



Kaspersky[®] Security for Windows Servers

Zuverlässige Sicherheit für geschäftskritische Prozesse auf Windows-Servern

Auf Windows-Servern basierte Maschinen können ein breites Spektrum von Aufgaben hosten, darunter viele, die unternehmenskritisch sein können. Daher ist es wichtig, dass keine Sicherheitsvorfälle oder Leistungsprobleme den Dauerbetrieb Ihrer Server unterbrechen. Der Schutz muss in Form einer Lösung bereitgestellt werden, die sich minimal auf die Ressourcennutzung und Systemstabilität auswirkt, während sie die Sicherheit der unterschiedlichen Geschäftsszenarien sicherstellt, die von Ihren Servern möglicherweise unterstützt werden.

Kaspersky Security for Windows Server ermöglicht stabile Next Generation-Sicherheit für Server in all den unterschiedlichen Rollen, die sie übernehmen. Für optimale Wirtschaftlichkeit kann die entsprechende Funktionalität durch unterschiedliche Lizenzen aktiviert werden, je nach Art der zu leistenden Aufgabe.

Wichtigste Vorteile

- **Ideal für geschäftskritische Szenarien**
Besonders anpassungsfähig an unterschiedliche Serverrollen, einschließlich geschäftskritischer Szenarien. Dank einer breiten Palette von Schutzkomponenten, zusammen mit verringertem Wartungsaufwand (z. B. weniger erforderliche Neustarts).
- **Geeignet für ältere Systeme**
Geringe Leistungsbeeinträchtigung bei älteren Umgebungen mit begrenzten Hardwareressourcen. Unterstützt Windows Server 2003 (wird von Microsoft mittlerweile nicht mehr unterstützt).
- **Zertifizierte Lösung**
Zertifizierte Kompatibilität mit Virtualisierungsplattformen und Betriebssystemen.

VORTEILE

Vielfach ausgezeichnete und anerkannter Schutz

Kaspersky Security for Windows Server basiert auf Technologien, die immer wieder die Anerkennung von Analysten, Erstplatzierungen in unabhängigen Tests und die Wertschätzung unserer Kunden erhalten. Dies ist die Bestätigung dafür, dass Sie uns Ihre geschäftskritischen Server anvertrauen können.

Besonders vielseitig

Kaspersky Security for Windows Server eignet sich für einen umfangreichen Bereich von Serveraktivitäten und -verwendungsarten, einschließlich Schutz von File-Servern, Netzwerkspeichern und anderen zentralen Elementen der Unternehmensinfrastruktur, um deren reibungslose und sichere Funktion zu gewährleisten.

Cloud-fähig

Kaspersky Security for Windows Server ist darauf ausgelegt, sowohl physische als auch virtuelle Server zu schützen, sodass Sie Server Workloads in Ihrer gesamten Hybrid Cloud-Infrastruktur sicher ausführen können – ob am Unternehmensstandort, im Rechenzentrum oder in öffentlichen Clouds.

Zentrale Verwaltung spart Zeit und Geld

Das Kaspersky Security Center bietet eine einheitliche Konsole, mit der Sie die Sicherheit Ihres Unternehmens verwalten können. Unabhängig davon, ob Ihr primäres Ziel die Benutzerfreundlichkeit oder die besonders fein abgestufte Kontrolle aller Aspekte Ihrer Infrastruktur über eine zentrale Verwaltungskonsole ist – Sie können die Besonderheiten Ihrer Unternehmenssicherheit an Ihre Systemkonfiguration und -anforderungen anpassen und so Betriebskosten reduzieren.

Systemanforderungen

Kaspersky Security for Windows Server wurde für Server entwickelt, die auf 32- oder 64-Bit-Versionen von Microsoft Windows ausgeführt werden:

- Windows Server 2003/2003 R2 SP2
- Windows Server 2008/2008 R2 SP1 oder höher (einschließlich Core-Modus)
- Windows Server 2012/2012 R2 (einschließlich Core-Modus)
- Windows Server 2016 (einschließlich Core-Modus)
- Small Business Server 2008/2011
- Windows MultiPoint Server 2011
- Windows Hyper-V Server 2008 R2 SP1 oder höher/2012/2012 R2/2016
- Windows Storage Server 2012/2012 R2/2016

Kaspersky Security for Windows Server kann auf den folgenden Terminalservern installiert werden:

- Microsoft Remote Desktop Services, basierend auf Windows 2008/2008 R2/2012/2012 R2/2016 Server
- Citrix XenApp 6.0, 6.5, 7.0, 7.5, 7.6, 7.15
- Citrix XenDesktop 7.0, 7.1, 7.5, 7.6, 7.15

Kaspersky Security 10.1 for Windows Server kann zum Schutz der folgenden Network Attached Storages (NAS) eingesetzt werden:

NetApp® unter einem der folgenden Betriebssysteme:

- Data ONTAP® 7.x und Data ONTAP 8.x im 7-Modus
- Data ONTAP 8.2.1 oder höher im Cluster-Modus

Dell EMC Celerra / VNX mit folgender Software:

- EMC DART 6.0.36 oder höher
- Celerra (CAVA) Anti-Virus Agent 4.5.2.3 oder höher
- Dell EMC Isilon mit OneFS 7.0 oder höher

Hitachi NAS auf einer der folgenden Plattformen:

