**Kaspersky®
Security for Storage**

High-performance cybersecurity for network-attached storages

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 data that resides on corporate network attached storage devices. Smooth integration through fast protocols preserves storage systems efficiency to maintain optimized end-user experience.

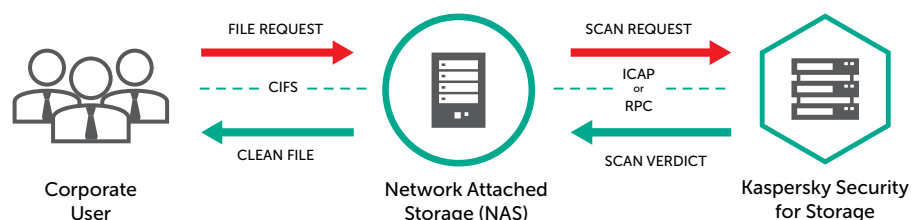**Why Customers Choose Kaspersky Security for Storage:**

- Powerful real-time anti-malware protection for EMC, NetApp, Dell, Hitachi, Oracle and IBM storages
- Cloud-assisted security with Kaspersky Security Network (KSN)
- Supports multiple protocols: CAVA agent, RPC and ICAP
- Dedicated security tasks for critical system area scans
- Flexible and granular configuration for always-on anti-malwarae scan
- Easy scalable and support for fault-tolerant deployments
- Adaptable utilization of system resources
- Certified with VMware™, Microsoft™ and other vendors
- Includes iSwift and iChecker antivirus scan optimization
- Unified management and orchestration via Kaspersky Security Center

Business Benefits:

- All files on your data storages are safe with no need to check AV on endpoints
- Integration with NAS via native API means less impact on end-users productivity
- Full visibility of datafile cybersecurity across your entire storage infrastructure

Highlights

- **Powerful, real-time anti-malware protection**
'Always-on' proactive protection, powered by global security intelligence (Kaspersky Security Network), for network attached storage (NAS) solutions. Kaspersky Lab's powerful anti-malware engine checks every file launched or modified for all forms of malware including viruses, worms and Trojans. Advanced heuristic analysis can identify 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 protection for NAS**
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.

FILE REQUEST   CIFS   CLEAN FILE   SCAN REQUEST   ICAP or RPC   SCAN VERDICT

Corporate User   Network Attached Storage (NAS)   Kaspersky Security for Storage

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**
  Cloud-based security from the 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.

Powered by HuMachine Intelligence, Kaspersky Lab's unique combination of Machine Learning, Threat Intelligence and Expertise, Kaspersky Security for Storage ensures that all data, whatever its source, is fully protected, with near-zero impact on systems performance.

Expert Analysis

HuMachine™

Machine Learning

Big Data / Threat Intelligence
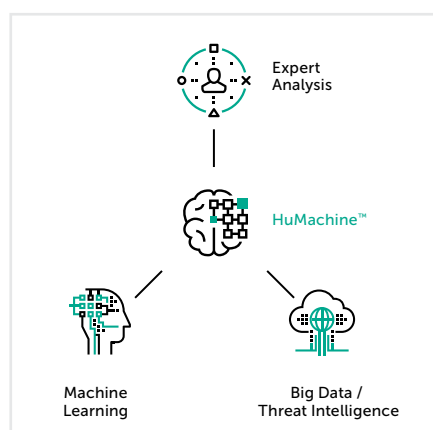
Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com