▶ KASPERSKY SECURITY FOR STORAGE

Hochwirksamer Schutz für Speicherumgebungen von EMC und NetApp

EINLEITUNG

Zerstörerische Malware kann sich mit erschreckender Geschwindigkeit in einer Organisation 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 robusten, hochwirksamen und skalierbaren Schutz für wertvolle und vertrauliche Unternehmensdaten, die sich in Speichersystemen von EMC™ VNX™ und NetApp befinden.

- Echtzeitschutz vor Malware
- Schutz für EMC VNX und NetApp
- Unterstützt zielgerichtete Aufgaben für die Scans kritischer Systembereiche
- Flexible Scan-Konfiguration
- Skalierbar und fehlertolerant
- Anpassbare Nutzung von Systemressourcen
- Schutz für Terminalserver
- Unterstützung für Server-Cluster
- Zertifizierte Kompatibilität mit VMware
- Umfasst die Virenscan-Optimierungen iSwift und iChecker
- Zentrale Verwaltung über das Kaspersky Security Center
- Berichte zur Programmleistung
- Unterstützt SNMP/MOM-Netzwerk-Management

WICHTIGSTE VORTEILE

LEISTUNGSSTARKER MALWARE-SCHUTZ IN ECHTZEIT

Allzeit aktivierter, proaktiver Schutz für netzwerkgebundene Speicherlösungen (NAS). Die leistungsstarke Anti-Malware-Engine von Kaspersky Lab scannt jede aufgerufene oder geänderte Datei auf sämtliche Arten von Malware, einschließlich Viren, Würmer und Trojaner. Eine fortschrittliche, ganzheitliche Analyse erkennt selbst neue und bisher unbekannte Bedrohungen.

OPTIMIERTE SYSTEMLEISTUNG

Hochwirksame Scans auf der Grundlage optimierter Scan-Technologie und flexibler Ausschlusseinstellungen sorgen für maximalen Schutz und schonen gleichzeitig die Systemleistung.

ZUVERLÄSSIG

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: Kaspersky Security Center.

FUNKTIONEN

ALLZEIT AKTIVIERTER, PROAKTIVER SCHUTZ
Die Scans der branchenführenden Anti-Malware-Engine von Kaspersky Lab, entwickelt von erfahrenen Fachleuten im Bereich der IT-Bedrohungen, bieten mit ihrer intelligenten Erkennungstechnologie proaktiven Schutz vor neu aufkommenden 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.

AUSGESCHLOSSENE ZONEN 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.

SCANS VON OBJEKTEN MIT AUTORUN-FUNKTION
Zur Erhöhung des Serverschutzes lassen sich Scans von Autorun-Dateien und Betriebssystemen durchführen, um so die Aktivierung von Malware beim Hochfahren des Systems zu verhindern.

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.

SCHUTZ FÜR HSM- UND DAS-LÖSUNGEN
Unterstützt Offline-Scanmodi zum wirksamen Schutz von Systemen mit Hierarchical Storage Management (HSM). Der Schutz von Direct Attached Storage (DAS) trägt ebenfalls dazu bei, die Nutzung von kostengünstigen Speichersystemen voranzutreiben.

SCHUTZ VON VIRTUALISIERTEN SYSTEMEN UND TERMINALSERVERN
Zur flexiblen Sicherheit gehört der Schutz von virtuellen (Gast-) Betriebssystemen in virtualisierten Hyper-V- und VMware-Umgebungen sowie von Terminalinfrastrukturen von Microsoft und Citrix.

VERWALTUNG

ZENTRALE 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 Kaspersky Security Center überprüft werden. Such- und Filterfunktionen erleichtern den schnellen Datenzugriff in sehr umfangreichen Protokollen.

SYSTEMANFORDERUNGEN

HARDWARE:
- x86-kompatible Systeme in einer Ein- oder Mehrprozessor-Konfiguration
- x86-64-kompatible Systeme in einer Ein- oder Mehrprozessor-Konfiguration

FESTPLATTENSPEICHER:
- Für die Installation aller Programmkomponenten: 70 MB
- Zum Speichern von Objekten in Quarantäne oder für die Sicherung: 400 MB (empfohlen)
- Zum Speichern von Protokollen: 1 GB (empfohlen)
- Zum Speichern von Datenbanken: 2 GB (empfohlen)

MINDESTKONFIGURATION:
- Prozessor: 1 Kern; Prozessorgeschwindigkeit: 1,4 GHz
- RAM: 1 GB
- 4 GB verfügbarer Festplattenspeicher

EMPFOHLENE KONFIGURATION:
- Prozessor: 4 Kerne; Prozessorgeschwindigkeit: 2,4 GHz
- RAM: 2 GB
- 4 GB verfügbarer Festplattenspeicher

SOFTWARE:
- Microsoft Windows Server 2003/2003 R2 x86/x64 Standard/Enterprise Edition
- Microsoft Windows Server 2008/2008 R2 x86/x64 Standard/Enterprise/Datacenter Edition
- Microsoft Windows Server 2012/2012 R2 Essentials/Standard/Foundation/Datacenter
- Microsoft Windows Hyper-V Server 2008 R2
- Microsoft Windows Hyper-V Server 2012/2012 R2

SERVER:
- Microsoft Terminal Services basierend auf Windows 2003 Server
- Microsoft Terminal Services basierend auf Windows 2008 Server
- Microsoft Terminal Services basierend auf 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

SPEICHERPLATTFORMEN:
EMC Celerra-/VNX-Dateispeicher:
- EMC DART 6.0.36 oder höher
- Celerra Antivirus Agent (CAVA) 4.5.2.3 oder höher

Anforderungen an NetApp-Speicher:
- Data ONTAP 7.x und Data ONTAP 8.x im 7-Modus-System
- Data ONTAP 8.2.1 oder höher im Cluster-Modus-System

vmware READY

Windows Server 2012 R2 Certified

KS-Storage/Version 0.2/May14/Global

KASPERSKY lab