Kaspersky Security for Storage

High Performance and Unique Protection
for NetApp Clustered Data ONTAP

www.kaspersky.com
#truecybersecurity

NetApp
Alliance Partner

Reliable protection for data storages

Data is core to any business, regardless of size. That's why it's critical to ensure that both your storage infrastructure and the security solution it depends upon are reliable and efficient. As businesses continue to roll out data storages across their IT estate, there is an ever-increasing need for security designed specifically to protect storages. Kaspersky Lab and NetApp are working together to address this.

Kaspersky Security for Storage provides robust, high-performance, scalable and unique protection for valuable and sensitive corporate data. The solution features Kaspersky Lab's award-winning anti-malware engine, with patented technologies that ensure the highest detection rates, defending against known and unknown malware.

NetApp® clustered Data ONTAP® OS key benefits:

- **Support More Workloads**
  Run SAN and NAS workloads simultaneously with the industry's only unified scale-out storage.
- **Consolidate Infrastructure**
  Expand scaling up to 103PB and include existing storage with FlexArray™.
- **Boost I/O-Intensive Apps**
  Reduce latency and speed operations with up to 1.7PB of hybrid flash.
- **Maximize Uptime**
  Experience >99.999% availability plus non-disruptive operations that eliminate planned downtime.
- **Realize Superior Value**
  Deliver up to 2x the price/performance of the previous generation.

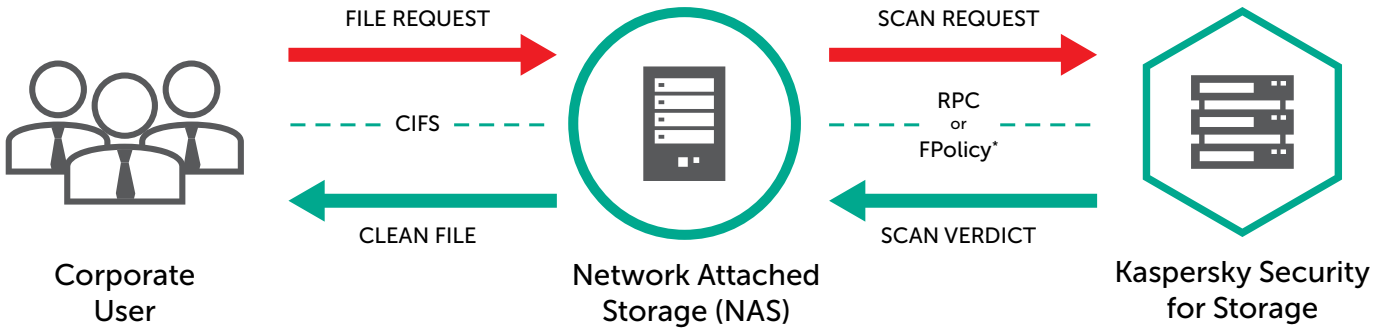
NetApp enterprise storage systems are engineered specifically to support existing workloads as well as adapting and scaling quickly to address new applications and evolving IT models. Powered by NetApp Clustered Data ONTAP and optimized for scale-out, NetApp enterprise systems unify your NAS storage infrastructure. With proven data management capabilities, Clustered Data ONTAP has the flexibility to keep up with changing business needs while delivering on core IT requirements. Clustered Data ONTAP software is the foundation for NetApp's Data Fabric, a vision for the future of data management.

Kaspersky Security for Storage is a powerful, highly scalable security solution designed to protect NetApp Clustered Data ONTAP storages with minimal impact on NAS performance.

Thanks to a close technological partnership with NetApp, we have developed unique NAS protection against crypto-malware. Using the NetApp FPolicy integration protocol and our patented[1] technologies, Kaspersky Security for Storages can now directly scan suspicious file assets and protect shared folders from ransomware.

Unique protection and exceptional fault tolerance are achieved, 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 to maintain continuous protection.

Kaspersky Security for Storage



[1] USA patent 14/951.970: System and method for detection of malicious data encryption programs
* More about FPolicy: https://library.netapp.com/ecmdocs/ECMP1120826/html/GUID-A7DBFCD5-4620-4423-8284-035BE31727C0.html

Security solution benefits

Unique NAS protection from ransomware and cryptors

Kaspersky Security for Storage delivers unique security – blocking ransomware and cryptor activity on your NetApp NAS. Thanks to NetApp's FPolicy protocol and Kaspersky Lab's unique patented technologies, it is now possible to stop ransomware activity directly on the storage side, not just on the end-user side, as was the case in the past.

Real-time protection for any file operation

Kaspersky Security for Storage delivers real-time security – deleting viruses, worms and other malicious objects. All file-level activity in data storage is protected in real time, regardless of whether the user opens or modifies the file or uploads it from a PC.

Reliable security solution with minimal impact on perfomance

Kaspersky Lab's latest anti-malware engine, optimized scanning technology and flexible exemption settings all help boost security with no adverse performance impact on data storage infrastructure.

Easy-to-use centralized management console

Kaspersky Security for Storage is designed for ease of use. Remote installation, configuration and administration, including notifications, updates and flexible reporting, are all handled through one unified console.

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.

Proactive anti-malware technologies

Kaspersky Lab's latest anti-malware engine uses advanced techniques – including heuristic analysis – to deliver outstanding levels of anti-malware protection for your data storages.

Cloud-assisted security

Kaspersky Security Network (KSN) is a complex distributed infrastructure dedicated to processing cybersecurity data streams from millions of voluntary participants around the world in real time. KSN communicates directly with your Kaspersky Security for Storage installation, delivering the highest levels of protection by identifying and responding almost instantaneously to known, unknown and even zero-day threats.

Flexible reporting and monitoring

Administrators can monitor operations via graphical reports, or by reviewing Microsoft Windows or Kaspersky Security Center event logs. An integrated search tool supports filters for quick searches of large-volume logs. Administrator notifications for an extensive range of events can be sent via the messaging service or email as well as to third-party monitoring solutions via SNMP.

What is FPolicy?

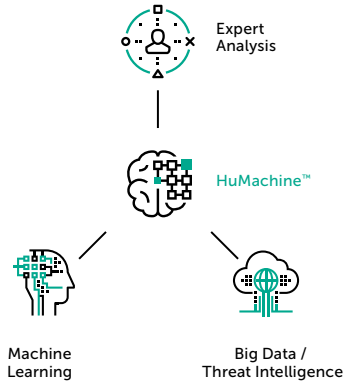
FPolicy is an infrastructure component of Data ONTAP that enables Kaspersky Security for Storage to monitor and set file access permissions.

Every time a client accesses a file from a storage system, based on the configuration of FPolicy, Kaspersky Security for Storage is notified about file access. This enables restrictions to be set for files that are created or accessed on the storage system.

FPolicy allows the creation of file policies that specify file operation permissions according to file type. For example, you can restrict certain file types, such as JPEG and .MP3 files, from being stored on the storage system.

FPolicy determines how the storage system handles requests from individual client systems for operations such as create, open, rename, and delete.

The FPolicy interface is a Data ONTAP API (called ONTAPI) that uses Remote Procedure Calls (RPC).



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber-Threat News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com