KASPERSKY SECURITY FOR BUSINESS – KATALOG PRODUKTŮ

Červenec–prosinec 2014

KASPERSKY SECURITY FOR BUSINESS.

Dostali jste za úkol posunout svůj podnik vpřed, ale nutnost reagovat na nenadálé situace v IT a neustálé řešení potíží vám ujídá čas. A nástroje, které vám jsou k dispozici, nevyhovují výzvám, jimž čelíte.

Potřebujete něco víc, řešení, které vám dá možnost zařadit vyšší stupeň. Bezpečnostní platforma společnosti Kaspersky právě to dokáže a změnou vašeho současného zabezpečení vám pomůže připravit váš podnik na budoucnost.

Zabezpečení fyzických zařízení, mobilních uživatelů a virtuální infrastruktury může být snazší a rychlejší, než jste si mysleli, a to s využitím jediné komplexní konzole. Inovativní technologie a znalosti hrozeb vestavěné do naší integrované platformy pomáhají snížit správní zátěž a vy tak získáte čas, ve kterém se můžete zaměřit na jiné priority IT, například na skutečné potřeby podnikání nebo zlepšování budoucnosti své organizace.

Rozhodli jste se dobře, když jste se rozhodli uvažovat o produktech Kaspersky Lab – můžeme vám pomoci zajistit to nejpokročilejší zabezpečení bez potíží, rizika nebo napjatého rozpočtu. Pomůžeme vám začít nový příběh o skvělém úspěchu. Příběh, kde budete vždy o krok před vznikajícími hrozbami, takový, kde právě vy a váš podnik určujete, co se bude dít.

Tým Kaspersky Lab

Více informací najdete na adrese www.kaspersky.com.
Nejnovější zprávy o ochraně před viry, spywarem či nevyžádanou poštou a jiných záležitostech a trendech zabezpečení IT najdete na adrese www.securelist.com.

▶ PODNIKOVÁ BEZPEČNOSTNÍ ŘEŠENÍ

Plynulý výkon prostřednictvím jediné platformy

Aplikace Kaspersky Security for Business nabízí širokou škálu nástrojů a technologií, které vám dávají možnost prohlížet, ovládat a chránit všechny vaše systémy – fyzické, mobilní i virtuální.

Aplikace Kaspersky Security for Business poskytuje jediné kompletní bezpečnostní řešení, do kterého patří ochrana proti malwaru, šifrování, mobilní zařízení, vyhodnocení zranitelných míst a dočasné opravy, správa systémů, vynucování zásad a nástroje pro správu – to vše řízené z jediné centrální konzole, se snadným zavedením, jednoduchým používáním a za jednu cenu od jediného prodejce, což vám umožňuje okamžitě demonstrovat obchodní hodnotu.

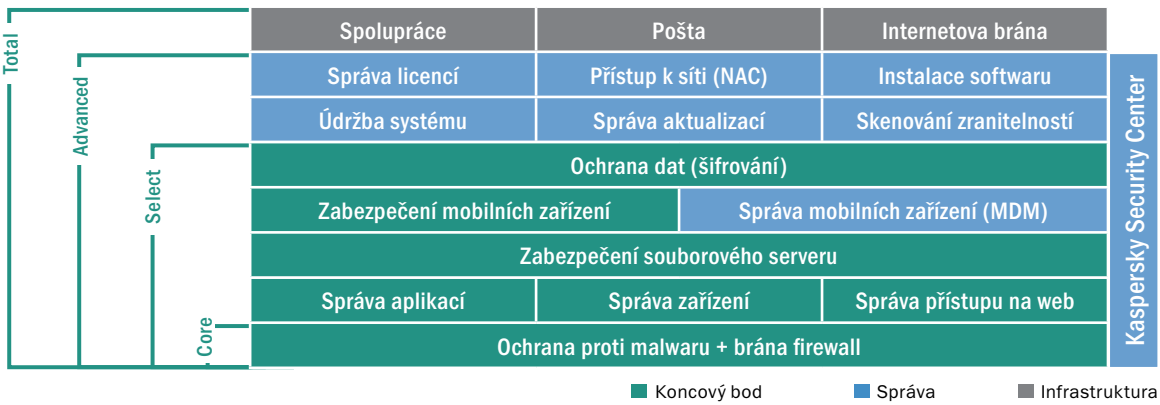
Kaspersky Endpoint Security for Business	Kaspersky Endpoint Security for Business je jednotná integrovaná bezpečnostní platforma. Začíná od nejlepší ochrany proti malwaru na světě – a její progresivní řešení umožňuje zahrnout prvky jako robustní aplikace, nástroje pro ovládání zařízení a webu, šifrování dat, zabezpečení mobilních zařízení a správy systémů a dočasných oprav. Vše se spravuje z jediné ústřední konzole – Kaspersky Security Center.	Stránky 6 až 8
Kaspersky Total Security for Business	Celá výkonná ochrana koncového bodu a bezpečnostní funkce aplikace Kaspersky Endpoint Security uvedené výše, společně se zabezpečením pošty, webu a serveru pro spolupráci stráží vaše hranice a zabezpečuje prostředí IT celého podniku.	Stránky 9
Cílená řešení Kaspersky	Samostatná řešení pro ochranu konkrétních oblastí vašeho podnikání. Některá z nich, např. Kaspersky Security for Mobile (stránky 12 až 13), jsou dostupná také jako součást aplikace Kaspersky Endpoint Security for Business. Jiná, jako Kaspersky Security for Virtualization (stránky 20 až 21), jsou dostupná pouze jako cílená řešení. Všechna jsou vybudována na stejné integrované platformě Kaspersky Security for Business a všechna řešení zabezpečení fyzických, mobilních a virtuálních zařízení se spravují centrálně prostřednictvím konzole Kaspersky Security Center.	Stránky 11 až 21

▶ VÍCE INFORMACÍ O KASPERSKY ENDPOINT SECURITY FOR BUSINESS

Aplikace Kaspersky Endpoint Security for Business nabízí kompletní bezpečnostní řešení, navržené předními světovými odborníky na zabezpečení. Jedná se o nejhlubší a do budoucnosti nejvíce namířenou ochranu s efektivním výkonem a přímočarou správou, která buduje několik linií zabezpečení vašeho podniku.

