o zabezpečení aplikací. Některá zařízení jsou dokonce rootovaná nebo je na nich proveden jailbreak.

Kaspersky Security for Mobile řeší tyto problémy tím, že umožňuje bezpečnou konfiguraci a nasazování smartphonů a tabletů s použitím stejné konzole, jako pro zabezpečení vaší sítě. Administrátoři IT si pak mohou být jisti, že uživatelská zařízení jsou konfigurovaná se správným nastavením, a že je lze zabezpečit pro případ ztráty, krádeže nebo zneužití.

► KASPERSKY SYSTEMS MANAGEMENT

Představujeme Kaspersky Systems Management. Toto řešení nabízí širokou škálu výkonných nástrojů pro zvýšení IT produktivity, vytvořených na bázi stejného kódu a spravované z jedné konzole. Výsledná platforma poskytuje tolik žádanou jednoduchost a automatizaci — a samozřejmě potřebnou bezpečnost a kontrolu.

RŮZNORODÉ IT NÁSTROJE ZPŮSOBUJÍ SLOŽITOST — A SLOŽITOST JE NEPŘÍTELEM BEZPEČNOSTI.

Zabraňte duplicitě

Odstraňte duplicitní úsilí, související s vytvořením samostatných systémů pro nové i stávající uživatele. S využitím systému zajišťování technologie lze obrazy disků vytvářet, rozmisťovat a provádět jejich správu z jednoho místa.

Zvyšte bezpečnost

Administrátoři nám říkají, že jejich dny jsou často naplněné tím, že zajišťují aktuálnost softwarových aktualizací. Společnost Kaspersky pomáhá odstraňovat tuto složitost tím, že identifikuje zranitelnosti, které mohou být okamžitě zneužity, a opravy, které lze odložit na později. Takové přidělování priorit pomáhá administrátorům plánovat si svůj čas a zvyšuje jejich bezpečnostní situaci.

Pracujte efektivně

Administrátoři mohou vzdáleně instalovat obrazy systému, aktualizace, softwarové záplaty a aplikace. Pokud se uživatel setká s problémem, může se IT vzdáleně přihlásit do jeho stroje a chybu odstranit. To znamená, že administrátor neztrácí čas běháním od stolu ke stolu, ani nemarní čas poskytováním méně produktivní telefonní podpory.

Tyto a další funkce jsou součástí produktu Kaspersky Systems Management a přistupuje se k nim z administrativní konzole Kaspersky Security Center. A protože to není tak, že by každý nástroj vyžadoval vlastní konsoli, jsou příkazy konzistentní a intuitivní a nevyžadují další školení.

FUNKCE PRO SPRÁVU SYSTÉMU:

ZAJIŠŤOVÁNÍ OPERAČNÍHO SYSTÉMU A APLIKACÍ

Snadné vytváření, ukládání, klonování a rozmisťování obrazů systému z centrálního úložiště. Zajišťuje, že systémy jsou uživateli dodávány bez problémů a s optimálním nastavením bezpečnosti. Tento nástroj je vhodný pro migraci na Microsoft Windows 8.

MĚJTE PŘEVAHU NAD ZRANITELNOSTMI

Skenování hardwaru a softwaru, spouštěné jedním kliknutím, porovnává výsledky s několika databázemi zranitelností, takže můžete stanovit pořadí důležitosti a určit, které zranitelnosti vyžadují pozornost neprodleně, a které lze odložit na později.

VZDÁLENÁ, FLEXIBILNÍ INSTALACE SOFTWARE

Minimalizujte pracovní zatížení sítě použitím ručního nebo plánovaného rozmisťování.

VZDÁLENÍ AGENTI

Přiřadte pracovní stanici na vzdáleném pracovišti nebo pobočce jako agenta pro centrální aktualizace. Ušetřete přenosové pásmo tím, že do vzdáleného pracoviště pošlete jednu aktualizaci — a použijete přiřazenou místní pracovní stanici pro distribuci aktualizace pro tuto lokalitu.

PODPORA TECHNOLOGIE WAKE-ON-LAN

Pro nasazení nebo technickou podporu v mimopracovní době může Kaspersky Systems Management vzdáleně zapínat pracovní stanice.

NÁSTROJE PRO ODSTRAŇOVÁNÍ ZÁVAD

Připojte se vzdáleně a bezpečně ke klientskému systému pro opravu závad — z jedné administrativní konzole.

