

► KASPERSKY ENDPOINT SECURITY FOR BUSINESS Select

Nástroje pro podporu mobilních pracovníků, zajištění konformity bezpečnostních zásad IT a blokování malwaru.

Úroveň ‚Select‘ zahrnuje funkce pro ochranu a nasazování mobilních zařízení pomocí komponenty Mobile Device Management (MDM) a mobilní ochrany před malwarem. Nástroje pro kontrolu koncových bodů (web, zařízení a aplikace) pomáhají vaší organizaci uplatňovat IT zásady, a tak udržují bezpečnost životně důležitých prvků vašeho IT prostředí.

Funkce, které potřebujete pro ochranu a správu

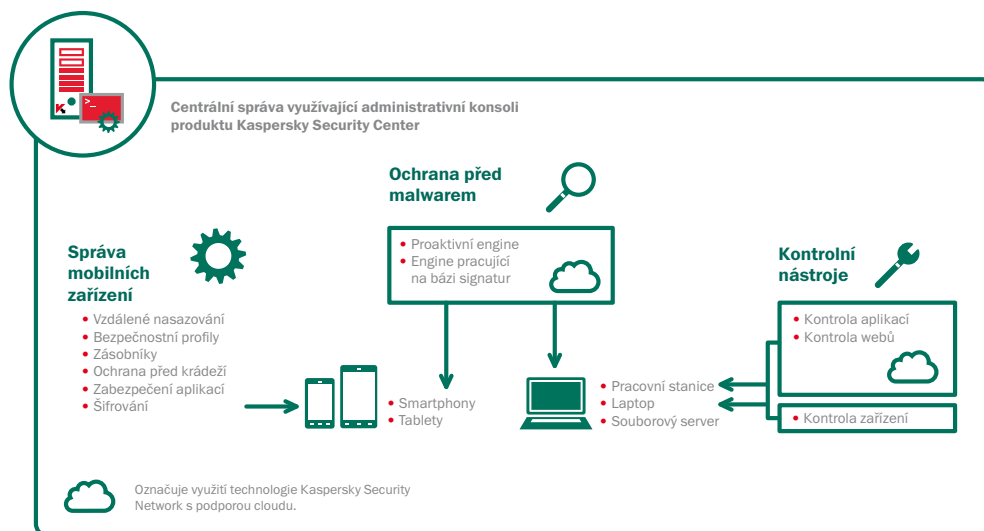
Společnost Kaspersky začlenila výkonné funkce do všech úrovní firemních produktů. Tyto technologie jsou však tak jednoduché a nekomplikované, že jsou vhodné pro jakoukoliv organizaci.

Která úroveň je pro vás nejvhodnější?

- CORE
- **SELECT**
- ADVANCED
- TOTAL

NEJVÝZNAMNĚJŠÍ FUNKCE:

- ANTI-MALWARE
- FIREWALL
- SÍŤ KASPERSKY SECURITY NETWORK S PODPOROU CLOUDU
- KONTROLA APLIKACÍ
- ZAŘAZOVÁNÍ APLIKACÍ NA TZV. WHITELIST
- KONTROLA WEBŮ
- KONTROLA ZAŘÍZENÍ
- OCHRANA SOUBOROVÉHO SERVERU
- SPRÁVA MOBILNÍCH ZAŘÍZENÍ
- ZABEZPEČENÍ MOBILNÍCH KONCOVÝCH ZAŘÍZENÍ (PRO TABLETY A SMARTPHONY)



HLAVNÍ RYSY:

VÝKONNÁ OCHRANA KONCOVÝCH ZAŘÍZENÍ PŘED MALWAREM

Skenovací stroje firmy Kaspersky pracují v operačním systému na více úrovních a odklánějí malware. Síť Kaspersky Security Network (KSN) s podporou cloudu chrání uživatele před novými hrozbami v reálném čase.

FLEXIBILNÍ, GRANULÁRNÍ NÁSTROJE KONTROLY

Na cloudu umístěná, kategorizovaná databáze bezpečných a nebezpečných aplikací a webů pomáhá administrátorům nastavit a uplatňovat pravidla pro aplikace a přístup k webu, přičemž granulární kontroly zajišťují, že se ke strojům na síti mohou připojit pouze určitá zařízení.

EFEKTIVNÍ MOBILNÍ NASAZOVÁNÍ 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 rozmisťovat bezdrátově s pomocí komponenty Kaspersky MDM.