Všechny součásti byly navrženy a vytvořeny v naší společnosti a společně představují jednotnou bezpečnostní platformu vyladěnou na potřeby vašeho podniku. Výsledkem je stabilní a integrované řešení bez trhlin, bez problémů s kompatibilitou a bez žádné další pracovní zátěže při budování systému.

Správci mohou sledovat, ovládat a chránit prostředí IT pomocí aplikace Kaspersky Endpoint Security for Business. Nástroje a technologie jsou jedinečně vyvážené mezi progresivními vrstvami tak, aby splňovaly vaše rozvíjející se potřeby zabezpečení a IT. Společnost Kaspersky vám může usnadnit práci.

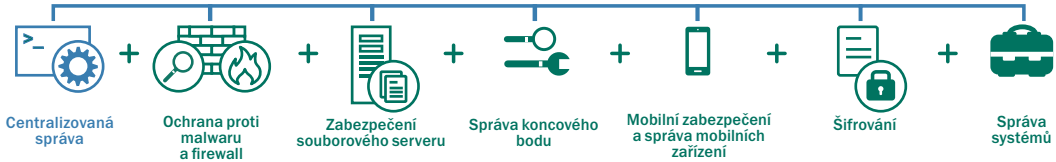


Společnost Kaspersky se může pochlubit komplexním seznamem technologií – všechny spolupracují na základě stejného kódu a dále je posiluje síť Kaspersky Security Network na bázi cloudu. To vše dává našim zákazníkům prvotřídní ochranu, kterou potřebují.

Stručně řečeno, nabízíme první platformu zabezpečení v rámci oboru, která byla od základu vybudována jako celek, usnadňující správci sledování, ovládání a zabezpečení vašeho světa.

KASPERSKY SECURITY CENTER

Jedna komplexní konzole pro správu



V centru tohoto jednotného přístupu je Kaspersky Security Center – intuitivní a plně škálovatelná konzole pro správu, která minimalizuje celkové náklady vlastnictví libovolného bezpečnostního řešení Kaspersky Lab.

Tato jednoduchá a spojitá správa zabezpečení pro stolní počítače, přenosná a mobilní zařízení i virtuální koncové body a servery prostřednictvím jediného rozhraní obsahuje:

- **kombinované zavádění zásad,**
- **samostatnou webovou konzoli,**
- **hlášení plánovaná a na vyžádání.**

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – CORE

Víceúrovňový model zabezpečení s nejpropracovanější ochranou proti malwaru

Aplikace Kaspersky Security for Business — Core zahrnuje:

VÝKONNÉ SKENOVÁNÍ KONCOVÉHO BODU NA PŘÍTOMNOST MALWARU

Působí na několika úrovních operačního systému, kde malware eliminuje pomocí heuristických technologií na bázi signatur a cloudu.

KASPERSKY SECURITY NETWORK: OCHRANA NA BÁZI CLOUDU

Informace z celosvětové sítě Kaspersky Security Network v reálném čase znamená, že je možné identifikovat a eliminovat nové a neznámé hrozby ve chvíli, kdy vzniknou.

SYSTÉM PREVENCE VNIKNUTÍ NA BÁZI HOSTITELE (HIPS) S OSOBNÍ BRÁNOU FIREWALL

Předdefinovaná pravidla pro stovky nejběžnějších aplikací zkracují dobu trávenou při konfiguraci firewallu.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – SELECT

Obsahuje ochranu souborového serveru, ovládání koncových bodů a zabezpečení a správu mobilních zařízení

Nástroje pro správu mobilních zařízení a detailní ovládání koncových bodů ve spojení s ochranou proti malwaru poskytují několik úrovní zabezpečení a chrání vaše data dokonce i na mobilních zařízeních patřících zaměstnancům. Ochrana souborového serveru zajišťuje, že se infekce prostřednictvím uložených dat nemůže rozšířit na zabezpečené koncové body.

SPRÁVA KONCOVÉHO BODU

Správa aplikací – s „dynamickými seznamy povolených položek“, využívajícími důvěryhodnost souborů v reálném čase pomocí sítě Kaspersky Security Network, umožňuje správcům IT povolit, blokovat či regulovat aplikace včetně využití scénáře „implicitního zákazu“. Správa oprávnění aplikací sleduje a omezuje aplikace provádějící podezřelé úkony.

Správa přístupu na web – na základě předem nastavených nebo vlastních databází nevhodných adres je možné vytvořit zásady procházení a sledovat uživatele na firemní síti a při roamingu.

Správa zařízení – umožňuje správcům nastavovat, plánovat a vynucovat datové zásady ovládající připojení vyměnitelných úložných zařízení a jiných periferních zařízení k libovolnému typu sběrnice.

ZABEZPEČENÍ MOBILNÍCH ZAŘÍZENÍ:

Ochrana mobilních zařízení proti malwaru – kombinace aktivních technologií na bázi signatury a cloudu zajišťuje výkonnou ochranu mobilních zařízení v reálném čase. Bezpečný prohlížeč a ochrana proti nevyžádané poště zvyšují zabezpečení.

Správa mobilních zařízení (MDM) – aplikace Kaspersky Security for Mobile podporuje funkce poskytované službami Microsoft Exchange Active Sync, Apple MDM a Samsung SAFE.

Vzdálená ochrana proti krádeži – sledování karty SIM, vzdálené uzamčení, úplné nebo selektivní, vymazání a vyhledání, to vše zabraňuje neoprávněnému přístupu k firemním datům v případě ztráty či krádeže mobilního zařízení.

Ovládání mobilních zařízení – správci mohou spravovat a omezovat využití aplikací, a takto zakázat použití nežádoucího nebo šedého softwaru.

Kromě blokování škodlivých adres mohou ovládat přístup na weby nesplňující firemní zásady.

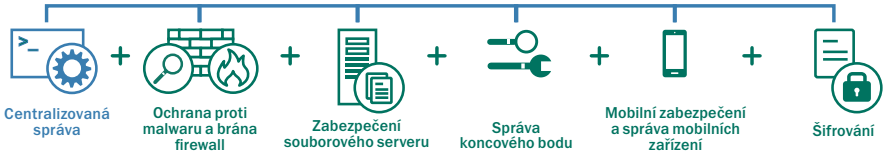
Kontejnerizace aplikací pro systém BYOD – firemní data a aplikace je možné izolovat od osobních souborů na zařízení zaměstnance umístěním firemních aplikací do speciálních kontejnerů, které je možné zašifrovat a mazat odděleně od uživatelových osobních dat.