PODPORA SLUŽBY MICROSOFT WSUS (WINDOWS SERVER UPDATE SERVICES)

Kaspersky Systems Management pravidelně synchronizuje data, co se týče dostupných aktualizací a záplat se servery, včetně aktualizací Microsoft Windows, stahuje je prostřednictvím služby Windows Update a efektivně je distribuuje.

KONTROLA PŘÍSTUPU K SÍTÍ (NAC)

S kontrolou přístupu k síti (Network Admission Control, NAC) můžete vytvářet pravidla pro 'hosty' v síti. Zařízení hostů (včetně mobilních zařízení) se automaticky rozpoznají a jsou odeslána na podnikový portál, odkud jim správné přihlašovací údaje umožní využívat zdroje, které jste povolili.

INVENTÁRNÍ SEZNAMY SOFTWARE A HARDWARU

Počítače, pevné disky a dokonce i vyměnitelná zařízení jsou automaticky odhalena a registrována. Zavedení nových zařízení spouští oznámení administrátorům. Tato funkce umožňuje administrátorům sledovat status a využití hardwaru na síti.

ZAJIŠŤOVÁNÍ A KONTROLA LICENCÍ

Kaspersky Systems Management hlásí přesně software, který je ve vašem prostředí používán. Tím umožňuje upravit vaše licenční náklady a identifikovat uživatele, kteří nedodržují předepsané náležitosti. Po nasazení nástrojů pro kontrolu koncových zařízení společnosti Kaspersky Lab můžete omezit používání pouze na schválené aplikace a verze - a omezit počet současně používaných licencí.

► KASPERSKY SECURITY FOR FILE SERVER

Kaspersky Security for File Server spolehlivě chrání servery pracující pod systémy Microsoft® Windows®, Novell NetWare a Linux před všemi typy škodlivých programů.

Antivirová ochrana sdíleného úložiště souborů je životně důležitá, protože jeden infikovaný soubor může infikovat pracovní stanice všech uživatelů daného zdroje. Správná ochrana souborového serveru zajišťuje, aby byli uživatelé a jejich data chráněni, ale také snižuje nebezpečí, že se škodlivé programy dostanou do záložních kopií souborů, protože to by mohlo způsobit opakované epidemie malwaru a další incidenty.

NEJVÝZNAMNĚJŠÍ RYSY PRODUKTU*

- Podporuje nejnovější verze platform Microsoft® Windows® a Linux
- Optimalizované využívání systémových zdrojů
- Podpora systémů správy hierarchických úložišť (Hierarchical Storage Management, HSM)
- Ochrana terinátových a clusterovaných serverů
- Certifikace VMware Ready
- Podpora souborového systému NSS
- Bezplatná podpora BSD

FUNKCE

- Ochrana souborových serverů pod Windows® (včetně Windows Server® 2008 R2), Linux (including Samba) nebo Novell NetWare
- Rozšířená proaktivní ochrana před novými škodlivými programy
- Antivirová ochrana v reálném čase
- Ošetření aktivních infekcí
- Plánované skenování datového úložiště
- Skenování kritických systémových oblastí
- Izolování infikovaných pracovních stanic
- Škálovatelnost
- Zálohování úložného prostoru před desinfekcí nebo odstraněním dat
- Centrální instalace, správa a aktualizace
- Volba metod instalace a správy
- Flexibilní systém skenování a scénářů v reakci na incidenty
- Systém notifikací o statusu aplikací
- Komplexní reporty o statusu ochrany sítě

APLIKACE

- 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

*Funkce produktu se mohou lišit v závislosti na kombinaci použitých komponent. Popis jednotlivých komponent viz www.kaspersky.com, kde najdete podrobnější informace o funkcích jednotlivých komponent.

► KASPERSKY SECURITY FOR MAIL SERVER

Kaspersky Security for Mail Server chrání poštovní servery a servery pro týmovou spolupráci před škodlivými programy a spamy.

Tento produkt obsahuje aplikace, které chrání poštovní provoz všech oblíbených serverů, včetně Microsoft® Exchange, Lotus® Domino®, Sendmail, Qmail, Postfix, Exim a CommuniGate Pro. Toto řešení lze použít i pro vytvoření dedikované poštovní brány.

NEJVÝZNAMNĚJŠÍ RYSY PRODUKTU*

OCHRANA POŠTOVNÍHO SERVERU.

