KASPERSKY SECURITY FOR WINDOWS SERVER™

Developed specifically for high performance corporate servers

As the complexity of corporate IT networks escalates, the highest levels of server protection are required. A single infected file on your corporate server can spread to every computer on your network, doing untold damage. An appropriate dedicated server security solution not only ensures that your critical data is protected against the latest malware threats, but also eliminates the danger of malware penetrating backup copies of files, leading to repeated outbreaks.

Kaspersky Security for Windows Server provides cost-effective, reliable, scalable security for shared file storage, with minimal impact on resources.

Application Highlights

PROTECTION FROM KNOWN, UNKNOWN AND ADVANCED MALWARE
Our industry-leading anti-malware engine ensures faster scans and less impact on system resources, providing the highest detection rate supported by cloud-assisted security (Kaspersky Security Network).

ADVANCED SECURITY FOR CRITICAL SERVERS
Powerful Application Launch Control in combination with Global Security Intelligence and Anti-Cryptor functionality adds further layers of advanced protection for your corporate storages and servers.

CERTIFIED SOLUTION
The application is certified compatible with virtualization platforms and operational systems.

Application Features

EFFECTIVE PROTECTION AGAINST MALICIOUS PROGRAMS

Always-on anti-malware protection and on-demand scanning. The application scans every file launched or modified, treating, deleting or quarantining any suspicious objects. If new software is installed or a file infection is suspected, the administrator can also launch an anti-malware scan targeting the suspect areas.

Cloud-assisted server protection. Kaspersky Security Network (KSN) delivers a faster than ever response to new threats, improving the performance of protection components and minimizing the risk of false positives.

Powerful Application Launch Control on servers. Providing unprecedented security by using configured rules to allow or block the startup of executable files, scripts, and MSI packages, or the loading of DLL modules onto servers.

Protecting shared folders from crypto-malware (Anti-Cryptor). When file encryption activity is detected, the application blocks the originating machine from accessing any network file resources.

Blocking access from hosts with suspicious activity. Functionality that blocks computer access to shared network folders on a protected server if any malicious activity has been shown by those computers while running the Real-Time File Protection or Anti-Cryptor tasks.

Proactive protection from malware. Advanced anti-malware protection technologies, including a heuristic analyzer, capable of identifying malicious programs with a very high degree of accuracy, even if its signature has not yet been added to anti-malware 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 malware from launching during system startup and can detect any hidden processes.

Flexible scan settings. The file scan settings enable the administrator to:

- Exempt certain processes from scanning
- Set the depth of protection
- Specify which file types must always be scanned and which should be exempted
- 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. Hyper-V, XenDesktop and VMware™ environments are also supported.

Cluster support. The application is ideally suited to a complex server cluster architecture, protecting both local disks and the cluster's shared disks currently owned by the protected node.

High performance

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

Load balancing. Resources can be allocated between Kaspersky Security for Windows Server and other applications according to pre-assigned priorities: anti-malware scans can also 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 for performance optimization purposes.

Uninterrupted server operation. Kaspersky Security for Windows Server does not require a server to be rebooted whenever anti-malware protection is installed or updated.

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.

Easy-to-use installation and management tools. Kaspersky Security Center is a management console that 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 IT Department-specific or internal security compliance requirements to be met.

Flexible setting of scan times. To minimize disruption and boost the availability of server resources, it's easy to set scanning start and finish times.

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.

How to buy

Kaspersky Security for Windows Server can be purchased as part of:

- Kaspersky Endpoint Security for Business – Select (excluding Application Launch Control)
- 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 and Kaspersky Security for Storage.

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

To learn more visit: www.kaspersky.com

SYSTEM REQUIREMENTS

- Kaspersky Security for Windows Server is designed for servers running either 32-bit or 64-bit versions of Microsoft Windows:
  - Microsoft Windows Server 2008 / 2008 R2 x86/x64 Standard / Enterprise / Datacenter SP1 or later (including Core mode)
  - Microsoft Windows Hyper-V Server 2008 R2 SP1 or later
  - Microsoft Windows Server 2012 / 2012 R2 Essentials / Standard / Foundation / Datacenter (including Core mode)
  - Microsoft Windows Hyper-V® Server 2012 / 2012 R2

- Kaspersky Security for Windows Server can be installed on the following terminal servers
  - Microsoft Remote Desktop Services based on Windows 2008 Server
  - Microsoft Remote Desktop Services based on Windows 2008 / 2012 / 2012 R2 Server
  - Citrix® XenApp® 6.0, 6.5, 7.0, 7.5, 7.6
  - Citrix XenDesktop® 7.0, 7.1, 7.5, 7.6.

Management console:

- Microsoft Windows XP SP2 / Vista® / 7 / 8 / 10 Enterprise / Professional x86/x64
- Microsoft Windows Server 2008 / 2008 R2 Standard / Enterprise / Datacenter SP1 or later x64
- Microsoft Windows Server 2012 / 2012 R2 Essentials / Standard / Foundation / Datacenter x64
- Microsoft Windows Hyper-V Server 2008 R2 SP1 / 2012 / 2012 R2 or later x64

Minimum hardware requirements:

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

CITRIX READY

vmware PARTNER TECHNOLOGY ALLIANCE

Windows Server 2012 R2 Certified

Kaspersky Security for Windows Server/Version 3/February 2016/Global

KASPERSKY lab