ZABEZPEČENÍ SOUBOROVÉHO SERVERU

Ochrana souborového serveru spravovaná společně se zabezpečením koncového bodu prostřednictvím konzole Kaspersky Security Center zajišťuje, aby se malware nemohl šířit na zabezpečené koncové body prostřednictvím uložených nakažených dat.

Kaspersky Endpoint Security — Select obsahuje také všechny součásti úrovně Core.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS – ADVANCED



Včetně šifrování a správy systémů

Aplikace Kaspersky Endpoint Security for Business — Advanced podporuje výkonnost a soulad při správě IT. Upřednostňované dočasné opravy, správa bitových kopií OS a vzdálené řešení problémů usnadňují každodenní správu. Infrastruktura, návštěvníci a inventáře přitom zůstávající pod pevnou kontrolou IT. Další úroveň zabezpečení přidává komplexní a transparentní šifrování a všechny součásti jsou spravovány prostřednictvím jediné uspořádané konzole – Kaspersky Security Center.

SPRÁVA SYSTÉMŮ

Správa zranitelných míst a dočasných oprav – automatizovaná detekce a upřednostnění zranitelných míst OS a aplikací, ve spojení s automatizovanou distribucí dočasných oprav a aktualizací.

Zavedení operačního systému – snadné vytvoření, ukládání a zavádění bitových kopií OS z centrálního umístění spolu s migrací OS.

Vzdálená distribuce softwaru a řešení problémů – vzdálené závádění a aktualizace z jediné konzole, automatizované pro více než 100 aplikací, může probíhat na vyžádání nebo podle plánu v klidnějších obdobích. Je plně podporováno vzdálené řešení problémů šetřící čas a v pobočkových kancelářích může přijímat aktualizace pro místní instalace s použitím technologie Multicast jediný „agent“.

Řízení přístupu k síti (NAC) – automaticky rozpoznává a kontroluje nová zařízení na síti a porovnává je s inventáři a bezpečnostními zásady IT, přičemž zabraňuje v přístupu podezřelým zařízením a přesměrovává zařízení zákazníků na přihlašovací portál.

Inventáře hardwaru a softwaru – kompletní přehled a ovládání (včetně blokování) veškerého softwaru zaváděného přes síť, společně s automatickou identifikací, registrací a sledováním veškerého hardwaru včetně vyměnitelných zařízení.

ŠIFROVÁNÍ

Komplexní ochrana souboru/složky a celého disku – vyberte si mezi ochranou celého disku nebo na úrovni souboru, která je pro uživatele transparentní, a za kterou stojí 256bitové šifrování Advanced Encryption Standard (AES). Takto se zajistí bezpečnost důležitých obchodních informací v případě krádeže či náhodné ztráty zařízení. Obsahuje podporu šifrování pro vyměnitelná zařízení.

Bezpečné sdílení dat – umožňuje uživatelům snadno sdílet šifrované a samorozbalovací balíčky a zajišťuje ochranu dat při sdílení prostřednictvím vyměnitelných zařízení, e-mailu, sítě či webu.

Aplikace Kaspersky Endpoint Security for Business – Advanced také obsahuje všechny součásti úrovní Select a Core.

KASPERSKY TOTAL SECURITY FOR BUSINESS

Včetně zabezpečení periférií pro servery a brány

Aplikace Kaspersky Total Security for Business zajišťuje nejúplnější platformu ochrany a správy v tomto odvětví. Aplikace Total Security for Business zabezpečuje všechny vrstvy vaší sítě a obsahuje mocné konfigurační nástroje zajišťující, aby uživatelé byli produktivní a neobtěžovali je žádné malwarové hrozby, bez ohledu na zařízení či umístění.

ZABEZPEČENÍ POŠTY

Účinně zabraňuje hrozbám na bázi e-mailu, phishingovým útokům a nevyžádané poště pomocí aktualizací v reálném čase na bázi cloudu, které nabízejí mimořádnou míru zachycení spamu a minimum falešně pozitivních výsledků. Součástí je i ochrana proti malwaru pro systém IBM Domino.

ZABEZPEČENÍ INTERNETOVÉ BRÁNY

Zajišťuje zabezpečený přístup k internetu v celé organizaci automatickým odstraněním škodlivých a potenciálně nebezpečných programů v datových přenosech HTTP(S) / FTP / SMTP a POP3.

ZABEZPEČENÍ SPOLUPRÁCE

Chrání servery a farmy SharePoint® proti všem formám malwaru, zatímco možnosti filtrování obsahu a souborů pomáhají bránit ukládání nevhodného obsahu.

Aplikace Kaspersky Total Security for Business také obsahuje všechny součásti úrovní Advanced, Select a Core.

FUNKCE PRODUKTU

Které řešení je pro vás to pravé?

	Core	Select	Advanced	Total	Pod správou produktu Security Center	Dostupné v cílených řešeních
Ochrana proti malwaru	●	●	●	●	●	
Brána firewall	●	●	●	●	●	
Správa aplikací		●	●	●	●	
Správa zařízení		●	●	●	●	
Správa přístupu na web		●	●	●	●	
Zabezpečení souborového serveru		●	●	●	●	●
Ochrana mobilních koncových bodů		●	●	●	●	●
Správa mobilních zařízení		●	●	●	●	●
Šifrování			●	●	●	
Správa bitových kopií OS			●	●	●	●
Správa licencí			●	●	●	●
Správa zranitelných míst			●	●	●	●
Správa dočasných oprav			●	●	●	●
Řízení přístupu k síti			●	●	●	●
Zabezpečení serveru pro spolupráci				●		●
Zabezpečení serveru pro poštu				●	●	●
Zabezpečení internetové brány				●		●
Zabezpečení virtuální infrastruktury					●	●
Zabezpečení úložného serveru					●	●

● Obsaženo ● Částečně obsaženo – podrobnosti viz stránky produktu

KASPERSKY SECURITY FOR FILE SERVER

Aplikace Kaspersky Security for File Server poskytuje cenově výhodné, spolehlivé a škálovatelné zabezpečení pro sdílená úložiště souborů bez viditelného dopadu na výkon systémů.

NEJDŮLEŽITĚJŠÍ INFORMACE

VÝKONNÁ OCHRANA PROTI MALWARU

Oceňovaný antimalwarový engine společnosti Kaspersky poskytuje výkonnou ochranu serverů, bránící i těm nejnovějším známým a potenciálním malwarovým hrozbám v přístupu do místní sítě prostřednictvím škodlivých či nebezpečných programů.

