kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Security for Business
Select

Kaspersky Endpoint Security for Business Select poskytuje inteligentní ochranu pro celou řadu platforem – včetně serverů a koncových bodů Linux. Vícevrstvé zabezpečení, které detekuje podezřelé chování a blokuje hrozby, včetně ransomware, a v kombinaci s cloudovými ovládacími prvky snižuje vaši citlivost na útoky – a funkce správy mobilních zařízení vám pomohou chránit data v mobilních zařízeních.

Funkce ochrany a správy, které potřebujete
Společnost Kaspersky integrovala efektivní funkce pro firmy do progresivní řady našich produktů. Zajistili jsme, aby technologie byly nekomplikované a dostatečně flexibilní pro použití v libovolné rostoucí firmě.

Víceúrovňová ochrana pro
- systémy Windows, Linux a Mac
- servery Windows a Linux
- kontejnery Windows Server
- mobilní zařízení Android a další
- výměnná úložiště

Bezkonkurenční obrana před
- zneužitím softwaru
- ransomwarem
- mobilním malwarem
- pokročilými hrozbami
- bezsouborovými hrozbami
- útoky typu PowerShell a na principu skriptů
- webovými hrozbami

Zahrnuté funkce
- Ochrana proti malwaru
- Hodnocení zranitelných míst
- Security Policy Adviser
- Izolace procesů
- Exploit Prevention a Rollback
- Správa bran firewall a brány firewall operačního systému
- Ochrana za pomoci technologie cloud
- Úplná integrace s Kaspersky EDR Optimum NOVINKA
- Úplná integrace s Kaspersky Sandbox NOVINKA
- Integrace SIEM prostřednictvím Syslog
- Ovládání aplikací
- Správa webu a zařízení
- Ochrana serverů a kontejnerů
- Vzdálené vymazání dat NOVINKA
- Obrana mobilních zařízení před hrozbami
- Reporting
- Cloudová konzole NOVINKA
- Webové a MMC konzole

Podrobnosti naleznete na našich webových stránkách zde.

Pokročilá ochrana a řízení

Agilní, adaptivní zabezpečení

Kaspersky Endpoint Security for Business Select bylo navrženo pro zabezpečení libovolného IT prostředí. Celá sada osvědčených a inovativních technologií řeší i pokročilé a neznámé hrozby, čímž snižuje riziko a udržuje vaši organizaci, data a uživatele v bezpečí.

Bezproblémová integrace s novými službami Kaspersky EDR Optimum a Kaspersky Sandbox usnadňuje přidání výkonné automatizované detekce a reakčních funkcí do této bezpečnostní „zbrojnice".

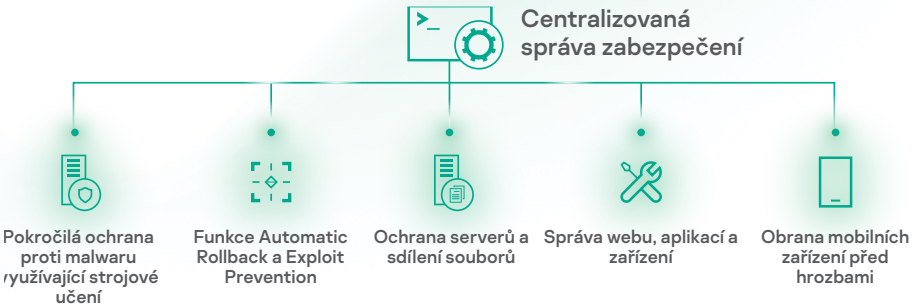
Centrální konzole pro správu – to nejlepší z obou světů

V cloudu, na místě nebo obojí? Rozhodnutí je na vás – a my vám zajistíme jednotnou správu prostřednictvím cloudové konzoly, nebo tradiční nasazení konzoly na místě, v cloudovém prostředí AWS nebo Azure.

Ať už zvolíte jakékoli řešení, naše konzole ve formě okna vám umožní zobrazit a spravovat celý bezpečnostní sektor a aplikovat vámi zvolené zásady zabezpečení na každý koncový bod, a to rychle a s minimem námahy za pomoci celé řady předkonfigurovaných scénářů.

Nejtestovanější a nejoceňovanější

Každoročně se naše produkty umísťují na čelních místech nezávislých testů a recenzí. Jsme hrdí na tento pozoruhodný výčet úspěchů a všechno uznání v rámci odvětví s ním spojené. A ještě více hrdí jsme na to, že naši zákazníci to vidí stejně, a trvale vyjadřují vysokou úroveň spokojenosti s našimi produkty a výkonem.