Ochrana poštovního provozu před malwarem a spamem pro všechny oblíbené poštovní systémy.

OPTIMALIZACE SYSTÉMOVÝCH ZDROJŮ

Nový antivirový engine, vyrovnávání zátěže na procesorech serveru a skenování výjimek snižují provozní zatížení systému.

INTEGRACE KSN PRO ANTISPAM

Zvyšuje míru rozpoznání spamu díky integraci s cloudovým engine firmy Kaspersky Lab pro identifikaci spamových hrozeb (KSN).

SNIŽUJE PROVOZNÍ ZATÍŽENÍ

Inteligentní filtrování spamu s podporou cloudu významně snižuje provozní zatížení.

FUNKCE

- Integrovaná ochrana poštovních serverů před všemi typy škodlivých programů
- Efektivní ochrana před spamem
- Antivirová ochrana v reálném čase
- Skenování e-mailů a databází podle časového plánu
- Ochrana pro poštovní servery Sendmail, Qmail, Postfix, Exim a CommuniGate Pro
- Skenování zpráv, databází a dalších objektů na serverech Lotus® Domino®
- Skenování všech zpráv na serveru Microsoft® Exchange včetně veřejných složek
- Filtrace zpráv podle typu přílohy
- Škálovatelnost
- Podpora clusterů Microsoft® Exchange Server 2007 a DAG for Microsoft® Exchange Server 2010
- Zálohování úložného prostoru před desinfekcí nebo odstraněním dat
- Izolování infikovaných objektů
- Možnost zrušení opakovaného skenování pošty
- Praktické nástroje pro instalaci, správu a aktualizaci
- Komplexní reporty o statusu ochrany
- Flexibilní systém skenování a scénářů v reakci na incidenty
- Systém notifikací o statusu aplikací

APLIKACE

- 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

*Funkce produktu se mohou lišit v závislosti na kombinaci použitých komponent. Popis jednotlivých komponent viz www.kaspersky.com, kde najdete podrobnější informace o funkcích jednotlivých komponent.

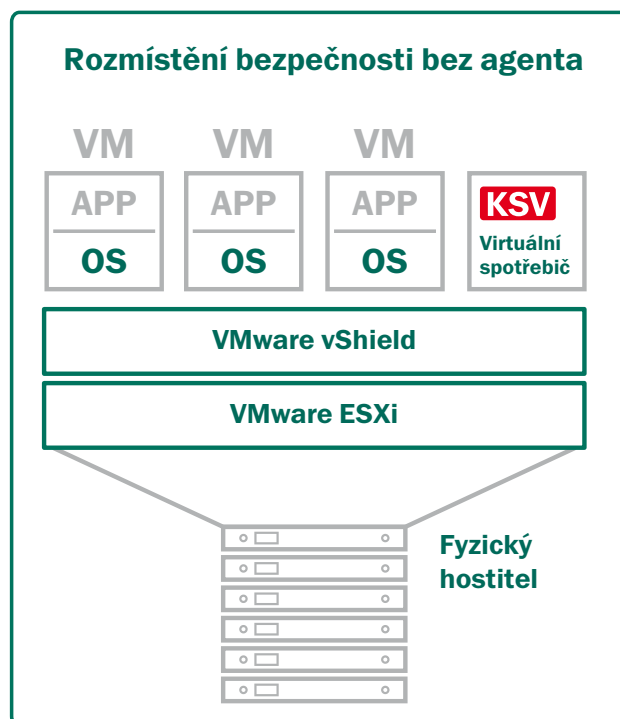
► KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization – vytvořený pro jedinečné požadavky virtualizovaných IT prostředí — poskytuje vysoce hodnocenou ochranu virtuálních serverů, desktopů i datových center před malwarem.

Kaspersky Security for Virtualization je antimalwarové řešení, které nepoužívá klienta. Představuje efektivnější způsob ochrany vaší virtualizované infrastruktury — s vyšším výkonem a menším dopadem na hustotu virtualizace. Aplikace se vyznačuje snadným rozmisťováním a disponuje funkcemi pokročilé správy, které usnadňují širokou škálu bezpečnostních úloh, a to napříč fyzickými i virtuálními výpočetními prostředky.

