Security for Data Centers

KASPERSKY SECURITY FOR STORAGE

High-performance protection for latest network-attached storages

OVERVIEW

Nowadays, 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®, Dell™, Hitachi HNAS, IBM® System Storage® N and Oracle® ZFS Storage Appliance systems.

- Real-time anti-malware protection for EMC, NetApp, Dell, Hitachi, Oracle and IBM
- Cloud-assisted security with Kaspersky Security Network (KSN)
- 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
- Certified VMware™ compatible
- Includes iSwift and iChecker antivirus scan optimization
- Centralized management via Kaspersky Security Center

Highlights

POWERFUL, REAL-TIME ANTI-MALWARE PROTECTION

'Always-on' proactive protection, powered by global security intelligence (the Kaspersky Security Network), for network attached storage (NAS) solutions. Kaspersky's powerful anti-malware engine checks 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 systems 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 Lab security solutions.

FLEXIBLE SCANNING

Kaspersky Lab's flexible scanning processes help you to secure your corporate network and optimize the load on your servers. You can define a wide range of scan settings, including depth of anti-malware protection, types of file to be scanned or to be excluded from scanning.

Features

ALWAYS-ON, PROACTIVE SECURITY
Kaspersky Lab'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.

CLOUD-ASSISTED SECURITY
Available in Kaspersky Security for Storage, the cloud-based Kaspersky Security Network (KSN) means malicious activities can be identified significantly faster, helping protect data storages from zero-day threats.

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

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.

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

REMOTE 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.

SUPPORTED STORAGE PLATFORMS

EMC Celerra / VNX storages:
– EMC DART 6.0.36 or above
– Celerra Antivirus Agent (CAVA) 4.5.2.3 or above

EMC Isilon storages:
- OneFS™ 7.0 or above

NetApp storages:
– Data ONTAP® 7.x and Data ONTAP 8.x in 7-mode
– Data ONTAP 8.2.1 or above in cluster-mode

IBM storages:
– IBM System Storage N series

Hitachi storages:
– HNAS 4100
– HNAS 4080
– HNAS 4060
– HNAS 4040
– HNAS 3090
– HNAS 3080

Dell storages:
– Dell Compellent™ FS8600

Oracle storages:
– Oracle ZFS Storage Appliance

OTHER NAS
– ICAP-compliant NAS
– RPC-compliant NAS

Learn more at www.kaspersky.com/data-center-security

KSS/Feb16/Global