VYSOKÝ VÝKON A SPOLEHLIVOST

Můžete mít důvěru, že aplikace Kaspersky Security for File Server nezpomalí nijak znatelně váš systém ani nenaruší obchodní operace, a to ani za podmínek velmi náročného síťového zatížení.

PODPORA VÍCE PLATFOREM

Jednotné a účinné bezpečnostní řešení pro heterogenní serverové sítě, podporující nejnovější platformy a servery včetně terminálových, clusterových a virtuálních serverů bez problémů s kompatibilitou.

BOHATÉ MOŽNOSTI SPRÁVY A SYSTÉMU HLÁŠENÍ

Efektivní, uživatelsky přívětivé nástroje pro správu, informace o stavu ochrany serveru, flexibilní nastavení času na skenování a rozsáhlý systém hlášení poskytují účinnou správu zabezpečení souborového serveru, což pomáhá snižovat náklady na vlastnictví.

FUNKCE

- **Ochrana proti malwaru v reálném čase** pro souborové servery s nejnovějšími verzemi systémů Windows® (včetně Windows® Server 2012/R2), Linux a FreeBSD (obojí včetně funkce Samba).
- **Ochrana terminálových serverů Citrix a Microsoft.**
- **Plně podporuje clusterové servery.**
- **Škálovatelnost** – podpora a snadné zabezpečení i těch nejkomplexnějších heterogenních infrastruktur.
- **Spolehlivost, stabilita a vysoká odolnost proti poruchám.**
- **Optimalizovaná inteligentní technologie skenování** včetně skenování na vyžádání a skenování důležitých oblastí systému.
- **Důvěryhodné zóny** pomáhají navýšit zabezpečení a přitom omezit množství zdrojů potřebných pro skenování.
- **Karanténa a zálohování** dat před čištěním nebo odstraněním.
- **Izolace** nakažených pracovních stanic.
- **Centralizovaná instalace, správa a aktualizace** s širokou nabídkou metod instalace a správy.
- **Flexibilní scénáře reakce na nález.**
- **Komplexní hlášení** o stavu ochrany sítě.
- **Systém upozornění na stav aplikací.**
- **Podpora systémů HSM** (Hierarchical Storage Management).
- **Ověřená podpora řešení Hyper-V a Xen Desktop.**
- **Certifikace VMware Ready.**
- **Podpora odolného systému souborů (ReFS).**

KASPERSKY SECURITY FOR MOBILE

Centralizovaná správa, zabezpečení a řízení koncových bodů v majetku podniku a v majetku zaměstnance (BYOD)

Díky aplikaci Kaspersky Security for Mobile je zabezpečená centralizovaná správa mobilních zařízení bezbolestná a přímočará, přičemž poskytuje cílenou ochranu, kterou potřebujete proti současným a budoucím hrozbám.

NEJDŮLEŽITĚJŠÍ INFORMACE

VYNIKAJÍCÍ OCHRANA PRO MOBILNÍ ZAŘÍZENÍ A JEJICH DATA
Mezi pokročilé schopnosti zabezpečení mobilních zařízení patří technologie ochrany proti malwaru či phishingu. Správa aplikací a procházení webu poskytuje hluboké úrovně komplexní ochrany firemních dat na vašich vlastních mobilních zařízeních i zařízeních vašich zaměstnanců.

SPRÁVA A OCHRANA VAŠICH DAT
V modelu BYOD (přineste si vlastní zařízení) je možné firemní data na zařízeních zaměstnanců izolovat do oddělených šifrovaných „kontejnerů“ a potom je v případě potřeby na dálku nezávisle vymazat – tím se zachová zabezpečení dat a zároveň se bude respektovat soukromí zaměstnance.

ZJEDNODUŠENÍ SPRÁVY MOBILNÍCH ZAŘÍZENÍ
Sjednocená a centralizovaná správa s integrací systému iOS a Samsung MDM s podporou funkcí Microsoft ActiveSync urychluje a zpřehledňuje vzdálenou správu a řízení mobilních zařízení na všech předních mobilních platformách pomocí technologie „over the air“ (OTA), což snižuje náklady na správu.

CENTRALIZOVANÁ SPRÁVA Z JEDNÉ OBRAZOVKY
Centralizovaná správa poskytuje kontrolu pro všechny platformy mobilních zařízení a zahrnuje všechny aspekty vaší infrastruktury. S konzolí Kaspersky Security Center je možné organicky prostřednictvím jediné konzole spravovat zabezpečení kteréhokoliv koncového bodu – firemních a zaměstnaneckých mobilních zařízení, pracovních stanic, notebooků a dokonce virtuální infrastruktury.

BEZPEČNOSTNÍ FUNKCE

- **Ochrana proti malwaru pro mobilní zařízení.** Antimalwarový engine společnosti Kaspersky Lab nabízí kombinaci technologií na bázi signatury a heuristické detekce, společně s ochranou proti novým a neznámým hrozbám, a to pomocí nepřetržitých aktualizací ze sítě Kaspersky Security Network (KSN), globální databáze společnosti Kaspersky Lab v reálném čase na bázi cloudu. K ochraně zařízení a dat na něm obsažených přispívá i prohlížeč Safe Browser a výkonná technologie ochrany proti phishingu.
- **Opatření proti krádeži.** V případě ztráty nebo krádeže zařízení je možné použít vzdálené uzamčení. Správci poté mohou dálkově provést úplné nebo selektivní vymazání zařízení, určit polohu hledaného zařízení pomocí hledání GPS a dostat automatické upozornění, jestliže dojde k odstranění či výměně karty SIM.
- **Správa aplikací.** Aplikace nainstalované na kterémkoliv mobilním zařízení je možné vzdáleně sledovat a řídit prostřednictvím předdefinovaných skupinových zásad. Uživatelům je možné povolit instalaci pouze schválených aplikací nebo jim zakázat instalaci těch, které jsou považovány za potenciálně nebezpečné či nevhodné. Aktivovat je možné také požadavek na opětovné přihlášení po zvolené době nečinnosti.
- **Správa přístupu na web.** Síť Kaspersky Security Network podporuje správu přístupu na web a bezpečné prohlížení internetu a identifikuje v reálném čase webové stránky nakažené malwarem nebo malware obsahující. Kromě blokování podezřelých webů mohou správci řídit přístup k typům webových stránek, které neodpovídají firemním zásadám – např. sociálním médiím, hazardním hrám, obsahu pro dospělé, proxy serverům nebo obchodům online.
- **Detekce incidentů typu jailbreak/rooting.** Jestliže dojde k incidentu typu jailbreak, je automaticky upozorněn správce, dojde k zablokování přístupu k firemním aplikacím a zařízení je možné selektivně či zcela vymazat.
- **Integrita firemních a osobních dat: kontejnery.** V rámci podpory scénáře umístění firemních dat v zařízení zaměstnance je možné firemní data umístit do izolovaných „kontejnerů“. Tím se zajišťuje maximální zabezpečení firemních dat a optimální integrita pro osobní obsah.
- **Ochrana firemních dat v kontejneru.** Na tyto kontejnery je možné uplatnit další funkce zabezpečení, například šifrování nebo další úroveň oprávnění. Když zaměstnanec z organizace odejde, je možné kontejnery vzdáleně vymazat a ponechat osobní soubory nedotčené.

