

Kaspersky® Anti-Virus pro Linux

Kaspersky® AV na platformě Linux je unikátní řešení zabezpečující kompletní antivirovou ochranu stanic, datových a aplikačních serverů a e-mailových bran běžících pod operačními systémy Linux a Unix (FreeBSD a BSDi).

Kaspersky® Anti-Virus pro stanice Linux

Obsahuje:

- **Kavscanner** pro dávkové kontroly / odvírování připojených filesystémů.
- **Aveserver** se spouští při startu a na základě požadavků aveclient provádí antivirovou.
- **Aveclient** dostává požadavek na skenování souborů z příkazové řádky, předá je daemonu aveserver a vypracuje zprávu o výsledku kontroly ve formě vhodné pro další zpracování.
- **Kavupdater** provádí aktualizaci virových databází několikrát denně z vybraného zdroje.

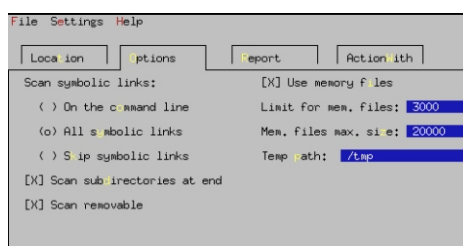
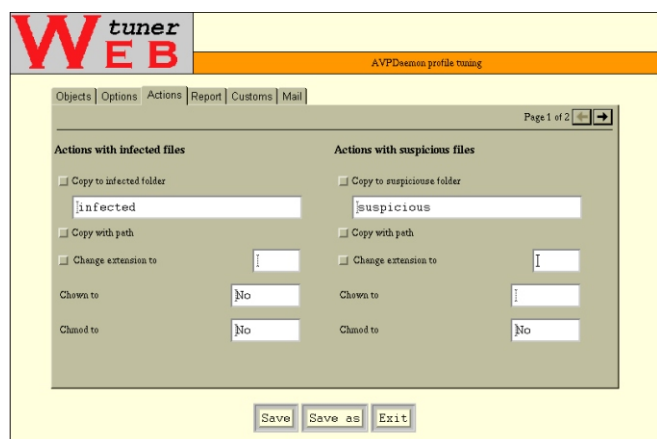
Kaspersky® Anti-Virus pro Linux/Unix file server

Systém antivirové ochrany pro datové a aplikační servery běžící pod Linuxem /Unixem (FreeBSD, OpenBSD, BSDi, Solaris).

Kaspersky® Anti-Virus pro Linux mail servery

Kaspersky® Anti-Virus zahrnuje předem připravené řešení pro integraci produktu do Sendmail, Qmail, Postfix a Exim. Je to perfektní řešení pro vytvoření vlastního centralizovaného systému pro filtrování e-mailového provozu a očistění od virů. Hlavní vlastnosti KAV pro Sendmail, Qmail, Postfix a Exim jsou:

- Skenování souborů a odstraňování počítačových virů a dalších škodlivých kódů v reálném čase („on-the-fly“).
- Plná centralizovaná kontrola nad interní i externí e-mailovou komunikací (z hlediska šíření potenciální virové infekce).
- Přesun infikovaných a podezřelých e-mailových zpráv na stanovenou adresu.
- Volitelné nastavení zpráv upozorňujících na virový incident.
- Vysoká integrace antivirového programu do administrátorského rozhraní.
- Snadné nastavení programu.



