kaspersky BRING ON THE FUTURE

Kaspersky Endpoint Security for Business

Advanced

Kaspersky Endpoint Security for Business Advanced kombinuje vícevrstvé zabezpečení s rozšířenými ovládacími nástroji pro zajištění efektivního řešení zabezpečení, které se rychle přizpůsobí za účelem ochrany proti novým hrozbám. Konzole pro správu zabezpečení a systémů šetří cenný čas a zdroje, zatímco další obranné vrstvy pomáhají eliminovat zranitelná místa a poskytují další ochranu citlivých dat.

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
- Správa zranitelných míst
- Security Policy Adviser
- 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
- Adaptive Anomaly Control
- Správa aplikací, webu
- a zařízení
- Ochrana serverů a kontejnerů
- Vzdálené vymazání dat NOVINKA
- Obrana mobilních zařízení před hrozbami
- Správa šifrování OS
- Konfigurace systému a nasazení
- Správa oprav
- Reporting
- Webové a MMC konzole

Podrobnosti naleznete na našich webových stránkách zde.

Pokročilá ochrana, řízení a správa systémů zabezpečení

Inteligentní zabezpečení pro koncové body a servery

Kaspersky Endpoint Security for Business Advanced byla navržena pro zabezpečení libovolného IT prostředí. Celá sada osvědčených a inovativních technologií, včetně Adaptive Anomaly Control, šifrování a automatizované správy oprav, řeší i pokročilé a neznámé hrozby, čímž snižuje riziko a udržuje vaši organizaci, data a uživatele v bezpečí.

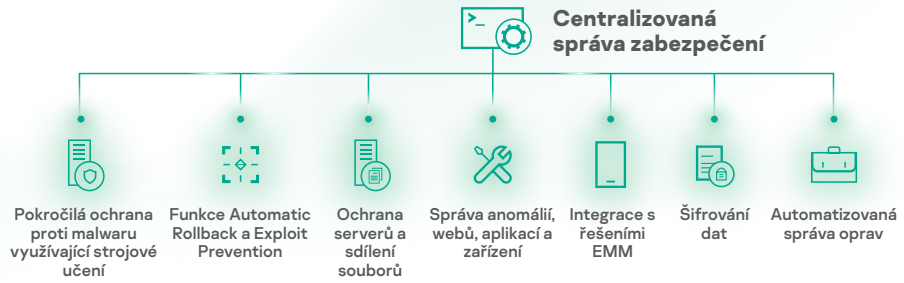
Nástroje pro správu systémů šetří čas a peníze, a bezproblémová integrace s novými službami Kaspersky EDR Optimum a Kaspersky Sandbox usnadňuje přidání výkonné automatizované detekce a reakčních funkcí do této bezpečnostní „zbrojnice".

Jedna konzole pro správu

Pomocí konzole pro správu ve formě okna mohou správci zobrazit a spravovat celý bezpečnostní sektor a aplikovat vámi zvolené zásady zabezpečení na každý koncový bod ve vašem podniku. To pomáhá s rychlou implementací zabezpečení s minimem přerušení a starostí za pomoci celé řady přednastavených 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 Adaptive Anomaly Control

Tato technologie automaticky pomáhá aplikovat nejvyšší přijatelnou úroveň zabezpečení pro každou roli v organizaci. Po prvním sledování konkrétních akcí a shromáždění informací o chování uživatelů a aplikací identifikuje a naučí se charakteristické vzorce chování, a to až po úroveň jednotlivých uživatelů. Pokud aplikace poté zobrazí abnormální chování v rozporu s tímto vzorcem, dojde k jejímu zablokování. To vše bez vyrušení koncových uživatelů.

O Kaspersky EDR Optimum NOVINKA

(prodáváno 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

(prodáváno 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

Vícevrstvá inteligentní ochrana

Ochrana před souborovými, webovými a mailovými hrozbami, brána firewall, ochrana před ohrožením sítě, prevence před útokem BadUSB a funkce AMSI Protection Provider poskytují základní ochranu, zatímco moderní ochranné prvky, mimo jiné HIPS, Kaspersky Security Network, Behavior Detection na principu strojového učení (s automatickou funkcí Roll-Back), ochrana před ransomwarem a funkce Exploit Prevention, dokáží detekovat a odrazit i nové a neznámé hrozby. Prevence průniku na bázi hostitele a centralizované ovládání webu, zařízení, aplikací a anomálií redukují vaše zranitelná místa a pomáhají uživatele udržet v bezpečí a produktivní.

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, řízení webu a antiphishing, možnosti správy mobilních zařízení a integrace do systémů EMM.

Šifrování a ochrana dat

Šifrování s certifikátem FIPS 140.2 a Common Criteria může být centrálně vyžadováno na úrovni souboru, disku nebo zařízení, s nativními šifrovacími nástroji, například Microsoft BitLocker a macOS FileVault.

Správa systému, zranitelných míst a oprav

Zjednodušení a centralizace úkolů správce za účelem úspory času a peněz, a také další zvyšování vašeho zabezpečení pomocí:

- pokročilého hloubkového skenování zranitelných míst a automatizované distribuce oprav
- času a zdrojů šetřícího nasazení OS a softwaru
- centralizovaného vytváření obrazu systému, ukládání a nasazení – ideální pro aktualizaci na systém Microsoft Windows 10
- Výkazy inventarizace hardwaru a softwaru – pro snazší řízení závazků ze softwarových licencí.

Flexibilní 360° správa

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

Integrace pro rozšířenou prevenci, detekci a reakci

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.

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

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.