▶ KASPERSKY SECURITY FOR STORAGE

High-Performance Protection for EMC, NetApp and Hitachi Storages

OVERVIEW

Lethal malware can spread throughout an organization at terrifying speed, capitalizing on the inter-operability of modern networks. In an ever-growing threat landscape, a single infected file unknowingly placed into storage can expose every node on the network to immediate risk.

Kaspersky Security for Storage provides robust, high-performance, scalable protection for valuable and sensitive corporate data stored on EMC Isilon™, Celerra and VNX™, NetApp, Hitachi and IBM storage systems.

- Real-time anti-malware protection for EMC, NetApp, Hitachi and IBM
- Supports CAVA agent, RPC and ICAP protocols
- Supports dedicated tasks for critical system area scans
- Flexible scan configuration
- Scalable and fault tolerant
- Adaptable utilization of system resources
- Terminal server protection
- Support for server clusters
- Certified compatible with VMware
- Includes iSwift and iChecker antivirus scan optimization
- Kaspersky Security Center management
- Application performance reporting
- Supports SNMP/MOM network management

HIGHLIGHTS

POWERFUL, REAL-TIME ANTI-MALWARE PROTECTION

'Always-on' proactive protection for network attached storage (NAS) solutions. Kaspersky's powerful anti-malware engine scans every file launched or modified for all forms of malware including viruses, worms and Trojans. Advanced heuristic analysis identifies even new and unknown threats.

OPTIMIZED PERFORMANCE

High performance scanning, featuring optimized scan technology and flexible exemption settings, delivers maximum protection while minimizing the impact on the system's performance.

RELIABLE

Exceptional fault-tolerance is achieved through a straightforward architecture using unified components designed and built to work together flawlessly. The result is a stable, resilient solution which, if forced to shut down, will restart automatically for reliable and continuous protection.

EASY TO ADMINISTER

Servers are remotely installed and protected 'out-of-the-box' with no reboots and are administered together through a simple, intuitive central console — Kaspersky Security Center — along with your other Kaspersky security solutions.

FEATURES

ALWAYS-ON, PROACTIVE SECURITY
Kaspersky's industry-leading anti-malware scanning engine, built by the world experts in threat intelligence, provides proactive protection against emerging and potential threats using smart technologies for enhanced detection.

AUTOMATIC UPDATES
Anti-malware databases update automatically with no disruption to scanning, ensuring continuous protection, and minimizing administrator workload.

EXEMPTED PROCESSES AND TRUSTED ZONES
Scan performance can be fine-tuned by created 'trusted zones' which, together with defined file formats and processes such as data backups, can be exempted from scanning.

AUTORUN OBJECT SCANNING
For increased server protection, autorun file and operating system scans can be run to prevent malware from launching during system start-up.

FLEXIBLE SCANNING FOR OPTIMIZED PERFORMANCE
Reduces scanning and configuration time and promotes load balancing, helping to optimize server performance. The administrator can specify and control the depth, breadth and timing of scan activity, defining which file types and areas must be scanned. On-demand scanning can be scheduled for periods of low server activity.

PROTECTS HSM AND DAS SOLUTIONS
Supports offline scan modes for the effective protection of Hierarchical Storage Management (HSM) systems. Direct Attached Storage (DAS) protection also helps promote the use of low cost storage solutions.

SUPPORT FOR ALL MAIN PROTOCOLS
Kaspersky Security for Storage supports the main protocols utilised by different storage systems: CAVA agent, RPC and ICAP.

VIRTUAL SYSTEMS AND TERMINAL SERVER PROTECTION
Flexible security includes protection for virtual (guest) operating systems in Hyper-V and VMware virtual environments, and for Microsoft and Citrix terminal infrastructures.

ADMINISTRATION

CENTRALIZED INSTALLATION AND MANAGEMENT
Remote installation, configuration and administration including notifications, updates and flexible reporting are handled through the intuitive Kaspersky Security Center. Command line management is also available if preferred.

CONTROL OVER ADMINISTRATOR PRIVILEGES
Different privilege levels can be assigned to each server's administrator, enabling compliance with specific corporate IT security policies.

FLEXIBLE REPORTING
Reporting can be delivered via graphical reports or through reviewing Microsoft Windows® or Kaspersky Security Center's event logs. Search and filtering tools provide quick access to data in large-volume logs.

SYSTEM REQUIREMENTS

HARDWARE:
- x86-compatible systems in a single-processor or multiple-processor configuration
- x86-64-compatible systems in single-processor or multiple-processor

DISK SPACE:
- For the installation of all application components: 70 MB
- For storing objects in quarantine or in backup: 400 MB (recommended)
- For storing logs: 1 GB (recommended)
- For storing databases: 2GB (recommended)

MINIMUM CONFIGURATION:
- Processor – 1 Core; processing speed 1.4 GHz
- RAM: 1 GB
- 4 GB of free hard drive space

RECOMMENDED CONFIGURATION:
- Processor – 4 Core; processing speed 2.4 GHz
- RAM: 2 GB
- 4 GB of free hard drive space

SOFTWARE:
- Microsoft Windows Server 2003/2003 R2 x86/x64 Standard/ Enterprise Edition
- Microsoft Windows Server 2008/2008 R2 x86/x64 Standard/ Enterprise/Datacenter Edition (including Core mode)
- Microsoft Windows Server 2012/20012 R2 Essentials / Standard / Foundation / Datacenter (including Core mode)
- Microsoft Windows Hyper-V Server 2008 R2
- Microsoft Windows Hyper-V Server 2012/2012 R2

SERVERS:
- Microsoft Terminal Services based on Windows 2003 Server;
- Microsoft Terminal Services based on Windows 2008 Server;
- Microsoft Terminal Services based on Windows 2012/ 2012 R2 Server;
- Citrix Presentation Server 4.0, 4.5;
- Citrix XenApp 4.5, 5.0, 6.0, 6.5;
- Citrix XenDesktop 7.0, 7.1, 7.5

STORAGE PLATFORMS:
EMC Celerra / VNX file storage:
- EMC DART 6.0.36 or above;
- Celerra Antivirus Agent (CAVA) 4.5.2.3 or above.

Requirements for EMC Isilon storage:
- EMC Isilon OneFS.

Requirements to NetApp storage:
- Data ONTAP 7.x и Data ONTAP 8.x in 7-mode regime;
- Data ONTAP 8.2.1 or higher in cluster-mode regime.

Requirements for IBM storages:
- IBM System Storage N series.

vmware READY

Windows Server 2012 R2 Certified

KS-Storage/Version 2/January 2015/Global

KASPERSKY lab