FUNKCE PRO ZAJIŠTĚNÍ OCHRANY A VÝKONU

- **Centrální zabezpečení.** Kaspersky Security for Virtualization je virtuální zařízení, které se připojuje do VMware vShield Endpoint — a zajišťuje funkce skenování malwaru. Představuje jeden antimalware engine a databázi pro každého fyzického hostitele.
- **Pokročilý antivirový engine.** Často oceňované antimalwarové technologie Kaspersky — spolu s vysokou frekvencí aktualizací — pomáhají při ochraně před novými a nastupujícími hrozbami. Heuristický analyzátor bojuje proti polymorfnímu malwaru.
- **Automatická ochrana.** Nové virtuální stroje jsou automaticky vybavovány ochranou proti malwaru, které pomáhají minimalizovat bezpečnostní mezery a nesprávné konfigurace. Kterýkoli VM host je vždy chráněn nejnovější databází signatur bez ohledu na to, zda byl tento virtuální stroj dříve offline.
- **Vyšší hustota virtualizace.** Protože Kaspersky Security for Virtualization je řešení, které nepoužívá agenta, pomáhá minimalizovat 'aktualizační vlny' a 'skenovací vlny', a tak dosahovat vyšší hustoty virtualizace, snižovat dopad na výkon systému a ošetřovat bezpečnostní mezery, které mohou vznikat u některých produktů, pracujících s agenty.



Produkt Kaspersky Security for Virtualization umožňuje antivir bez agenta pro nasazení produktů VMware.

FUNKCE PRO SPRÁVU:

JEDNA KONSOLE PRO SPRÁVU.

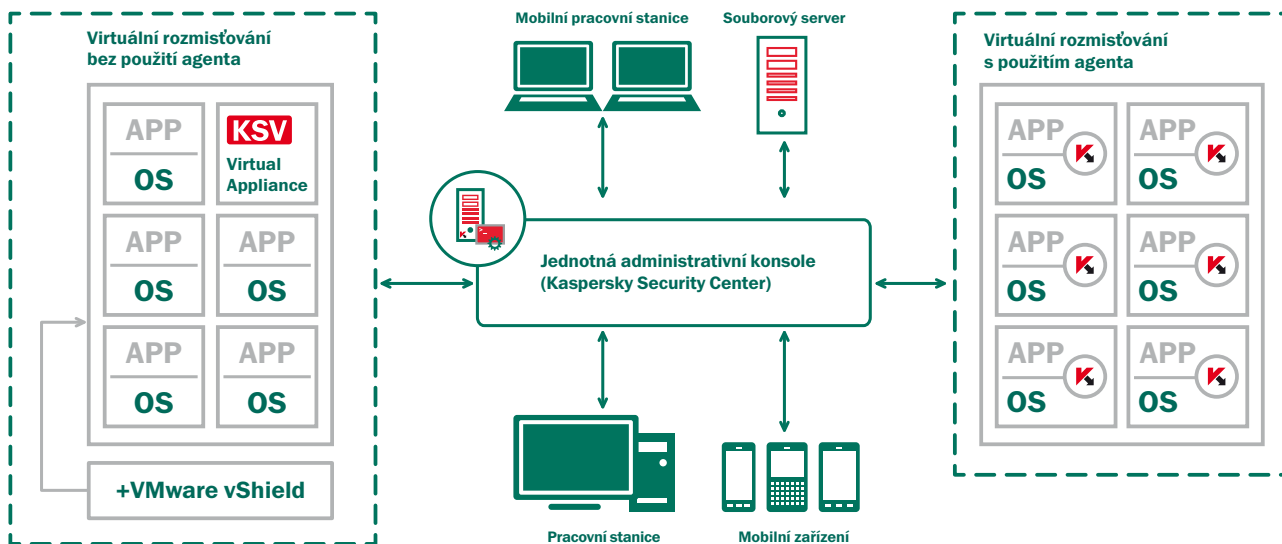
Kaspersky Security Center — který je k dispozici bez dodatečných nákladů — je jedna konzole pro správu, která umožňuje provádět správu virtuálních i fyzických strojů a mobilních zařízení.

PODPORUJE VMWARE VMOTION.

S plnou podporou produktu VMware vMotion zajišťuje Kaspersky Security for Virtualization nepřerušitelnost ochrany v případech, kdy dochází k přesunu pracovní zátěže z jednoho hostitele ESXi na druhého. Za předpokladu, že nový hostitel disponuje nezbytnými licencemi, bude ochrana následovat pracovní zatížení a bezpečnostní nastavení zůstanou stejná.