FUNKCE PRO SPRÁVU

- **Správa mobilních zařízení.** Aplikace Kaspersky Security for Mobile podporuje funkce poskytované službami Microsoft Exchange Active Sync, Apple MDM a Samsung SAFE. Správci mohou vynutit nastavení kódu PIN, definovat složitost hesla, spravovat funkce šifrování, zabránit používání kamery a spravovat související funkce pro širokou škálu smartphonů a tabletů, vzdáleně z jediného rozhraní.
- **Technologie OTA.** Smartphonům a tabletům je možné povolit přístup do firemní sítě pomocí technologie „over the air“ (OTA) prostřednictvím odkazu nebo kódu QR zaslaného zaměstnanci e-mailem nebo zprávou SMS. Řešení pak může být automaticky nnainstalováno, pro zabránění mezerám v zabezpečení IT.
- **Správa více platforem prostřednictvím jediné konzole.** Nejsou potřeba samostatné konzole pro každou součást MDM – správa mobilních zařízení všech platforem se odehrává prostřednictvím jediné konzole, Kaspersky Security Center. Kromě mobilních zařízení je možné také společně spravovat vzdáleně ze stejné jedinečné konzole zabezpečení fyzických koncových bodů a virtuálních systémů včetně šifrování a vynucování zásad.

KASPERSKY SYSTEMS MANAGEMENT

Efektivita a rozšířené zabezpečení IT

Představujeme vám řešení Kaspersky Systems Management. Toto řešení nabízí rozsáhlou sadu výkonných nástrojů IT pro produktivitu v prostředích Windows, napsané ve stejném kódu a spravované z jedné konzole. Výsledná platforma poskytuje jednoduchost a automatizaci, jakou chcete, a zabezpečení a správu, jakou potřebujete.

NEJDŮLEŽITĚJŠÍ INFORMACE

POSÍLENÉ ZABEZPEČENÍ
Načasované a automatizované zjišťování a stanovování priority zranitelných míst v operačních systémech a softwaru, spolu s rychlou a automatizovanou distribucí požadovaných dočasných oprav a aktualizací, podle potřeby zvyšují vaše zabezpečení a zároveň snižují administrativní zátěž.

EFEKTIVNÍ PRÁCE
Správci mohou vzdáleně distribuovat a instalovat aktualizace, opravy a aplikace. Vzdálené řešení problémů znamená, že správce neplýtvá časem přesuny z kanceláře do kanceláře nebo na telefonu. Pracovní zátěž pomáhá snižovat rovněž centralizované a automatizované nasazování operačních systémů, které eliminuje zdvojení práce při nastavování jednotlivých uživatelů.

ŘÍZENÍ S ÚPLNÝM PŘEHLEDEM
Díky úplnému přehledu o síti z jediné konzole ví správci o všech aplikacích a zařízeních, včetně zařízení hostů, která se do sítě připojí. Tento přehled pomáhá při centralizované správě přístupu uživatelů a zařízení k firemním datům a softwarovým aplikacím v souladu se zásadami IT.

CENTRÁLNÍ SPRÁVA
Tyto a další funkce jsou součástí aplikace Kaspersky Systems Management a ke všem společně se přistupuje prostřednictvím konzole pro správu Kaspersky Security Center. Protože jednotlivé nástroje nevyžadují vlastní oddělenou konzoli, jsou příkazy konzistentní a intuitivní a není potřeba žádné další zaškolení.

SOUČÁSTI

NASAZENÍ OPERAČNÍHO SYSTÉMU A APLIKACÍ

Snadná tvorba, ukládání, klonování a nasazování bitových kopií systému z centrálního umístění. Zajišťuje, že se systémy předávají uživateli bez problémů a s optimálním nastavením zabezpečení včetně nasazení po pracovní době prostřednictvím služby Wake-On-LAN. Tento nástroj se dobře hodí pro migraci operačních systémů.

VYHODNOCOVÁNÍ ZRANITELNÝCH MÍST A SPRÁVA DOČASNÝCH OPRAV

Skenování hardwaru a softwaru jediným kliknutím porovnává výsledky mezi různými databázemi zranitelných míst, automaticky stanovuje jejich prioritu a definuje místa, která vyžadují okamžitou pozornost a která lze odložit po pracovní době. Opravy a aktualizace je poté možné na tomto základě automaticky nasazovat – buď na vyžádání, nebo v režimu plánování.

POSKYTOVÁNÍ A SPRÁVA LICENCÍ

Přehled o počtu uživatelů aplikace v kterémkoliv okamžiku pomáhá optimalizovat náklady na licence a sledovat, kde náklady uživatelům neodpovídají.

DISTRIBUCE SOFTWARU

Software lze nasazovat vzdáleně a aktualizovat z jedné konzole. Automaticky lze instalovat a aktualizovat přes 100 nejoblíbenějších aplikací (zjištěných pomocí platformy Kaspersky Security Network). Navíc díky možnosti provádět tyto činnosti i po pracovní době se proces distribuce dále zjednodušuje. Zcela podporováno je vzdálené řešení problémů ze stejné konzole na libovolném systému klienta a pomocí technologie Multicast je možné jako centrální „agenty“ pro místní distribuci aktualizací přiřadit pracovní stanice v pobočkových kancelářích. Výsledkem jsou rychlejší aktualizace softwaru s menšími nároky na šířku pásma.

