Kaspersky® Security for Windows Servers

Resilient security for business-critical processes running on Windows Servers

Windows Server based machines can host a very wide range of tasks, including many which may be mission-critical to your organization. So it's important than no security incidents or performance issues interrupt their continuous operation. Protection must come in the form of a solution which impacts minimally on resource usage and systems stability, while ensuring the security of all the various business scenarios your servers may be supporting.

Kaspersky Security for Windows Servers provides resilient next generation security for servers in all the many roles they undertake. For optimum cost-effectiveness, appropriate functionality can be enabled using different licenses, according to the type of task being addressed.

Highlights

- **Perfect for mission-critical scenarios**
  Highly adaptable to differing server roles, including mission-critical scenarios, thanks to a wide range of protection components, coupled with reduced maintenance requirements (such as the need for rebooting).
- **Suitable for legacy systems**
  Low performance impact for legacy environments with limited hardware resources. Supports Windows Server 2003 (now no longer supported by Microsoft).
- **Certified solution**
  Certified compatible with virtualization platforms and operating systems.

BENEFITS

Most awarded, most recognized, and most appreciated protection

Kaspersky Security for Windows Servers is based on technologies that consistently attract analyst recognition, podium positions in independent tests and the appreciation of our customers. Independent confirmation that you can entrust your business-critical servers to us.

Exceptional versatility

Kaspersky Security for Windows Servers is suitable for a wide range of server activities and usage types, including the protection of file servers, network storages and other key elements of corporate infrastructure, ensuring their smooth and safe functioning.

Cloud-adapted and cloud-ready

Kaspersky Security for Windows Servers is designed to protect both physical and virtualized servers, enabling you to run server workloads securely throughout your hybrid cloud infrastructure; on-premise, in the datacenter and in public clouds.

Centralized management – save time and money

Kaspersky Security Center offers a unified console with which to manage your security. Whether your key objective is ease of use or the most granular control over all aspects of your infrastructure from a 'single pane of glass', you can adjust the specifics of your corporate security to your systems configuration and requirements, reducing operational costs.

System requirements

Kaspersky Security for Windows Server is designed for servers running either 32-bit or 64-bit versions of Microsoft Windows:

- Windows Server 2003 / 2003 R2 SP2.
- Windows Server 2008 / 2008 R2 SP1 or later (including Core mode)
- Windows Server 2012 / 2012 R2 (including Core mode)
- Windows Server 2016 (including Core mode)
- Small Business Server 2008 / 2011
- Windows MultiPoint Server 2011
- Windows Hyper-V Server 2008 R2 SP1 or later / 2012 / 2012 R2 / 2016
- Windows Storage Server 2012 / 2012 R2 / 2016

Kaspersky Security for Windows Server can be installed on the following terminal servers:

- Microsoft Remote Desktop Services based on Windows 2008 / 2008 R2/ 2012 / 2012 R2 / 2016 Server
- Citrix XenApp 6.0, 6.5, 7.0, 7.5, 7.6, 7.15
- Citrix XenDesktop 7.0, 7.1, 7.5, 7.6, 7.15

Kaspersky Security 10.1 for Windows Server can be used to protect the following network attached storages:

NetApp® with one of the following operating systems:

- Data ONTAP® 7.x and Data ONTAP 8.x in 7-mode
- Data ONTAP 8.2.1 or higher in cluster-mode

Dell EMC Celerra / VNX with the following software:

- EMC DART 6.0.36 or higher
- Celerra (CAVA) Anti-Virus Agent 4.5.2.3 or higher
- Dell EMC Isilon with OneFS 7.0 or later

Hitachi NAS on one of the following platforms:

- HNAS 4100
- HNAS 4080
- HNAS 4060
- HNAS 4040
- HNAS 3090
- HNAS 3080

IBM NAS series IBM System Storage N series

Oracle NAS Systems series Oracle ZFS Storage Appliance

Dell NAS on the platform Dell Compellent FS8600

Minimum hardware requirements:

- Processor – 1.4 GHz single core
- RAM: 1 GB
- Drive subsystem – 4 GB

Application Features

Next Generation protection against malware and more. Kaspersky Security for Windows Servers is based on our unique multi-layered protection platform, supported by Machine Learning and human expertise, enabling the detection of all forms of malware attack, including advanced, sophisticated and emerging threats. Kaspersky Security Network (KSN) delivers a rapid response to new threats, improving protection performance and reducing the risk of false positives to near-zero.

Shared folder and storage protection against crypto-malware. A unique anti-cryptor component blocks the encryption of files on shared resources originated by a malicious process running on a different machine on the network. This functionality applies to both Windows-based file servers and NetApp storage systems

Exploit prevention. Powerful Exploit Prevention technology watches over protected processes to prevent exploits from attacking unpatched and even zero-day vulnerabilities in applications and system components.

Systems hardening. Adopting a Default Deny scenario using Application Launch Control optimizes your system's resilience to data breaches. By prohibiting the running of any application other than specified programs, services, and trusted system components, you can automatically block most forms of malware completely. Implemented in combination with Kaspersky Device Control, running in Default Deny mode also prevents unsolicited storage, considerably reducing your attack surface and boosting your server security.

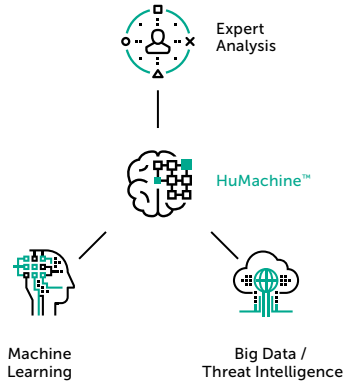
Systems integrity. Ensuring that critical system components and processes (as well as applications) remain intact is essential both for the smooth functioning of your servers and for the security of the sensitive data they are working with. Components of Kaspersky Security for Windows Server such as File Integrity Monitor and Log Inspection don't just identify unwanted changes to your systems - they, can also detect different indicators of a security breach, in compliance with regulations including PCI/DSS.

Traffic security. Kaspersky Security for Windows Server now filters traffic for malware, verifies web links and provides web-resource control, based on Kaspersky Lab categories, for any external system supporting the ICAP protocol, including proxy servers and storages.

Terminal server protection. An extensive range of remote access environments can be secured, including Microsoft Remote Desktop Services and Citrix XenApp/ Xen Desktop.

Windows Firewall management. Your Windows server firewalls can be configured directly from Kaspersky Security Center, giving you the convenience of local firewall management through a single unified console.

SIEM integration. Kaspersky Security for Windows Server integrates with most leading SIEM systems, converting events in application logs into formats supported by the syslog server, so that these can be recognized and imported into your SIEM. The application supports conversion into both structured data and JSON formats.



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
- Kaspersky Hybrid Cloud Security

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

www.kaspersky.com