

# KASPERSKY SECURITY FOR STORAGE

*Protection haute performance pour les derniers périphériques de stockage en réseau (NAS)*

## ANALYSE

De nos jours, les programmes malveillants peuvent infecter toute une entreprise en un temps record, en exploitant l'interopérabilité des réseaux actuels. Dans un contexte de plus en plus menaçant, un simple fichier infecté placé sans le savoir dans un espace de stockage peut exposer chaque nœud du réseau à un risque immédiat.

Kaspersky Security for Storage fournit une protection solide, évolutive et haute performance pour des données d'entreprise importantes et sensibles stockées sur des systèmes EMC™ Isilon™, Celerra™ et VNX™, NetApp®, Dell™, Hitachi HNAS, IBM® System Storage® N et Oracle® ZFS Storage Appliance.

- Protection en temps réel contre les programmes malveillants pour EMC, NetApp, Dell, Hitachi, Oracle et IBM
- Sécurité basée dans le Cloud avec Kaspersky Security Network (KSN)
- Prise en charge de l'agent CAVA et des protocoles RPC et ICAP
- Prise en charge des tâches dédiées pour l'analyse des zones système critiques
- Configuration flexible des analyses
- Évolutivité et tolérance aux pannes
- Utilisation flexible des ressources système
- Certification compatible VMware™
- Optimisation des analyses antivirus iSwift et iChecker incluse
- Gestion centralisée avec Kaspersky Security Center

## Points forts

### PUISSANTE PROTECTION EN TEMPS RÉEL CONTRE LES PROGRAMMES MALVEILLANTS

Protection proactive « permanente » associée à la veille mondiale sur la sécurité (Kaspersky Security Network) pour les solutions de stockage en réseau (NAS). Le puissant moteur contre les programmes malveillants de Kaspersky Lab inspecte chaque fichier lancé ou modifié à la recherche de programmes malveillants de tous types, tels que virus, vers et chevaux de Troie. Une analyse heuristique avancée permet d'identifier les nouvelles menaces encore méconnues.

### PERFORMANCES OPTIMISÉES

Une analyse haute performance, associée à une technologie d'analyse optimisée et des paramètres d'exclusion flexibles, offre une protection maximale tout en réduisant l'impact sur les performances système.

### FIABILITÉ

Une architecture directe utilisant des composants unifiés conçus pour travailler parfaitement ensemble permet d'atteindre une remarquable tolérance aux pannes. Vous bénéficiez ainsi d'une solution stable et résistante qui, en cas d'arrêt forcé, redémarrera automatiquement afin d'assurer une protection fiable et continue.

### SIMPLICITÉ D'ADMINISTRATION

Les serveurs sont installés et protégés à distance dès la mise en service, sans nécessiter de redémarrage, et sont administrés conjointement à partir d'une console centralisée simple et intuitive, Kaspersky Security Center, complétée par d'autres solutions de sécurité de Kaspersky Lab.

### ANALYSE PROGRAMMÉE OU À LA DEMANDE

Les processus flexibles d'analyse de Kaspersky Lab contribuent à sécuriser votre réseau d'entreprise et à optimiser la charge sur vos serveurs. Vous pouvez définir une série étendue de paramètres d'analyse, dont le niveau de protection contre les programmes malveillants, les types de fichier à numériser ou à exclure de l'analyse.

## Fonctionnalités

### SÉCURITÉ PROACTIVE PERMANENTE

Référence en la matière, le moteur d'analyse pour la protection contre les programmes malveillants de Kaspersky Lab, développé par nos experts mondiaux, offre une protection proactive contre les nouvelles menaces et les menaces potentielles à l'aide de technologies intelligentes de détection avancée.

### MISES À JOUR AUTOMATIQUES

Les bases de données des programmes malveillants sont mises à jour automatiquement sans interruption d'analyse afin de garantir une protection continue et de réduire la charge de travail pour l'administrateur.

### SÉCURITÉ BASÉE DANS LE CLOUD

Disponible dans Kaspersky Security for Storage, Kaspersky Security Network (KSN) basé dans le Cloud permet d'identifier bien plus rapidement toute activité malveillante et aide à protéger les périphériques de stockage de données contre les menaces « zero-day ».

### ZONES FIABLES ET PROCESSUS EXCLUS

La configuration des performances d'analyse peut être affinée en créant des « zones de confiance » qui, au même titre que des formats de fichiers et des procédures définies, comme des sauvegardes de données, pourront être exclues des analyses.

### ANALYSE FLEXIBLE POUR DES PERFORMANCES OPTIMISÉES

Réduit les temps d'analyse et de configuration et favorise l'équilibrage de la charge, pour des performances serveur optimales. L'administrateur peut spécifier et contrôler la profondeur, l'ampleur et le moment de l'activité d'analyse, et définir les types de fichiers et les zones à analyser. Il est également possible de programmer des analyses à la demande sur des périodes de faible activité des serveurs.

### SUPPORT DE TOUS LES PRINCIPAUX PROTOCOLES

Kaspersky Security for Storage prend en charge les principaux protocoles utilisés par différents systèmes de stockage : Agent CAVA, RPC et ICAP.

### INSTALLATION ET GESTION CENTRALISÉES À DISTANCE

L'installation, la configuration et l'administration, dont les notifications, les mises à jour et la création de rapports flexibles, se fait à distance à partir de la console intuitive Kaspersky Security Center. Vous pouvez également opter pour une gestion par ligne de commande si vous le souhaitez.

### CONTRÔLE DES PRIVILÈGES ADMINISTRATEUR

Différents niveaux de privilèges peuvent être affectés à chaque administrateur de serveur afin de respecter les politiques de sécurité informatique propres à l'entreprise.

### RAPPORTS FLEXIBLES

La création de rapports peut se faire en s'appuyant sur des rapports graphiques ou en consultant les journaux d'événements de Microsoft® Windows® ou de Kaspersky Security Center. Les outils de recherche et de filtrage permettent d'accéder rapidement aux données recherchées dans des journaux volumineux.

Plus d'informations sur : [www.kaspersky.com/data-center-security](http://www.kaspersky.com/data-center-security)

## PLATEFORMES DE STOCKAGE PRISES EN CHARGE

### Stockages EMC Celerra/VNX :

- EMC DART 6.0.36 ou version ultérieure
- Celerra Antivirus Agent (CAVA) 4.5.2.3 ou version ultérieure

### Systèmes de stockage EMC Isilon :

- OneFS™ 7.0 ou version ultérieure

### Systèmes de stockage NetApp :

- Data ONTAP® 7.x et Data ONTAP 8.x en régime à 7 modes
- Data ONTAP 8.2.1 ou version ultérieure en régime de mode en cluster

### Systèmes de stockage IBM :

- Stockage IBM System série N

### Systèmes de stockage Hitachi :

- NHAS 4100
- NHAS 4080
- NHAS 4060
- NHAS 4040
- NHAS 3090
- NHAS 3080

### Systèmes de stockage Dell :

- Dell Compellent™ FS8600

### Systèmes de stockage Oracle :

- Oracle ZFS Storage Appliance

### AUTRES PRODUITS NAS

- NAS compatible ICAP
- NAS compatible RPC