INVENTÁŘE HARDWARU A SOFTWARU

Počítače, pevné disky i vyměnitelná zařízení se automaticky zjišťují a zařazují do inventáře. Zavedení nového zařízení aktivuje upozornění správci, který může sledovat stav a využití hardwaru v síti. Inventář softwaru rovněž přesně sleduje, jaký software se v kterémkoliv okamžiku používá. Tento inventář lze nasadit ve spojení s nástroji pro správu koncových bodů společnosti Kaspersky Lab a blokovat nebo omezovat použití specifických softwarových aplikací.

ŘÍZENÍ PŘÍSTUPU K SÍTI (NAC)

Funkce NAC usnadňuje a zpřehledňuje řízení přístupu hostů. Nová zařízení v síti se automaticky rozpoznají a zkontrolují pomocí inventáře hardwaru a zásad zabezpečení IT. Podezřelým zařízením lze přístup k síti odepřít, kdežto zařízení hostů lze přesměrovat na přihlašovací portál a udělit jim přístup k internetu.

CENTRALIZOVANÁ SPRÁVA

Nástroje Kaspersky Systems Management tvoří součást jednotné integrované platformy zabezpečení a poskytují tak komplexní schopnosti zabezpečení a správy IT prostřednictvím centrální konzole pro správu – Kaspersky Security Center. Aplikace Kaspersky Security Center podporuje správu zabezpečení pro stolní počítače i mobilní a virtuální koncové body napříč firemní sítí pomocí jediného rozhraní, čímž se eliminuje složitost a posiluje vaše zabezpečení.

KASPERSKY SECURITY FOR MAIL SERVER

Aplikace Kaspersky Security for Mail Server poskytuje vynikající ochranu pro provoz probíhající na poštovních serverech před spamem, phishingem a obecnými i pokročilými malwarovými hrozbami, a to i ve velmi komplexních heterogenních infrastrukturách.

NEJDŮLEŽITĚJŠÍ INFORMACE

OCHRANA PŘED MALWAROVÝMI HROZBAMI

Výkonnou ochranu proti malwaru poskytuje oceňovaný antimalwarový engine společnosti Kaspersky Lab, podporovaný v reálném čase sítí Kaspersky Security Network na bázi cloudu, společně s aktivní ochranou proti zneužití a filtrováním škodlivých adres URL.

OCHRANA PROTI SPAMU

U mailových serverů na bázi systému Microsoft Exchange nebo Linux se prokázalo, že antispamový engine společnosti Kaspersky Lab na bázi cloudu blokuje až 99,92 % spamu plýtvajícího časem a zdroji s 0 % až 0,05 % falešně pozitivních nálezů.

OPTIMALIZACE SYSTÉMOVÝCH ZDROJŮ

Vyrovnávání zatížení, technologie optimalizovaného skenování a důvěryhodné výjimky – to vše pomáhá snižovat objem zdrojů nezbytných ke skenování malwaru, přičemž inteligentní filtrování spamu výrazně snižuje provozní zátěž.

JEDNODUCHÁ A FLEXIBILNÍ SPRÁVA

Uživatelská vstřícnost, nástroje správy a hlášení, informace o stavu ochrany mailu plus flexibilní nastavení skenování poskytují efektivní správu zabezpečení pošty a dokumentů, aby bylo možné snížit celkové náklady na vlastnictví.

FUNKCE

- **Ochrana proti malwaru v reálném čase** podporovaná sítí Kaspersky Security Network na bázi cloudu.
- **Pokročilá ochrana** pomocí technologie ZETA Shield před dosud neznámým zneužitím, a dokonce před zranitelnostmi nulté hodiny.
- **Efektivní ochrana proti spamu.**
- **Antispamové skenování** všech zpráv na bázi cloudu v reálném čase na serverech Microsoft® Exchange včetně veřejných složek pomocí sítě Kaspersky Security Network.
- **Plánované skenování e-mailů** a databází Domino.
- **Skenování zpráv, databází a dalších objektů na serverech** IBM Domino®.
- **Filtrování zpráv** na základě rozpoznávání formátu, velikosti a názvu přílohy.
- **Snadný a pohodlný** postup aktualizace databáze ochrany proti malwaru a spamu.
- **Zálohování úložiště dat** před čištěním nebo odstraněním.
- **Škálovatelnost a odolnost proti poruchám.**
- **Snadná instalace a flexibilní integrovaná správa.**
- **Výkonný systém upozornění.**
- **Komplexní hlášení** o stavu ochrany sítě.

KASPERSKY SECURITY FOR INTERNET GATEWAY

Aplikace Kaspersky Security for Internet Gateway představuje špičkové řešení ochrany proti malwaru, které zajišťuje bezpečný nepřetržitý přístup k internetu pro všechny vaše zaměstnance.

NEJDŮLEŽITĚJŠÍ INFORMACE

VÝKONNÁ OCHRANA ZKRACUJE PROSTOJE A NARUŠENÍ

Oceňovaný antimalwarový engine společnosti Kaspersky Labs brání nejnovějším známým a potenciálním malwarovým hrozbám v přístupu do místní sítě prostřednictvím škodlivých či nebezpečných programů.

EFEKTIVITA VÝKONU DÍKY OPTIMALIZACI

Optimalizovaná, inteligentní technologie skenování a vyrovnávání zatížení snižují zatížení zdrojů a pomáhají zachovat cennou šířku pásma, aniž by se tím zkrátil výkon zabezpečení.

PODPORA VÍCE PLATFOREM

Podpora nejnovějších platforem a serverů včetně serverů přináší vysokou hodnotu pro organizace vyznačující se velkými objemy síťového provozu v heterogenních prostředích. Podpora platformy Microsoft Forefront TMG sahá od ochrany firemní pošty až po ochranu webové brány.

PŘÍMOČARÁ SPRÁVA A HLÁŠENÍ

Jednoduché a uživatelsky vstřícné nástroje pro správu, flexibilní nastavení skenování a systémy hlášení stavu ochrany.

FUNKCE

- **Nepřetržitá aktivní ochrana** proti vznikajícím a známým malwarovým hrozbám.
- **Vynikající míra detekce malwaru** v kombinaci s minimem falešně pozitivních nálezů.
- **Optimalizovaná, inteligentní technologie skenování.**
- **Skenování provozu** HTTP, HTTPS a FTP z publikovaných serverů v reálném čase.
- **Ochrana serveru Squid**, nejpoužívanějšího serveru proxy systému Linux.
- **Pohodlné nástroje** pro instalaci, správu a aktualizace.
- **Flexibilní skenovací nástroje a scénáře reakce na nález**.
- **Vyrovnávání zatížení** procesorů serveru.
- **Škálovatelnost a odolnost proti poruchám.**
- **Komplexní hlášení** o stavu ochrany sítě.

