



## Kaspersky<sup>®</sup> Security for Storage

# Cybersecurity der nächsten Generation für Network Attached Storage (NAS)

Malware kann sich mit hoher Geschwindigkeit in einem Unternehmen ausbreiten und macht sich dabei die Interoperabilität moderner Netzwerke zunutze. Bei immer umfangreicheren Bedrohungen kann eine einzige Datei, die unwissentlich in einem Speicher abgelegt wird, jeden Netzwerk-Node einem sofortigen Risiko aussetzen.

Kaspersky Security for Storage bietet starken, hochwirksamen und skalierbaren Schutz für wertvolle und vertrauliche Daten, die sich auf Netzwerkspeichergeräten von Unternehmen befinden. Die nahtlose Integration durch schnelle Protokolle gewährleistet die Effizienz der Speichersysteme und somit ein optimales Benutzererlebnis.

### Warum Kunden

#### Kaspersky Security for Storage wählen:

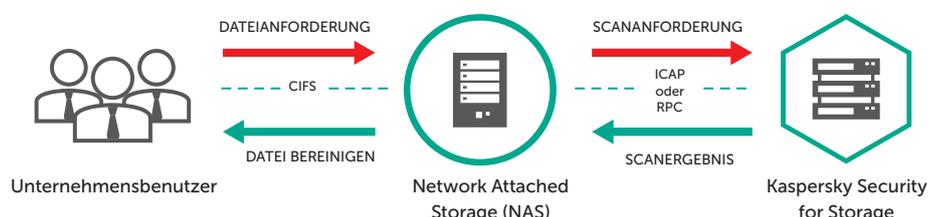
- Leistungsstarker Malware-Schutz in Echtzeit für Speichersysteme von EMC, NetApp, Dell EMC, Hitachi, Oracle, IBM und HPE
- Cloud-basierte Sicherheit durch das Kaspersky Security Network (KSN)
- Unterstützt mehrere Protokolle: CAVA agent, RPC und ICAP
- Zielgerichtete Aufgaben für die Scans kritischer Systembereiche
- Flexible und fein abgestimmte Konfiguration für den allzeit aktivierten Anti-Malware-Scan
- Einfache Skalierbarkeit und Unterstützung für fehlertolerante Bereitstellungen
- Anpassbare Nutzung von Systemressourcen
- Zertifizierung für VMware™, Microsoft™ und andere Anbieter
- Umfasst die Virenschutz-Optimierungen iSwift und iChecker
- Einheitliche Verwaltung und Orchestrierung über das Kaspersky Security Center

### Geschäftliche Vorteile:

- Alle Dateien auf Ihren Datenspeichern sind sicher – ohne dass Sie den Virenschutz an Endpoints prüfen müssen.
- Weniger Auswirkungen auf die Endbenutzer-Produktivität durch Integration mit NAS über die native API
- Vollständige Transparenz der Cybersicherheit Ihrer Dateien über Ihre gesamte Speicherinfrastruktur hinweg

## Wichtigste Vorteile

- **Leistungsstarker Malware-Schutz in Echtzeit** Allzeit aktivierter vorausschauender Schutz für NAS-Lösungen (Network Attached Storage), basierend auf globalen Sicherheitsinformationen (Kaspersky Security Network). Die leistungsstarke Anti-Malware-Engine von Kaspersky Lab prüft jede aufgerufene oder geänderte Datei auf sämtliche Arten von Malware, einschließlich Viren, Würmer und Trojaner. Eine fortschrittliche, ganzheitliche Analyse kann selbst neue und bisher unbekannte Bedrohungen erkennen.
- **Optimierte Leistung** Hochwirksame Scans auf der Grundlage optimierter Scan-Technologie und flexibler Ausschlusseinstellungen sorgen für maximalen Schutz und schonen gleichzeitig die Systemleistung.
- **Zuverlässiger Schutz für NAS** Eine unkomplizierte Architektur, deren einheitliche Komponenten auf ein reibungsloses Zusammenspiel ausgelegt sind, ermöglicht eine außergewöhnliche Fehlertoleranz. Dadurch ergibt sich eine stabile, widerstandsfähige Lösung, die bei erzwungenem Herunterfahren automatisch neu startet und dadurch zuverlässigen, durchgehenden Schutz gewährleistet.
- **Einfache Verwaltung** Die Server werden per Fernzugriff installiert und ohne Neustart sofort in den Schutz einbezogen. Verwaltet werden sie zusammen mit anderen Sicherheitslösungen von Kaspersky Lab über eine unkomplizierte, zentrale Konsole: Das Kaspersky Security Center.