O Kaspersky EDR Optimum NOVINKA
(k zakoupení samostatně)

Funkce EDR již integrované do Kaspersky Endpoint Security for Business mohou být dále posíleny novou službou Kaspersky EDR Optimum. Výsledkem je úplná viditelnost a schopnost aplikovat analýzu kořenových příčin za účelem úplného porozumění stavu ochrany vaší společnosti před pokročilými hrozbami. Váš IT specialista na zabezpečení obdrží informace a přehledy potřebné pro účinné vyšetřování a rychlou a přesnou reakci na události, než dojde k případným škodám – a také základní funkce vyhledávání hrozeb (IoC skenování).

O Kaspersky Sandbox NOVINKA
(k zakoupení samostatně)

Kaspersky Sandbox automaticky chrání před pokročilými hrozbami schopnými obejít ochranu koncových bodů. Na základě technologie emulace dynamických hrozeb využívá Kaspersky Sandbox naše osvědčené postupy při boji proti komplexním hrozbám a útokům na úrovni APT, čímž zajistí automatizovanou reakci napříč všemi koncovými body.

Klíčové funkce

Základní ochrana

Naše základní prvky ochrany před hrozbami tvoří základ efektivního zabezpečení před běžnými hrozbami. Mezi ně patří ochrana před souborovými, webovými a mailovými hrozbami, brána firewall, ochrana před ohrožením sítě, prevence před útokem BadUSB a funkce AMSI Protection Provider.

Pokročilá ochrana před hrozbami na principu strojového učení

Prvky rozšířené ochrany, jež zahrnují **Kaspersky Security Network, Behavior Detection,** Anti-Ransomware Protection a Exploit Prevention, dokáží detekovat a odrazit i nové a neznámé hrozby. Funkce Behavior Detection, řízená statickým i dynamickým strojovým učením, analyzuje aktivitu procesů v reálném za účelem detekce nejsofistikovanějších hrozeb, například bezsouborového malwaru nebo útoků na principu skriptů. Jakmile je škodlivý proces identifikován a označen, je ukončen a funkce Remediation Engine vrátí zpět veškeré změny.

Cloudové ovládací prvky pro zdokonalení zásad a prevence narušení

Prevence průniku na bázi hostitele a centralizované **ovládání webu, zařízení** a **aplikací** redukují vaše zranitelná místa a pomáhají uživatele udržet v bezpečí a produktivní. Kaspersky Lab má svou vlastní vyhrazenou laboratoř pro dynamický whitelisting, která udržuje nepřetržitě sledovanou a aktualizovanou databázi více než 2,5 miliard důvěryhodných programů.

Flexibilní 360° správa

Kaspersky Security Center je centrální konzole pro správu, která správcům usnadňuje konfiguraci, nasazení, aktualizaci a správu zabezpečení. Zjednodušuje aplikaci skupinových úkolů, zásad, profilů zásad a vytváření zpráv.

Systémy Windows, Mac, Linux – vše je pokryto

Ochrana pro koncové body a servery Windows a Linux a pro pracovní stanice Mac – to vše je spravováno ze stejné konzole, což je ideální pro smíšená prostředí.

Správa a ochrana mobilních zařízení

Výkonný software na ochranu proti malwaru v kombinaci s cloudem řízeným vyhledáváním hrozeb chrání před nejnovějšími hrozbami. Funkce řízení webu a antiphishing zajišťují spolehlivé a bezpečné filtrování webu za účelem blokování přístupu na škodlivé a jiné nežádoucí webové stránky. Funkce správy mobilních zařízení a integrace se systémy EMM zjednodušují dodržování předpisů, povolování a celkové řízení.

Integrace pro rozšířenou prevenci, detekci a reakci NOVINKA

Kaspersky Endpoint Security for Windows je určen pro integraci do Kaspersky Sandbox a Kaspersky EDR Optimum pro pokročilou automatizovanou detekci a reakci.

Vyzkoušejte si sami

Proč si nevyzkoušet adaptivní ochranu proti pokročilým hrozbám, které cílí na vaši firmu? Navštivte tuto stránku, kde naleznete bezplatnou 30denní zkušební verzi aplikace Kaspersky Endpoint Security for Business.

Jsme prověření. Jsme nezávislí. Jsme transparentní. Zavázali jsme se k budování bezpečnějšího světa, ve kterém technologie zlepšují naše životy. Proto je zabezpečujeme, aby všichni lidé všude na světě mohli využívat nekonečné možnosti, které přinášejí. Pečujte o kybernetickou bezpečnost pro bezpečnější zítřky.

Zjistěte více na stránce kaspersky.com/transparency

Proven. Transparent. Independent.

Novinky v oblasti kybernetických hrozeb: www.securelist.com
Novinky v oblasti zabezpečení IT: business.kaspersky.com
Zabezpečení IT pro malé až střední podniky: kaspersky.com/business
Zabezpečení IT pro firmy: kaspersky.com/enterprise

www.kaspersky.com