Kaspersky® Anti-Hacker - personální firewall

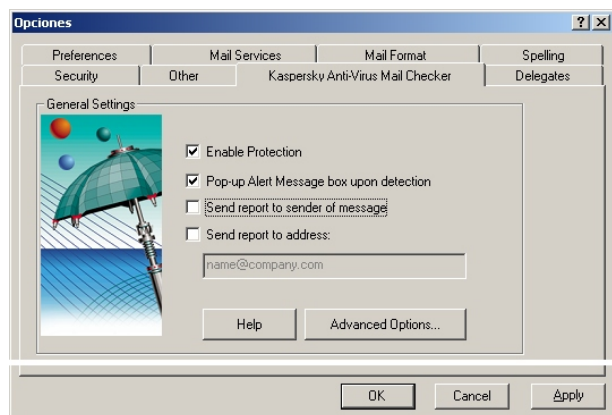
Kaspersky® Anti-Hacker je personální firewall, který poskytuje komplexní ochranu PC běžícím pod Windows před pokusy o neoprávněný přístup k datům a před útoky hackerů jak z Internetu, tak z Intranetu.

- **Komplexní kontrola síťových aktivit** - Kaspersky® Anti-Hacker umožňuje kontrolu síťové aktivity systému pomocí dvouúrovňové analýzy.
- **Sledování aktivit aplikací spojených s Internetem - (vysoká úroveň)**. Integrovaná analýza aktivit aplikací spojených s Internetem jako jsou webové prohlížeče, aplikace pošty, aplikace přenosu dat, atd.
- **Filtrace paketů příchozích a odchozích dat - (nízká úroveň)**. Kaspersky® Anti-Hacker na této úrovni přímo analyzuje pakety, odeslané nebo přijaté na počítač.
- **Nastavení pravidel filtrace** - na základě požadavků uživatele umožňuje tvorbu nebo změnu pravidel pro sledování aktivit aplikace stejně.
- **Úrovně zabezpečení podle přání zákazníka** - Kaspersky® Anti-Hacker umožňuje na základě požadavků uživatele výběr z pěti úrovní zabezpečení, od úplného vypnutí ochrany až po úplnou blokadu veškerých internetových spojení. Pro každou z těchto úrovní lze stanovit pravidla zabezpečení a filtrace paketů.
- **Efektivní ochrana proti známým typům hackerských útoků** - Kaspersky® Anti-Hacker částečně funguje v automatickém režimu. Díky technologii SmartStealth™ je obtížnější detekovat Váš počítač zvnějšku. Tento režim umožňuje úspěšnou prevenci hackerských útoků včetně DoS (Denial of Service), ale nemá žádný negativní účinek na výkonnost počítače.
- **Samoučící se systém** - Kaspersky® Anti-Hacker umožňuje rozšířit seznam bezpečnostních pravidel aplikací připojených k Internetu pomocí samoučících se funkcí.
- **Kontrola integrity spustitelných souborů** - Kaspersky® Anti-Hacker chrání aplikace před nepovolenými pokusy o nahrazení původních spustitelných souborů. Kontrola integrity spustitelných souborů je prováděna na základě kontrolních součtů (CRC).

Kaspersky® Antispam - Výkonná filtrace zpráv

Kaspersky® Anti-Spam kombinuje **čtyři metody pro analýzu příchozí zprávy**. Nejdříve je zpráva kontrolována pomocí **jádra SpamTest™**, které používá metodu unikátního rozpoznání obsahu a které dokáže oddělit spamové zprávy od běžných mailů. Potom je použita **metoda podpisu** každá zpráva je porovnávána se **vzory**, které jsou uloženy v denně aktualizované databázi.

Dále jsou použity formální charakteristiky zpráv, např. adresa odesílatele, metoda distribuce, atd. Nakonec je použit tzv. **«black list»**, standardní metoda filtrování zpráv, která je založena na seznamu adres, které jsou označeny jako zdroje spamu. Tyto adresy jsou uloženy v denně aktualizované databázi.



Kaspersky® Anti-Spam filtruje obsah všech součástí zprávy (včetně záhlaví a příloh) a zpracovává přílohy, které jsou uloženy ve formátu Plain Text ASCII, HTML, MS Word 6.0 a RTF.

Vícejazyčná podpora - Kaspersky® Anti-Spam pracuje s jazykovými moduly pro angličtinu, ruštinu, němčinu, francouzštinu a španělštinu.