## Unterstützte Speicherplattformen

### HPE-Speicher:

- HPE 3PAR StoreServ-Dateicontroller auf File Persona 3.3.1
- HPE 3PAR StoreServ 7000c-, 8000-, 9000-, 20000-Speicher auf File Persona 3.3.1

### EMC Celerra-/VNX-Speicher:

- EMC DART 6.0.36
- Celerra Antivirus Agent (CAVA) 4.5.2.3

### EMC Isilon-Speicher:

- OneFS™ 7.0

### NetApp-Speicher:

- Data ONTAP® 7.x und 8.x im 7-Modus
- Clustered Data ONTAP® 8.x und 9.x

### IBM-Speicher:

- IBM System Storage N Series

### Hitachi-Speicher:

- HNAS 4100, 4080, 4060, 4040
- HNAS 3090, 3080
- Virtual Storage Platform G-Serie

### Dell-Speicher:

- Dell Compellent™ FS8600 auf FluidFS 6.x
- Dell Compellent™ FS8600 auf FluidFS 5.x

### Oracle-Speicher:

- Oracle ZFS Storage Appliance

### ANDERE NAS-SYSTEME

- ICAP-kompatible NAS-SYSTEME
- RPC-kompatible NAS-SYSTEME

  
**Hewlett Packard  
Enterprise**

  
**EMC<sup>2</sup>**

  
**Gold  
Partner**

  
**Technology Partner**

  
**HITACHI**  
Hitachi Data Systems

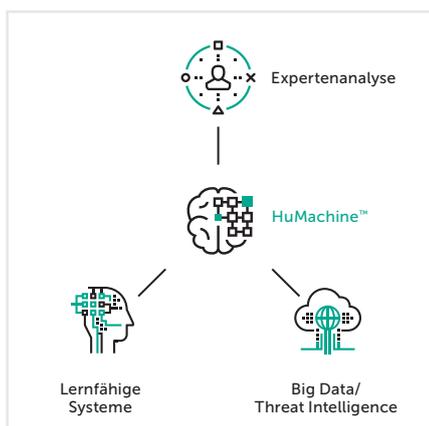
**Technology  
Alliance  
Partner**

  
**NetApp**  
Alliance Partner

# Funktionen

- **Allzeit aktivierter, proaktiver Schutz** Die Scans der branchenführenden Anti-Malware-Engine von Kaspersky Lab, entwickelt von erfahrenen Fachleuten im Bereich Threat Intelligence, bieten mit ihrer intelligenten Erkennungstechnologie proaktiven Schutz vor neu auftretenden und potentiellen Bedrohungen.
- **Automatische Updates** Die Malware-Datenbanken aktualisieren sich automatisch ohne Unterbrechung der Scanvorgänge, sodass durchgängiger Schutz und minimale Belastung der Administratoren sichergestellt sind.
- **Cloud-basierte Sicherheit** Durch die Cloud-basierte Sicherheit des Kaspersky Security Network (KSN) können schädliche Aktivitäten wesentlich schneller erkannt werden, wodurch Datenspeicher vor Zero-Day-Bedrohungen geschützt werden.
- **Ausgenommene Prozesse und vertrauenswürdige Bereiche** Feinjustieren lässt sich die Scan-Leistung durch die Einrichtung vertrauenswürdiger Bereiche, die von den Scans ausgenommen werden können. Das Gleiche gilt für festgelegte Dateiformate und Prozesse wie Datensicherungen.
- **Optimale Leistung durch flexible Scans** Verringert die Scan- und Konfigurationsdauer und unterstützt Load Balancing zur Optimierung der Serverleistung. Der Administrator kann die Tiefe, Breite und Zeitplanung der Scanvorgänge bestimmen und festlegen, welche Dateitypen und Bereiche zu scannen sind. Scans nach Bedarf lassen sich für Zeiten mit geringerer Serveraktivität planen.
- **Unterstützung aller wichtigen Protokolle** Kaspersky Security for Storage unterstützt die wichtigsten, von verschiedenen Speichersystemen verwendeten Protokolle: CAVA agent, RPC und ICAP.
- **Zentrale Remote-Installation und -Verwaltung** Installation, Konfiguration und Verwaltung per Fernzugriff, einschließlich Benachrichtigungen, Updates und flexiblem Reporting, erfolgen über das intuitiv bedienbare Kaspersky Security Center. Alternativ lassen sich die Funktionen auch über die Befehlszeile verwalten.
- **Kontrolle über Administratorrechte** Jedem Administrator eines Servers können verschiedene Berechtigungsebenen zugewiesen werden, sodass sich spezielle IT-Sicherheitsrichtlinien des Unternehmens einhalten lassen.
- **Flexible Reporting-Funktionen** Zu Reporting-Zwecken können grafische Berichte bereitgestellt oder die Ereignisprotokolle von Microsoft® Windows® oder dem Kaspersky Security Center überprüft werden. Such- und Filterfunktionen erleichtern den schnellen Datenzugriff in sehr umfangreichen Protokollen.

Mithilfe von HuMachine Intelligence, der einzigartigen Kombination aus Machine Learning, Threat Intelligence und Expertise von Kaspersky Lab, stellt Kaspersky Security for Storage sicher, dass alle Daten unabhängig von ihrer Quelle vollständig geschützt sind. Zudem sind fast keine Auswirkungen auf die Systemleistung zu verzeichnen.



Kaspersky Lab  
Cybersicherheit für Unternehmen: [www.kaspersky.de/enterprise-security](http://www.kaspersky.de/enterprise-security)  
Neues über Cyberbedrohungen: [de.securelist.com/](http://de.securelist.com/)  
IT-Sicherheitsnachrichten: [www.kaspersky.de/blog/b2b/](http://www.kaspersky.de/blog/b2b/)

#truecybersecurity  
#HuMachine

[www.kaspersky.de](http://www.kaspersky.de)

© 2017 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.