



*Produsele Business Kaspersky Lab sunt create pentru a proteja chiar și cele mai complexe și dinamice sisteme de rețea: produsele noastre includ suport pentru toate tipurile de noduri de rețea și platforme, precum și o scalabilitate avansată.*

## Solutii Anti-Virus pentru Check Point Firewall-1

activone.ro



Kaspersky Anti-Virus for Check Point Firewall-1 furnizează o protecție de înaltă calitate pentru întreg traficul HTTP, FTP și SMTP care trece prin Check Point FireWall-1. Soluția detectează programe periculoase, programe de tip spyware, adware etc.

### Funcții

- Protecție antivirus
- Administrare și configurare
- Cerințe de sistem

### Protecție antivirus

**Scanare antivirus a traficului de intrare și ieșire.** Aplicația scanează traficul de intrare și ieșire împotriva virușilor, procesează cerințele CVP din paravanul de protecție. Obiectele scanate includ traficul web, conținutul și atașamentele e-mailurilor, inclusiv fișierele arhivate și comprimate. Soluția nu detectează doar obiectele infectate, ci și obiectele ce pot fi catalogate ca suspecte, protejate de parole sau deteriorate.

**Protecție împotriva programelor cu potențial ostil.** Administratorii pot alege fie baza de date antivirus standard fie pe cea extinsă. Astfel soluția detectează nu numai programele periculoase, ci și pe cele potențial ostile de tip spyware etc.

**Selecție a tipurilor de fișiere pentru o mai mare viteză de scanare.** Se pot exclude de la scanare fișierele arhivate sau se poate configura aplicația pentru a scana doar fișierele arhivate până la un anumit nivel. Aplicația poate fi configurată să scaneze doar anumite tipuri de fișiere (tipul de fișier este definit de structura internă), ceea ce înseamnă că doar obiectele predispușe la infectare sunt scanate.

**Limită de timp pentru scanarea fiecărui obiect.** Administratorul poate seta o perioadă maximă de timp pentru scanarea fiecărui obiect pentru a reduce orice întrerupere a activității utilizatorului.

**Scanare instantanee.** Pentru a spori performanța aplicației obiectele sunt scanate în RAM fără a le salva pe disc.

**Algoritmi inteligenți.** În timpul scanării, obiectele sigure sunt transmise utilizatorului final folosind algoritmi inteligenți care măresc viteza de operare a aplicației fără a afecta calitatea detecției.

**Opțiuni de procesare pentru obiectele infectate.** Obiectele infectate pot fi șterse sau dezinfectate. De asemenea, este posibilă ignorarea rezultatelor scanării - adică obiectul să fie trimis utilizatorului final fără a fi procesat.

**Copii de rezervă.** Înainte de procesarea obiectelor infectate (dezinfectate sau șterse), este posibil să fie create copii de rezervă ale acestora. Administratorul poate configura copierea de rezervă, pentru fiecare protocol de transfer de date în parte.

### **Administrare și configurare**

**Administrare convenabilă.** Interfața administrativă este bazată pe Microsoft Management Console 1.2, ceea ce este un instrument familiar pentru majoritatea administratorilor de sistem.

**Scalabilitate.** Administratorul de sistem poate alege să utilizeze copii multiple ale motorului antivirus și servere multiple CVP (care pot opera pe servere diferite).

**Actualizări automate ale bazei de date antivirus.** Actualizările bazei de date antivirus pot fi descărcate pe stațiile de lucru direct de pe serverele de Internet Kaspersky Lab sau de pe un fișier al rețelei locale. În cazul în care actualizările sunt deteriorate sau incomplete, este posibilă restaurarea unei bazei de date antivirus anterioară.

**Sistem de sofisticat de notificare.** Produsul poate trimite notificări administratorului de sistem despre orice eveniment critic din timpul operațiunilor aplicației, fie folosind instrumentele clasice Check Point Firewall-1<sup>®</sup> fie prin e-mail.

**Sistem de raportare îmbunătățit.** Setările flexibile pentru configurarea statisticilor și rapoartelor, permit administratorului de sistem să aleagă detaliile dorite pentru colectarea de date și întocmirea de rapoarte.

**Suport tehnic gratuit.** Utilizatorii înregistrați au acces la serviciul de suport tehnic gratuit al Kaspersky Lab prin telefon și e-mail. Specialiștii tehnici sunt disponibili 24 ore pe zi, 7 zile din 7, pentru a răspunde întrebărilor legate de instalare, configurare și utilizare a aplicației în engleză, franceză, germană și rusă.

### **Server administrare :**

#### **Cerințe hardware :**

Procesor Intel Pentium processor, 300 MHz sau mai performant;

Cel puțin 512 MB RAM disponibil

Cel puțin 20 MB spațiu liber pe disc pentru instalare (nu include spațiul necesar pentru stocarea de rezervă și alte fișiere necesare pentru funcționarea soluției)

Cel puțin 1 GB spațiu disponibil pe disc pentru stocarea de rezervă a fișierelor și stocarea temporară a datelor ce urmează a fi scanate).

#### **Cerințe software :**

Microsoft Windows 2000 Professional cu Service Pack 4 sau mai recent

Microsoft Windows XP Professional Edition cu Service Pack 2 sau mai recent

Microsoft Windows 2000 Server cu Service Pack 4 sau mai recent

Microsoft Windows 2000 Advanced Server cu Service Pack 4 sau mai recent  
Microsoft Windows Server 2003 Standard Edition sau mai recent  
Microsoft Windows Server 2003 Enterprise Edition sau mai recent.

**Consola de administrare :**

**Cerințe hardware :**

Procesor Intel Pentium II 300 MHz sau mai performant  
256 MB RAM;  
10 MB spațiu liber pe disc.

**Cerințe software :**

Microsoft Windows 2000 Professional cu Service Pack 4 sau mai recent  
Microsoft Windows XP Professional Edition cu Service Pack 2 sau mai recent  
Microsoft Windows 2000 Server cu Service Pack 4 sau mai recent  
Microsoft Windows 2000 Advanced Server cu Service Pack 4 sau mai recent  
Microsoft Windows Server 2003 Standard Edition sau mai recent  
Microsoft Windows Server 2003 Enterprise Edition sau mai recent.