FUNKCE SPECIFICKÉ PRO SERVERY MICROSOFT FOREFRONT TMG A ISA:

- sledování stavu aplikací v reálném čase,
- skenování připojení sítí VPN,
- skenování provozu HTTPS v reálném čase (pouze servery TMG),
- ochrana e-mailového provozu (prostřednictvím protokolů POP3 a SMTP),
- Úložiště záloh (pouze servery TMG).

KASPERSKY SECURITY FOR COLLABORATION

Aplikace Kaspersky Security for Collaboration poskytuje prvotřídní ochranu platformy v reálném čase, kdy pomáhá vynutit interní zásady komunikace a ukládání, aby uživatelé mohli klidně spolupracovat.

NEJDŮLEŽITĚJŠÍ INFORMACE

PRVOTŘÍDNÍ OCHRANA PROTI MALWARU

Aplikace Kaspersky Security for Collaboration, vybavená nejnovějším oceňovaným antimalwarovým enginem společnosti Kaspersky Lab, zjišťuje a eliminuje malwarové hrozby. Výkonná ochrana proti vznikajícímu a neznámému malwaru v reálném čase je poskytována prostřednictvím sítě Kaspersky Security Network na bázi cloudu, spolu s technologií ochrany proti phishingu chránící sdílená data před webovými hrozbami.

KOMPLETNÍ ZABEZPEČENÍ PLATFORMY

Využíváte-li server Microsoft SharePoint Server, víte, že řešení ochrany koncových bodů jsou nevyhovující, jelikož spravovaný obsah se ukládá do databáze SQL. Z tohoto důvodu byla navržena aplikace Kaspersky Security for Collaboration, zabezpečující celou farmu SharePoint a všechny její uživatele.

SPRÁVA OBSAHU A ÚLOŽIŠTĚ

Funkce filtrování obsahu a souborů pomáhají při vynucování vašich komunikačních zásad a standardů, identifikaci a blokování nevhodného obsahu a zabraňují nehospodárnému ukládání nevhodných souborů a formátů souboru.

JEDNODUCHÁ SPRÁVA

Zabezpečení celé serverové farmy lze spravovat centrálně z jediného přehledného řídicího panelu. Administrativa je rychlá a přímočará, bez nutnosti žádného speciálního zaškolování.

FUNKCE

- **Výkonná ochrana proti malwaru**. Bezpečnostní skenování při přístupu a na pozadí využívá informace o nových a vznikajících hrozbách v reálném čase.
- **Ochrana proti phishingu.** Ve webovém obsahu jsou vyhledávány phishingové odkazy a uživatelská data jsou tak chráněna před odcizením.
- **Filtrování souborů.** Analyzuje skutečné formáty souborů bez ohledu na příponu a nedovoluje uživatelům ukládat stanovené typy souborů (např. hudbu, video, spustitelné soubory).
- **Filtrování obsahu.** Analýza podle klíčových slov (přednastavených nebo uživatelsky vytvořených) zabraňuje ukládání souborů s nevhodným obsahem.
- **Zálohování a ukládání** dat před čištěním nebo odstraněním.
- **Integrace se službou Active Directory.** Zjednodušené nastavení a ověřování uživatelů.
- **Centralizovaná správa.** Globální nastavení lze pro všechny chráněné servery konfigurovat pomocí jediného řídicího panelu.
- **Jednoduchá správa.** Jasné a snadno pochopitelné rozhraní nabízející běžně používané scénáře.

KASPERSKY SECURITY FOR STORAGE

Aplikace Kaspersky Security for Storage poskytuje robustní, výkonnou a škálovatelnou ochranu cenným a citlivým firemním datům nahraným do systémů úložišť EMC™ VNX™ a NetApp.

NEJDŮLEŽITĚJŠÍ INFORMACE

VÝKONNÁ OCHRANA PROTI MALWARU V REÁLNÉM ČASE

Nepřetržitá aktivní ochrana pro řešení úložišť připojených k síti (NAS). Výkonná ochrana proti malwaru společnosti Kaspersky skenuje všechny spuštěné či upravované soubory, jestli neobsahují jakoukoliv formu malwaru včetně virů, červů a trojských koní. Pokročilá heuristická analýza identifikuje i nové a neznámé hrozby.

OPTIMALIZOVANÝ VÝKON

Výkonné skenování, nabízející optimalizovanou skenovací technologii a pružné nastavení výjimek, zajišťuje maximální ochranu a zároveň minimalizuje dopad na výkon systému.

SPOLEHLIVOST

Výjimečná odolnost proti poruchám díky jednoduché architektuře využívající jednotné komponenty navržené a sestavené tak, aby hladce spolupracovaly. Výsledkem je stabilní a odolné řešení, které v případě nuceného vypnutí provede automatický restart a zajistí spolehlivou nepřetržitou ochranu.

SNADNÁ SPRÁVA

Servery se instalují vzdáleně a jsou chráněné ihned bez potřeby restartu. Spravovány jsou společně prostřednictvím konzole Kaspersky Security Center společně s dalšími řešeními zabezpečení společnosti Kaspersky.

FUNKCE

- **Nepřetržité aktivní zabezpečení.** Pro úložné systémy EMC a NetApp proti vznikajícím a potenciálním hrozbám.
- **Automatické aktualizace**. Nedochází k přerušení skenování.
- **Vyjmuté procesy a důvěryhodné zóny.** „Důvěryhodné zóny“, definované formáty souborů a stanovené procesy je možné ze skenování vyjmout.
- **Skenování objektů automatického spuštění.** Zabránění spuštění malwaru během spouštění systému.
- **Optimalizovaný výkon díky pružnému skenování.** Správce může určit a řídit hloubku, šířku a načasování skenování a definovat, které typy souborů a oblasti je nutné skenovat. Včetně technologií iSwift a iChecker.
- **Chrání řešení HSM a DAS**. Podporuje řešení skenování offline pro technologie Hierarchical Storage Management (HSM) a Direct Attached Storage (DAS).
- **Ochrana virtuálních systémů a terminálových serverů.** Chrání virtuální operační systémy (hosty) v prostředích Hyper-V a VMware a terminálové infrastruktury Microsoft a Citrix.
- **Centralizovaná instalace a správa.** Spravováno prostřednictvím intuitivní konzole Kaspersky Security Center. V případě potřeby je dostupná i správa z příkazového řádku.
- **Kontrola nad oprávněními správců.** Správci každého serveru je možné přiřadit různé úrovně oprávnění.
- **Flexibilní hlášení.** Prostřednictvím grafických hlášení nebo pomocí protokolů událostí systému Microsoft Windows® či konzole Kaspersky Security Center. Nástroje pro hledání a filtrování poskytují rychlý přístup k datům v objemných protokolech.

KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization je flexibilní řešení, které nabízí vašemu prostředí jak ochranu tak výkon.

SECURITY VIRTUAL APPLIANCE (SVA)

Kaspersky Lab nabízí v tomto oboru dvě bezkonkurenční řešení, obě založená na produktu Security Virtual Appliance.

Kaspersky Lab Security Virtual Appliance (SVA) centrálně skenuje všechny VM hostitelského prostředí. Tato architektura nabízí účinnou ochranu virtuálních počítačů (VM) bez obětování zdrojů koncového bodu, eliminuje skenování AV, aktualizační „smrště“ a „instant-on gaps“ (proluky mezi vytvořením virtuálního zařízení a aktualizací jeho zabezpečení) a vytváří lepší poměry konsolidace.

INTEGRACE DO ARCHITEKTURY PLATFORMY

Kaspersky Security for Virtualization podporuje platformy VMware, Microsoft Hyper-V a Citrix Xen a jejich jádrové technologie.

VMware	Microsoft Hyper-V	Citrix Xen
High Availability	Dynamic Memory	Dynamic Memory Control
vCenter Integration	Cluster Shared Volumes	VM Protection & Recovery (VMPR)
vMotion – host DRS	Live Backup	Xenmotion (live migration)
Horizon view (full clones & linked clones)	Live Migration	Multi-Stream ICA
		Citrix Receiver
		Personal vDisk

LIGHT AGENT PRO POKROČILOU OCHRANU

Kaspersky Security for Virtualization zahrnuje účinného, ale nenáročného agenta, který je nasazen na každém virtuálním počítači. To umožňuje aktivaci pokročilých bezpečnostních funkcí koncových bodů. Ty zahrnují monitorování zranitelností, správu aplikací, zařízení a webu, antivirovou ochranu rychlých zpráv, mailu a webu, a pokročilou heuristiku. Výsledkem je účinné vícevrstvé zabezpečení kombinované s efektivním výkonem.

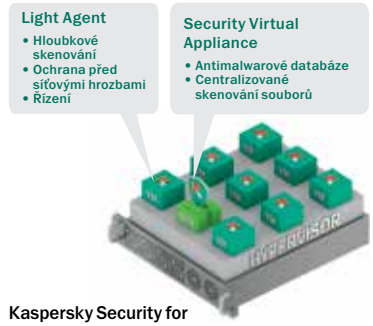
VOLITELNÁ KONFIGURACE BEZ AGENTA PRO PROSTŘEDÍ VMWARE

Vysoká úroveň integrace s technologiemi VMware znamená, že řešení Kaspersky Security for Virtualization může také být velmi snadno zavedeno a spravováno na této platformě v konfiguraci zabezpečení bez agenta. Všechny činnosti spojené se zabezpečením jsou soustředěny v Security Virtual Appliance ve spojení s vShield pro okamžitou automatickou ochranu virtuálních počítačů a s vCloud pro síťovou ochranu.

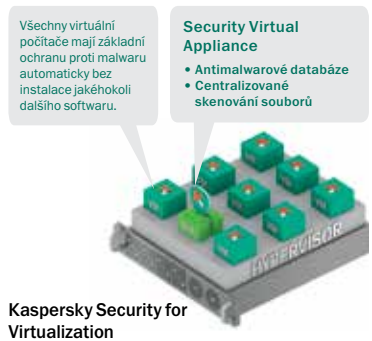
FLEXIBILNÍ LICENCOVÁNÍ

S ohledem na vaše potřeby je Kaspersky Security for Virtualization dostupné v těchto licenčních řešeních:

- Licencování podle počtu zařízení:
  - podle počtu dektopů,
  - podle počtu serverů.
- Licencování na základě množství zdrojů:
  - podle počtu jader.



Kaspersky Security for Virtualization
Konfigurace s light agentem



Kaspersky Security for Virtualization
Konfigurace bez agenta*

RŮZNÉ PLATFORMY: JEDNA CENA

Jedna licence Kaspersky Security for Virtualization zahrnuje podporu pro virtuální prostředí založené na Citrixu, Microsoftu a VMwaru.

KLÍČOVÉ FUNKCE PRODUKTU

- **Centralizovaná správa pomocí Kaspersky Security Center**
- **Centralizovaná ochrana VM na bázi SVA**
- **Pokročilá ochrana proti malwaru**
- **Host-based Intrusion Prevention (HIPS) a firewall**
- **Správa koncového bodu pro aplikace, webový přístup a periferní zařízení**
- **Zabezpečení na bázi cloudu pomocí Kaspersky Security Network**
- **Network attack blocker**
- **Ochrana proti phishingu**
- **Antivirus pro IM, e-mail a internetový provoz**
- **Žádné další instalace nebo restarty pro nové VM****

* Pokročilé funkce zabezpečení jako karanténa souborů, HIPS, skenování zranitelnosti a správa koncových bodů nejsou v této konfiguraci dostupné.
** Pro neperzistentní VM je okamžitá ochrana dostupná, když je light agent zahrnut do bitové kopie VM. Pro perzistentní VM musí administrátor zavést light agenta manuálně v průběhu instalace.

KASPERSKY LAB POBOČKY

Společnost Kaspersky podporuje místní podniky z poboček po celém světě. Více informací o způsobech zakoupení řešení Kaspersky Security for Business získáte u místního prodejce.


Kazachstán
Ruská federace
Ukrajina
Izrael
Turecko
Spojené arabské emiráty
Čína
Hongkong
Indie
Japonsko
Malajsie
Jižní Korea
Jihoafrická republika
Austrálie

Kaspersky Lab ZAO, Moskva, Rusko
www.kaspersky.com

Vše o internetovém zabezpečení:
www.securelist.com

Najděte svého partnera:
www.kaspersky.com/buyoffline

KASPERSKY lab