INTEGRACE S PRODUKTEM VMWARE VCENTER.

Kaspersky Security for Virtualization získává informace o virtuálních strojích z vCentra — včetně seznamu virtuálních strojů a příslušných parametrů. Kromě toho, že pracovníkům IT poskytuje lepší transparentnost, zajišťuje tato integrace s vCentrem automatickou ochranu po každou konfiguraci nového virtuálního stroje.



► KASPERSKY SECURITY FOR INTERNET GATEWAY

Produkt Kaspersky Security for Internet Gateway zajišťuje bezpečný přístup na internet pro všechny zaměstnance v organizaci.

Produkt Kaspersky Security for Internet Gateway podporuje nejoblíbenější brány na platformách Windows a Linux. Známé škodlivé a potenciálně nebezpečné programy, pracující s protokolem HTTP, HTTPS, FTP, POP3 nebo SMTP, jsou automaticky odstraněny z datového toku. Díky technologii optimalizace, škálovatelnosti a podpoře nejnovějších platforem je ideálním produktem pro velké organizace s velkými objemy provozu.

PRODUCT HIGHLIGHTS*

- Ochrana produktu Microsoft® Forefront® TMG
- Široká škála nástrojů pro správu pravidel a konfigurací
- Skenování připojení sítí VPN
- Ochrana poštovního provozu (pro protokoly POP3 a SMTP)
- Skenování provozu HTTP a FTP z publikovaných serverů
- Certifikace VMware Ready

FUNKCE

- Skenování internetového provozu v reálném čase s použitím protokolů HTTP, HTTPS, FTP, POP3 a SMTP.
- Integrovaná ochrana před všemi typy škodlivých programů.
- Podpora proxy serverů Squid, Blue Coat a Cisco®.
- Záloha úložiště
- Vyvažování pracovní zátěže procesorů serveru
- Škálovatelnost
- Praktické nástroje pro instalaci, správu a aktualizaci
- Flexibilní systém skenování a scénářů v reakci na incidenty
- Komplexní reporty o statusu ochrany sítě

APLIKACE

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

*Funkce produktu se mohou lišit v závislosti na kombinaci použitých komponent. Popis jednotlivých komponent viz www.kaspersky.com, kde najdete podrobnější informace o funkcích jednotlivých komponent.

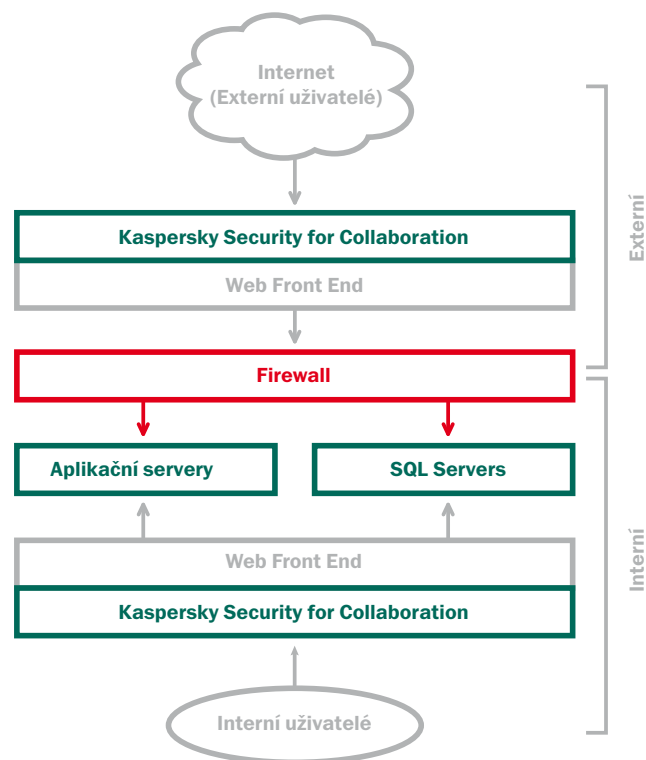
► KASPERSKY SECURITY FOR COLLABORATION

Produkt Kaspersky Security for Collaboration využívá nejnovější technologie pro ochranu vaší platformy pro týmovou spolupráci. Spojuje v sobě jednoduchost správy s vysokou mírou detekce malwaru.

