▶ KASPERSKY ANTI-VIRUS FOR WINDOWS® SERVERS ENTERPRISE EDITION

Kaspersky Anti-Virus for Windows® Servers Enterprise Edition protects data on servers using Microsoft® Windows® operating systems. The product has been developed specifically for high performance corporate servers.

The file server is an essential part of a modern company's network and is used for storing and exchanging data. File servers are used to store intellectual property, some of the most valuable assets that a company can have, and lost or damaged data can cause irreparable damage to a business. The server can become infected via end-user PCs and other external devices connected directly to it. Large corporate networks will typically comprise server clusters and terminal servers which makes the network infrastructure more complex and vulnerable to potential threats. File servers therefore require the type of protection that can only be provided by dedicated software. Kaspersky Anti-Virus for Windows® Servers Enterprise Edition is a modern solution designed to protect high-performance file servers from malware.

Application Highlights

EXTRA PROTECTION FROM VIRUSES, WORMS AND TROJANS
An anti-malware engine ensures faster scans and lower use of system resources.

VMWARE READY
The application is certified compatible with the VMware virtualization platform.

CITRIX READY
The application is certified with Citrix solutions, including Citrix XenApp 6.0, 6.5 and XenDesktop 7.0, 7.1.

▶ APPLICATION FEATURES

Effective protection against malicious programs

Always-on antivirus protection and on-demand scanning. The application scans every file that is launched or modified and treats, deletes or quarantines any suspicious objects. If new software is installed or a file infection is suspected, the administrator can also launch a targeted antivirus scan of the suspect areas.

Proactive protection from malware. The anti-malware engine incorporates advanced anti-malware protection methods such as an heuristic analyzer capable of identifying malicious programs with a very high degree of accuracy, even if its signature has not yet been added to the antivirus databases.

Scanning the operating system's critical areas. A dedicated task can be run to scan those areas of the operating system that are most exposed to infection. For example, scanning autorun files can help prevent a virus from launching during system startup or detect any hidden processes.

Flexible scan settings. The file scan settings enable the administrator to: exempt certain processes from scanning; set the depth of antivirus protection; specify which file types must always be scanned and which should be exempted completely and preset responses to suspicious and infected objects according to threat type. This approach helps optimize the server load and ensures the flexible management of corporate network security.

Terminal and Virtual server protection. The application protects Microsoft® Terminal Services and Citrix XenApp servers, ensuring that end-users working in desktop/application publishing modes remain protected and are notified of events using the terminal services. Hyper-V, XenDesktop and VMware environments are also supported.

Cluster support. The application is ideally suited to the complex server cluster architecture typically found in large companies. It protects the local disks of the server's file system as well as the cluster's shared disks currently owned by the protected node.
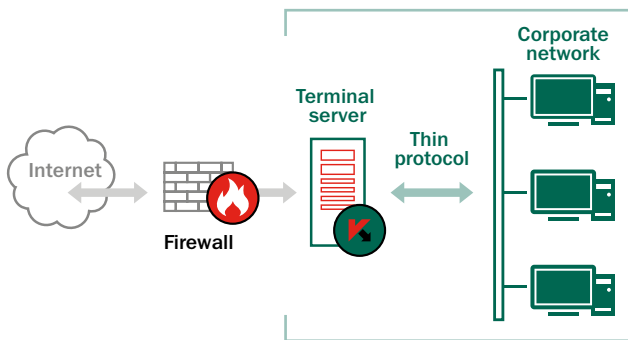
Terminal server protection by Kaspersky Anti-Virus for WSEE

High performance

Scalability. On multiple-processor servers, the administrator can specify the number of antivirus threads to ensure server requests are processed faster.

Load balancing. The application helps allocate the server's resources between the antivirus solution and other applications according to preassigned priorities: antivirus scanning can run in background mode.

Selection of trusted processes. The administrator can exempt secure processes such as data backups or defragmentation of the hard drive from scanning if their performance is affected by the scanning process.

Uninterrupted server operation. Kaspersky Anti-Virus for Windows® Servers Enterprise Edition does not require the server to be rebooted when the antivirus protection is installed or updated. Rebooting the server is undesirable/not an option for most corporate networks.

Flexible administration

Selection of management tools. The application can be managed either directly or remotely via the Microsoft® Management Console, Kaspersky Security Center, or by using the command line. The latest version of the product provides an intuitive graphical interface for the Microsoft® Management Console.

Centralized installation and management. The application supports the distributed logging of events and the storage of statistics on all protected servers.

Easy-to-use installation and management tools. Kaspersky Security Center is a management consolethat supports the remote installation and configuration of the application simultaneously on several servers, as well as helping to manage its operation and to receive updates and notifications.

Control over administrator privileges. The application enables various privilege levels to be assigned to each server's administrator, allowing any IT department-specific or internal security requirements to be met.

Flexible setting of scan times. To ensure the best use of server resources and minimize disruption to users, antivirus scan start and finish times can be set exactly. This limits on-demand scans to periods of minimum server load, such as at night or at weekends.

Notification system. The application supports administrator notifications via the messaging service or email for an extensive event list. The application is integrated with Simple Network Management Protocol (SNMP) and can operate with Microsoft® Operations Manager (MOM), or the administrator can monitor the application's operation by reviewing Microsoft® Windows® or Kaspersky Security Center event logs.

▶ SYSTEM REQUIREMENTS

Supported operating systems:
- Microsoft® Windows Server® Standard/ Professional/ Data Center
- Microsoft® Windows Server® 2012 R2 Standard/ Professional/ Data Center Microsoft® Windows Server® 2008 R2
- Microsoft® Windows Server® 2008 x86/x64
- Microsoft® Windows Server® 2003 R2 x86/x64
- Microsoft® Windows Server® 2003 x86/x64
- Microsoft Windows Hyper-V Server 2012/2012 R2
- Microsoft Windows Hyper-V Server 2008 R2
- Citrix XenDesktop 7.0, 7.1

Management console:
- Microsoft® Windows® 7 Professional x86/x64
- Microsoft® Windows® XP Professional x86/x64
- Microsoft® Windows Vista® x86/x64

Minimum hardware requirements:
- Processor – Intel® Pentium® IV
- Processing speed 2.4 GHz
- RAM: 512 MB
- Disk drive subsystem – 1 IDE drive

How to buy

Kaspersky Anti-Virus for Windows® Servers Enterprise Edition can be purchased as part of:
Kaspersky Endpoint Security for Business – Select
Kaspersky Endpoint Security for Business – Advanced
Kaspersky Total Security for Business

It can also be purchased as part of the Targeted Solution Kaspersky Security for File Server.

A list of Kaspersky Lab partners is available at: **www.kaspersky.com/buyoffline**.

To learn more visit: www.kaspersky.com

KASPERSKY🄱