

▶ KASPERSKY ANTI-VIRUS FOR STORAGE

In modern heterogeneous networks, a single virus can spread very quickly as it is virtually impossible to isolate a newly detected network infection immediately. Corporate users often place various files into file storages, thus exposing all nodes on the corporate network to risk, from workstations to shared file storage facilities.

Kaspersky Lab has developed Kaspersky Anti-Virus for Storage — a dedicated solution to protect EMC™ Celerra™/VNX™ storage systems. The product is fully compatible with all network storage products from the EMC Celerra / VNX family and provides an unprecedentedly high level of security. It detects and removes all types of malware from files and archives stored on EMC Celerra/VNX storage products. All data is scanned on-the-fly as it is being written to storage or while it is being modified.

«... Kaspersky Lab has tightly integrated Kaspersky Anti-Virus for Storage with EMC unified storage systems, offering customers enhanced protection. ... EMC and Kaspersky continue to collaborate to ensure our mutual customers have the highest level of support possible for their information infrastructure initiatives.»

ROB HAZEN,
Director, ISV and OEM Partners,
EMC Corporation

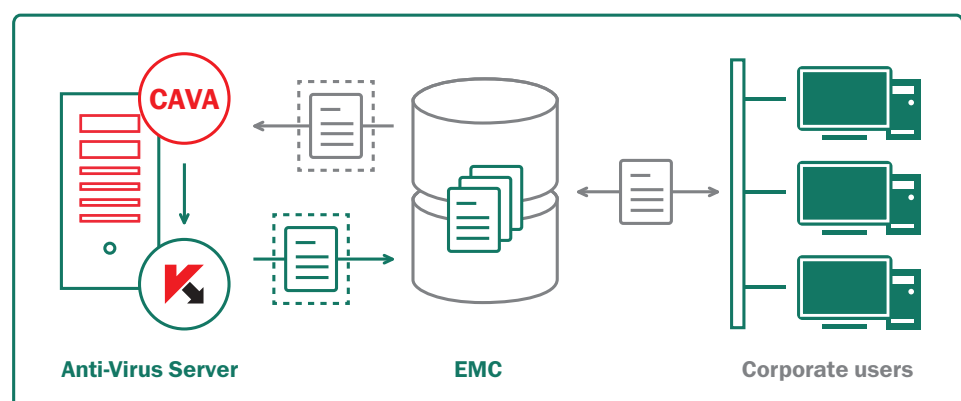
PRODUCT FEATURES

Always-on anti-virus protection and on-demand scanning. The product scans every file that is launched or modified, treats or deletes any suspicious objects, and/or quarantines them for further analysis.

Proactive protection from malware. The new anti-virus engine incorporates advanced anti-malware protection methods such as an heuristic analyser capable of identifying malicious programs with a very high degree of accuracy.

Backup copying. Any suspicious objects that are detected are placed into quarantine. If the product performs any actions on an infected object, an unmodified copy is first placed into backup storage.

Flexible scan settings. The file scan settings enable the administrator to: exempt certain processes from scanning; set the depth of anti-virus protection; specify which file types must always be scanned and which should be exempted completely, etc. This approach helps optimise the server load and ensures the flexible management of corporate network security.



Kaspersky Anti-Virus for Storage functional scheme

BENEFITS

HIGH PERFORMANCE

The new anti-virus engine, optimised scan technology and flexible exemption settings ensure maximum performance from the product.

REAL-TIME PROTECTION

The product protects file storages in real-time, deleting viruses, worms and other malicious programs.

RELIABILITY

The product will restart automatically if forced to shut down, maintaining High Value world-class malware protection for your infrastructure.

USER-FRIENDLY MANAGEMENT

Managing the product is fast and easy for the system administrator: it can be installed remotely, is efficient and straightforward to use.

REGULAR UPDATES

The anti-virus databases are updated automatically, ensuring continuous protection, minimizing routine work and saving the administrator time.

SELECTION OF TRUSTED PROCESSES

The administrator can exempt secure processes such as data backups from scanning if their performance is affected by the scanning process.

SUPPORT OF HIERARCHICAL STORAGE MANAGEMENT (HSM)

The product is compatible with disk storage management systems (Hierarchical Storage Management) and provides effective anti-virus protection for file systems with complex hierarchies.

SUPPORT FOR WINDOWS SERVER® 2008 R2

The product is certified compatible with the new version of Windows Server 2008 R2, including Server Core and Microsoft® Hyper-V® Server 2008 R2.

How to Buy

For more information on **Kaspersky Anti-Virus for Storage**, or to purchase contact your reseller.

ADMINISTRATION

SELECTION OF MANAGEMENT TOOLS

The product can be managed either directly or remotely via the Microsoft Management Console, the Kaspersky Security Center, or by using the command line. The console provides graphical reports on the protection status of the EMC Celerra/VNX equipment.

CENTRALISED INSTALLATION AND MANAGEMENT

Kaspersky Security Center is a centralised management tool that supports the remote installation and configuration of the product, as well as helping to manage its operation and to receive updates and notifications.

CONTROL OVER ADMINISTRATOR PRIVILEGES

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

NOTIFICATION SYSTEM

The product supports administrator notifications via the messaging service or email for an extensive event list. The product is integrated with Simple Network Management Protocol (SNMP) and can operate with Microsoft Operations Management (MOM).

FLEXIBLE REPORTING SYSTEM

The administrator can monitor the product's operation via graphical reports or by reviewing Microsoft Windows®, or Kaspersky Security Center's event logs. The integrated search tool supports filters, allowing quick searches of large-volume logs to be undertaken.

SYSTEM REQUIREMENTS

SUPPORTED OPERATING SYSTEMS:

- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2008 x86/x64
- Microsoft Windows Server 2003 R2 x86/x64
- Microsoft Windows Server 2003 x86/x64

MANAGEMENT CONSOLE:

- Microsoft Windows 7 Professional x86/x64
- Microsoft Windows XP Professional all service packs supported 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

EMC CELERRA/VNX FILE STORAGE

CONTACT DETAILS

Not all features are available on all platforms
www.kaspersky.com.au/business

Download a free trial
www.kaspersky.com.au/trials