Kaspersky Security for Collaboration používá vysoce ceněný antivirový engine společnosti Kaspersky pro ochranu prostředí Microsoft® SharePoint®. S touto vysoce hodnocenou technologií pro detekci malwaru dokáže chránit jeden server nebo celé farmy serverů SharePoint, funkce filtrování souborů a obsahu současně pomáhají zabránit ukládání nevhodného obsahu.

FUNKCE

- Inovativní technologie rozpoznání malwaru je koncipována pro identifikaci a blokování hrozeb v reálném čase při pokusech o stahování nebo uploadování
- Zabraňuje koncovým uživatelům ukládat určité typy souborů (např. hudbu, video nebo spustitelné soubory) nebo soubory s nevhodným textem
- Nastavení pro globální správu lze konfigurovat na všech chráněných serverech z jediného dashboardu
- Jednoduchá, intuitivní správa — bez nutnosti zvláštního školení
- Integrace s Active Directory zefektivňuje nastavení a autentifikaci uživatelů
- Detailní žurnály a záloha upravených souborů pomáhají administrátorům při reakcích na narušení nebo bezpečnostní problémy
- Podrobný, flexibilní reporting



► KASPERSKY SMALL OFFICE SECURITY

Produkt Kaspersky Small Office Security je navržen speciálně pro malé podniky. Poskytuje vysoce dostupnou ochranu nejvyšší kvality pro PC a servery, která se vyznačuje svojí rychlostí a snadností instalace, konfigurace i používání.

Kaspersky Small Office Security poskytuje IT zabezpečení světové třídy bez nutnosti IT specialistů. Umožňuje snadnou instalaci, nezpomaluje systém a zajišťuje imunitu vašeho podniku vůči všem typům hrozeb a malwaru. Udržuje zdravý provoz vašeho digitálního prostoru s nejlepší možnou ochranou vašeho podniku.

FUNKCE

- Ochrana před viry, spywarem, trojskými koňmi atd. v reálném čase
- Omezuje přístup zaměstnanců na weby, k aplikacím, hrám a sociálním sítím
- Plná ochrana vašich obchodních dat s plánovanými automatickými zálohami
- Ukládání dat v šifrovaných 'sejfech', odkud je lze bezpečně přenášet pomocí e-mailu nebo USB disku
- Generování a bezpečné ukládání obtížně prolomitelných hesel pro vás a vaše zaměstnance
- Zajišťuje maximální výkon systému častými aktualizacemi a nenáročným provozem
- Pokročilé technologie, které okamžitě blokují útoky hackerů
- Nástroje pro vyladění bezpečnosti podnikových IT sítí včetně WiFi
- Utilita File Shredder (tj. skartovač souborů) pro mazání utajovaných dat tak, aby nebylo možné je obnovit nebo ukrást

ADMINISTRACE

- Centrální správa bezpečnosti sítí z jednoho PC
- Jednoduché, intuitivní rozhraní
- Snadná správa zvyšuje zabezpečení sítí
- Správa pravidel pro používání webu

APLIKACE UVNITŘ

- Podporované platformy / operační systémy produktu Kaspersky Small Office Security:
- Microsoft® Windows® (včetně Microsoft® Windows® 7)
 - Windows® Servers (včetně Windows Server® 2008 R2)

Kaspersky Lab ZAO, Moscow, Russia
www.kaspersky.com

Vše o internetové bezpečnosti:
www.securelist.com

Najděte partnera ve svém okolí:
www.kaspersky.com/buyoffline

© Kaspersky Lab ZAO. Všechna práva vyhrazena. Registrované ochranné známky a značky služeb jsou majetkem příslušných vlastníků. Mac a Mac OS jsou registrované ochranné známky společnosti Apple Inc. Cisco je registrovaná ochranná známka nebo ochranná známka společnosti Cisco Systems, Inc. a/nebo přidružených společností v USA a v některých dalších zemích. IBM, Lotus, Notes a Domino jsou ochranné známky společnosti International Business Machines Corporation, registrované v mnoha jurisdikcích po celém světě. Linux je registrovanou ochrannou známkou společnosti Linus Torvalds v USA a dalších zemích. Microsoft, Windows, Windows Server a Forefront jsou registrované ochranné známky společnosti Microsoft Corporation v USA a v dalších zemích. Android je obchodní známkou společnosti Google, Inc. Ochranná známka Blackberry patří společnosti Research in Motion limited a je registrovaná v USA a může být podána k registraci nebo registrována v dalších zemích.

