▶ KASPERSKY SECURITY FOR STORAGE

Hoogwaardige bescherming voor EMC-, NetApp- en Hitachi-storage

OVERZICHT

Schadelijke malware kan zich in hoog tempo binnen uw organisatie verspreiden, gebruikmakend van de interoperabiliteit van moderne netwerken. Het aantal dreigingen wordt steeds groter en wanneer er één geïnfecteerd bestand in de storage staat zonder dat u dat weet, loopt elke node in het netwerk direct gevaar.

Kaspersky Security for Storage biedt robuuste, krachtige en schaalbare bescherming voor waardevolle en vertrouwelijke bedrijfsgegevens die zijn opgeslagen op storagesystemen van EMC Isilon™, Celerra en VNX™, NetApp, Hitachi en IBM.

- Realtime anti-malwarebescherming voor EMC, NetApp, Hitachi en IBM
- Ondersteunt CAVA-agent en de protocollen RPC en ICAP
- Ondersteunt speciale taken voor scans van essentiële systeemzones
- Flexibele scanconfiguratie
- Schaalbaar en fouttolerant
- Aanpasbaar gebruik van systeembronnen
- Bescherming van terminalservers
- Ondersteuning voor serverclusters
- Gecertificeerd compatibel met VMware
- Omvat iSwift- en iChecker-anti-virusscanoptimalisatie
- Kaspersky Security Center-beheer
- Rapportage van applicatieprestaties
- Ondersteunt SNMP/MOM-netwerkbeheer

VOORDELEN

KRACHTIGE REALTIME BESCHERMING TEGEN MALWARE

Permanente proactieve bescherming voor NAS-oplossingen (Network Attached Storage). De krachtige anti-malware-engine van Kaspersky Lab scant elk bestand dat wordt geopend of bewerkt op enige vorm van malware, zoals virussen, wormen of trojans. De geavanceerde heuristische analyse identificeert zelfs nieuwe en onbekende dreigingen.

GEOPTIMALISEERDE PRESTATIES

Hoogwaardige scanprestaties dankzij geoptimaliseerde scantechnologie en flexibele uitzonderingsinstellingen zorgen voor een maximale beveiliging en een minimale impact op de systeemprestaties.

BETROUWBAAR

Uitzonderlijke fouttolerantie wordt gerealiseerd door een eenvoudige architectuur met geïntegreerde onderdelen die ontworpen en gebouwd zijn om probleemloos samen te werken. Het resultaat is een stabiele, robuuste oplossing die, als deze geforceerd wordt afgesloten, automatisch opnieuw opstart voor betrouwbare en ononderbroken bescherming.

BEHEERGEMAK

Servers worden op afstand geïnstalleerd en zijn standaard en zonder noodzakelijke herstart beschermd. Deze worden, evenals uw andere beveiligingsoplossingen van Kaspersky, samen beheerd via één eenvoudige en intuïtieve centrale console: Kaspersky Security Center.

FUNCTIES

PERMANENTE PROACTIEVE BEVEILIGING
De toonaangevende anti-malware-engine, ontwikkeld door 's werelds grootste deskundigen op het gebied van informatieverzameling over dreigingen, voorziet in proactieve bescherming tegen nieuwe en potentiële dreigingen met intelligente technologieën voor hogere detectiepercentages.

AUTOMATISCHE UPDATES
De anti-malwaredatabases worden automatisch bijgewerkt zonder het scannen te onderbreken. Zo beschikt u over ononderbroken bescherming, terwijl de werklast voor de beheerder wordt geminimaliseerd.

UITGESLOTEN PROCESSEN EN VERTROUWDE ZONES
De scanprestaties kunnen verder worden verfijnd door 'vertrouwde zones' te creëren en door aan te geven dat bepaalde bestandsindelingen en processen, zoals het maken van back-ups van gegevens, kunnen worden uitgesloten bij het scannen.

SCANNEN VAN AUTOMATISCH UITVOERBARE OBJECTEN
Om het beveiligingsniveau van servers verder te verhogen, kunnen automatisch uitvoerbare bestanden en het besturingssysteem worden gescand om te voorkomen dat malware opstart bij het starten van het systeem.

FLEXIBEL SCANNEN VOOR GEOPTIMALISEERDE PRESTATIES
Verkort de scan- en configuratietijd en bevordert de werklastverdeling, hetgeen helpt de serverprestaties te optimaliseren. De beheerder kan de diepte, omvang en timing van de scanactiviteit opgeven en daarbij bepalen welke bestandstypen en zones moeten worden gescand. On-demand scans kunnen worden ingepland voor momenten met beperkte serveractiviteit.

