

Kaspersky® **Anti-Virus**

for Check Point Firewall-1

Kaspersky® Anti-Virus for Check Point Firewall-1 provides high-quality antivirus protection for all HTTP, FTP and SMTP traffic that passes through Check Point Firewall-1. The solution detects malicious programs, spyware, adware, joke programs, etc.

Kaspersky Anti-Virus for Check Point Firewall-1 is compatible with the family of Microsoft Windows operating systems, and is fully optimized to meet the demands of large organizations that have heavy volumes of traffic. Advantages of the solution include high performance, advanced scalability and support for the latest hardware platforms.

Main advantages

Reliable protection

Kaspersky Lab is a technological leader in the information security industry. Kaspersky Lab's antivirus solutions not only boast the highest detection rates of malicious programs, but also detect and treat viruses in web traffic, email messages and attachments (including archives and compressed files).

Free technical support

Registered users have access to Kaspersky Lab's free technical support service. Technical specialists are available round-the-clock to answer questions related to the installation, configuration and use of the product in English, French, German and Russian.

Scalability and flexibility

The system administrator can choose to run multiple copies of the antivirus engine and multiple CVP servers (which can operate on different physical servers).

Optimized for Intel Xeon

The solution is optimized for use on computers with the most up-to-date hardware components, such as Intel Xeon processors.

Simple and convenient administration

The administrative interface is based on the Microsoft Management Console, which is a familiar tool for most system administrators.

Product capabilities

Antivirus protection

Antivirus scanning. The application scans all objects in incoming and outgoing traffic for viruses, processing CVP requests from the firewall. The program detects not only infected objects, but also objects that can be classed as suspicious, secure or damaged, as well as attachments.

Protection from potentially malicious programs. Administrators can choose to use either a standard or extended set of antivirus databases. This enables the program to detect not only malicious programs, but also malicious software, spyware, joke programs, etc.

Excluding file types for faster scanning. It is possible to exclude archive files from scanning altogether, or to configure the program to scan only archives below a certain nesting level. The program can be configured to scan only certain types of files (file type is defined by internal structure), which means that only objects prone to infection are scanned.

Limiting time spent on scanning each object. The administrator can set a maximum time for scanning each object to minimize any disruption to the user.

On-the-fly scanning. To increase the application's performance, objects are scanned in the operating memory.

Intelligent algorithms. During scanning, safe objects are forwarded to the end user using intelligent algorithms that speed up the application's operation without sacrificing detection quality.

Processing options for infected objects. Infected objects can either be deleted or treated. It is also possible to disregard the scan result – that is, to send the object to the end user without processing.

Administration and configuration

Convenient administration

The administrative interface is based on the Microsoft Management Console, which is a familiar tool for most system administrators.

Sophisticated notification system

The product can send notifications to the system administrator about any critical events in the application's operation, either using the tools in Check Point Firewall-1 or via email.

Improved reporting system

Flexible settings for configuring statistics and reports allow the system administrator to choose the desired detail for data collection and reports.

Services

Backup copies. Before infected objects are processed (treated or deleted), it is possible to create backup copies of them. The administrator can configure backup copying for each data transfer protocol separately.

Automatic updates to antivirus databases. Updates to antivirus databases can be downloaded to workstations directly from Kaspersky Lab servers or from a folder on the local network. If updates are damaged or incomplete, it is possible to roll back antivirus databases to a previous intact version.

Straightforward licensing scheme. Our economical and easy-to-use licensing system is designed to make sense to users. The product is licensed per user.

System requirements

Administrative server

Hardware requirements

- Intel Pentium processor, 300 MHz or higher
- Intel Pentium processor, 300 MHz or higher
- At least 512 MB RAM
- At least 20 MB available HDD space for program installation (not including space needed for backup storage and other catalogues)
- No less than 1 GB available HDD space for backup storage of files and temporary storage of data awaiting scanning)

Management console

Hardware requirements

- Intel Pentium II processor, 300 MHz or higher
- 256 MB RAM
- 10 MB available HDD space

Software requirements

- Microsoft Windows 2000 Professional with Service Pack 4 or higher
- Microsoft Windows XP Professional Edition with Service Pack 2 or higher
- Microsoft Windows 2000 Server with Service Pack 4 or higher
- Microsoft Windows 2000 Advanced Server with Service Pack 4 or higher
- Microsoft Windows Server 2003 Standard Edition or higher
- Microsoft Windows Server 2003 Enterprise Edition or higher

Languages: English, Russian
Version: 5.5

Contact information:

Kaspersky Lab HQ

10, bld 1,
1st Volokolamskii Proyezd
Moscow 123060
Russian Federation
Phone: +7 495 797 8700
www. kaspersky.com
Email: sales@kaspersky.com



©2006 Kaspersky Lab Ltd.

Kaspersky® Anti-Virus and Kaspersky® Security are registered trademarks of Kaspersky Lab Ltd. Intel, the Intel logo, Xeon, and Xeon Inside are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

All other names and trademarks are the copyrighted work of their respective owners.