FUNKCE PRO OCHRANU KONCOVÝCH BODŮ:

ČASTÉ AKTUALIZACE A OCHRANA S VYUŽITÍM SIGNATUR

Průmyslem ověřená tradiční metoda identifikace malwarových hrozeb na bázi signatur.

BEHAVIORÁLNÍ ANALÝZA PROVÁDĚNÁ KOMPONENTOU SYSTEM WATCHER

Zajišťuje proaktivní ochranu před hrozbami, které ještě nebyly zaznamenány v databázích signatur.

OCHRANA S PODPOROU CLOUDU

Síť Kaspersky Security Network (KSN) zajišťuje podstatně kratší odezvu na podezřelé hrozby než tradiční způsoby ochrany. Doba odezvy sítě KSN na hrozbu malwaru může být pouhých 0,02 sekundy!

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

Předem definovaná pravidla pro stovky nejběžnějších aplikací zkracují dobu nutnou pro konfiguraci firewallu.

KONTROLY KONCOVÝCH ZAŘÍZENÍ:

KONTROLA APLIKACÍ

Umožňuje IT administrátorům nastavovat pravidla, která povolují, blokují nebo regulují aplikace (nebo kategorie aplikací).

KONTROLA WEBŮ

Znamená, že kontroly pro přístup k webu na bázi koncového zařízení jsou vázány na uživatele – ať v podnikové síti, nebo při vzdáleném přístupu.

KONTROLA ZAŘÍZENÍ

Umožňuje uživatelům nastavit, plánovat a uplatňovat datová pravidla pro vyměnitelné paměti a další periferní zařízení bez ohledu na to, zda se připojují přes USB nebo pomocí jiné sběrnice.

DYNAMICKÝ ZÁPIS NA TZV. WHITELIST

FUNKCE PRO ZAJIŠTĚNÍ BEZPEČNOSTI MOBILNÍCH ZAŘÍZENÍ:

INOVATIVNÍ TECHNOLOGIE OCHRANY PŘED MALWAREM

Výsledkem kombinované proaktivní detekce na bázi signatur s podporou cloudu je ochrana v reálném čase. Bezpečný webový prohlížeč a řešení ochrany před spamem zvyšují bezpečnost.

ROZMISŤOVÁNÍ SE PODPOROU OTA (OVER THE AIR)

Možnost centrální předběžné konfigurace a nasazování aplikací s použitím SMS, e-mailu a PC.

NÁSTROJE PRO VZDÁLENOU OCHRANU PŘED KRÁDEŽÍ

Funkce SIM-Watch, Remote Lock, Wipe and Find zabraňují neoprávněnému přístupu k podnikovým datům v případě krádeže nebo ztráty mobilního zařízení.

KONTROLA APLIKACÍ PRO MOBILNÍ ZAŘÍZENÍ

Monitoruje aplikace instalované v mobilním zařízení podle předem definovaných skupinových pravidel. Obsahuje skupinu „povinné aplikace“.

PODPORA PRO ZAŘÍZENÍ VE VLASTNICTVÍ ZAMĚSTNANCŮ

Podniková data a aplikace jsou izolovány v šifrovaných zásobnících, které jsou však pro uživatele transparentní. Tato data lze samostatně smazat.

► JEDINÁ SKUTEČNĚ BEZPEČNOSTNÍ PLATFORMA

Jedna konsole pro správu

Administrátor má z jedné obrazovky přehled o celé bezpečnostní situaci a může provádět správu virtuálních strojů, stejně jako fyzických a mobilních zařízení.

Jedna bezpečnostní platforma

Společnost Kaspersky Lab vyvinula všechny součásti tohoto řešení sama, bez pomoci třetích stran. To znamená, že stejní programátoři využívali stejný kód a vytvořili tak technologie, které si spolu dokonale rozumějí a spolupracují. Výsledkem je stabilita celého řešení, integrované zásady, jednoduchý reporting a intuitivní využití různých nástrojů.

Jedna cena

Všechny nástroje jsou od jednoho dodavatele a jsou součástí jedné instalace, takže nemusíte procházet novými procesy zdůvodňování a rozpočtování, abyste uvedli do souladu svá bezpečnostní rizika a cíle podniku.

NE VŠECHNY FUNKCE JSOU K DISPOZICI NA VŠECH PLATFORMÁCH.

Pro další informace navštivte www.kaspersky.com

KESB-S/Version 0.1/Nov12/Global

© 2012 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners. Windows is a registered trademark of Microsoft Corporation in the United States and other countries. Android is a trademark of Google, Inc. The Trademark BlackBerry is owned by Research In Motion Limited and is registered in the United States and may be pending or registered in other countries.

KASPERSKY Lab