BESCHERMT HSM- EN DAS-OPLOSSINGEN
Ondersteunt offline scanmodi voor een effectieve bescherming van HSM-systemen (Hierarchical Storage Management). Bescherming voor DAS-oplossingen (Direct Attached Storage) bevordert het gebruik van betaalbare storage-oplossingen.

ONDERSTEUNING VOOR ALLE BELANGRIJKE PROTOCOLLEN
Kaspersky Security for Storage ondersteunt de belangrijkste protocollen die door verschillende storagesystemen worden gebruikt: CAVA agent, RPC en ICAP.

BESCHERMING VAN VIRTUELE SYSTEMEN EN TERMINALSERVERS
Flexibele beveiliging omvat beveiliging voor virtuele (gast)besturingssystemen in virtuele Hyper-V- en VMware-omgevingen en voor Microsoft- en Citrix-terminalinfrastructuren.

BEHEER

GECENTRALISEERDE INSTALLATIE EN CENTRAAL BEHEER
Installatie, configuratie en beheer op afstand, met meldingen, updates en flexibele rapportage via het intuïtieve Kaspersky Security Center. Indien gewenst is ook beheer via de opdrachtregel mogelijk.

CONTROLE OVER BEHEERDERSRECHTEN
Verschillende rechtenniveaus kunnen worden toegewezen aan serverbeheerders, waardoor compliance met specifieke bedrijfsbeleidsregels voor IT-beveiligingsbeleid kan worden gegarandeerd.

FLEXIBELE RAPPORTAGE
Rapportage kan plaatsvinden via grafische rapporten of via de gebeurtenislogboeken van Microsoft Windows® of Kaspersky Security Center. Zoek- en filtertools bieden snelle toegang tot gegevens in omvangrijke logboeken.

SYSTEEMVEREISTEN

HARDWARE:
- x86-compatibele systemen in een configuratie met één of meerdere processors
- x86-64-compatibele systemen met één of meerdere processors

SCHIJFRUIMTE:
- Voor de installatie van alle applicatiecomponenten: 70 MB
- Voor storage van objecten in quarantaine of in back-up: 400 MB (aanbevolen)
- Voor storage van logboeken: 1 GB (aanbevolen)
- Voor storage van databases: 2 GB (aanbevolen)

MINIMALE CONFIGURATIE:
- Processor – 1 kern; verwerkingssnelheid 1,4 GHz
- RAM: 1 GB
- 4 GB vrije ruimte op de harde schijf

AANBEVOLEN CONFIGURATIE:
- Processor – 4 kernen; verwerkingssnelheid 2,4 GHz
- RAM: 2 GB
- 4 GB vrije ruimte op de harde schijf

SOFTWARE:
- Microsoft Windows Server 2003/2003 R2 x86/x64 Standard / Enterprise Edition
- Microsoft Windows Server 2008/2008 R2 x86/x64 Standard / Enterprise / Datacenter Edition (inclusief Core-modus)
- Microsoft Windows Server 2012/20012 R2 Essentials / Standard / Foundation / Datacenter (inclusief Core-modus)
- Microsoft Windows Hyper-V Server 2008 R2
- Microsoft Windows Hyper-V Server 2012/2012 R2

SERVERS:
- Microsoft Terminal Services gebaseerd op Windows 2003 Server;
- Microsoft Terminal Services gebaseerd op Windows 2008 Server;
- Microsoft Terminal Services gebaseerd op Windows 2012/ 2012 R2 Server;
- Citrix Presentation Server 4.0, 4.5;
- Citrix XenApp 4.5, 5.0, 6.0, 6.5;
- Citrix XenDesktop 7.0, 7.1, 7.5

STORAGE-PLATFORMS:
EMC Celerra-/VNX-bestands-storage:
- EMC DART 6.0.36 of hoger;
- Celerra Antivirus Agent (CAVA) 4.5.2.3 of hoger.

Vereisten voor EMC Isilon-storage:
- EMC Isilon OneFS.

Vereisten voor NetApp-storage:
- Data ONTAP 7.x и Data ONTAP 8.x in 7-modus;
- Data ONTAP 8.2.1 of hoger in clustermodus.

Vereisten voor IBM-storage:
- IBM System Storage N-serie.

KS-Storage/Version 2/januari 2015/Global