- HNAS 4100
- HNAS 4080
- HNAS 4060
- HNAS 4040
- HNAS 3090
- HNAS 3080

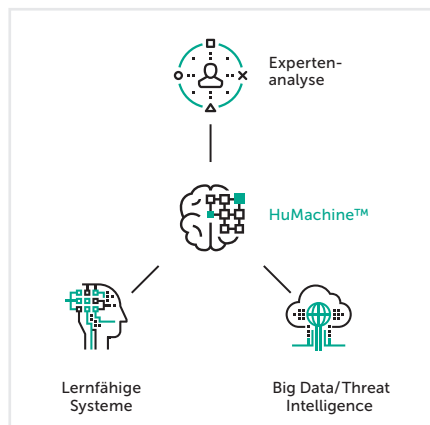
IBM NAS-Serie IBM System Storage N-Serie

Oracle NAS-Systemserie Oracle ZFS Storage Appliance

Dell NAS auf der Plattform Dell Compellent FS8600

Mindestanforderungen für die Hardware:

- Prozessor: 1,4 GHz, Einzelkern
- RAM: 1 GB
- Laufwerk-Subsystem: 4 GB



Programmfunktionen

Next Generation-Schutz vor Malware und mehr. Kaspersky Security for Windows Server basiert auf unserer einzigartigen mehrstufigen Schutzplattform, unterstützt durch maschinelles Lernen und menschlicher Expertise, und ermöglicht die Erkennung aller Formen von Malware-Angriffen, darunter auch hoch entwickelte, komplexe und neu entstehende Bedrohungen. Das Kaspersky Security Network (KSN) reagiert schnell auf neue Bedrohungen, erhöht die Schutzleistung und verringert das Risiko von Fehlalarmen auf nahezu Null.

Freigegebene Ordner und Speicherschutz vor verschlüsselter Malware. Eine Antiverschlüsselungs-Komponente blockiert die Verschlüsselung von Dateien in gemeinsam genutzten Ressourcen, die von einem Prozess schädlicher Natur auf einer anderen Maschine im Netzwerk verursacht werden könnte. Diese Funktionalität gilt sowohl für Windows- als auch für NetApp-Speichersysteme.

NEU: Exploit Prevention. Die leistungsstarke Exploit-Präventionstechnologie wacht über geschützte Prozesse, um zu verhindern, dass Exploits nicht gepatchte oder gar Zero-Day-Schwachstellen in Programmen und Systemkomponenten angreifen.

NEU: System-Hardening. Durch Anwendung eines Default-Deny-Szenarios mittels Programmstart-Kontrolle wird die Stabilität Ihres Systems gegenüber Datenschutzverletzungen optimiert. Durch das Unterbinden der Ausführung jeglicher Programme, Services und vertrauenswürdiger Systemkomponenten, die nicht explizit von Ihnen zugelassen wurden, können Sie die meisten Formen von Malware automatisch vollständig blockieren. In Kombination mit der Gerätekontrolle von Kaspersky Lab wird mit der Ausführung im Default Deny-Modus auch eine unerwünschte Speicherung verhindert. So wird Ihre Angriffsfläche erheblich reduziert und Ihre Serversicherheit enorm gesteigert.

NEU: Systemintegrität. Sicherzustellen, dass geschäftskritische Systemkomponenten und Prozesse (sowie Programme) intakt bleiben, ist sowohl für das reibungslose Funktion Ihrer Server als auch für die Sicherheit der sensiblen Daten, mit denen sie arbeiten, unverzichtbar. Die Komponenten von Kaspersky Security for Windows Server, z. B. die Dateiintegritätsüberwachung (File Integrity Monitor, FIM) oder die Protokollüberprüfung, identifizieren nicht nur unerwünschte Änderungen an Ihren Systemen, sondern können auch unter Einhaltung bestimmter Vorschriften wie z. B. PCI DSS verschiedene Indikatoren für eine Sicherheitsverletzung erkennen.

NEU: Sicherheit des Datenverkehrs. Kaspersky Security for Windows Server untersucht jetzt Datenverkehr auf Malware, überprüft Weblinks und bietet Webressourcenkontrolle auf Grundlage der von Kaspersky Lab definierten Kategorien für alle externen Systeme, die das ICAP-Protokoll unterstützen, einschließlich Proxy-Servern und Speichern.

Schutz für Terminalserver. Eine Vielzahl von Fernzugriffsumgebungen kann gesichert werden, darunter Microsoft Remote Desktop Services und Citrix XenApp/Xen Desktop.

NEU: Verwaltung von Windows-Firewalls. Die Firewalls Ihrer Windows-Server können direkt über das Kaspersky Security Center konfiguriert werden, sodass die Verwaltung lokaler Firewalls bequem über eine einzige, einheitliche Konsole erfolgen kann.

NEU: SIEM-Integration. Kaspersky Security for Windows Server lässt sich in die meisten führenden SIEM-Systemen integrieren, wobei Ereignisse in Programmprotokollen in vom Syslog-Server unterstützte Formate umgewandelt werden, sodass sie erkannt und in SIEM importiert werden können. Das Programm unterstützt die Konvertierung sowohl in strukturierte Daten- als auch in JSON-Formate.

Hinweise zum Kauf

Kaspersky Security for Windows Server ist erhältlich als Bestandteil von:

- Kaspersky Endpoint Security for Business – Select (ohne Programmstart-Kontrolle)
- Kaspersky Endpoint Security for Business – Advanced
- Kaspersky Total Security for Business
- Kaspersky Hybrid Cloud Security

Das Programm kann auch als Teil einer der folgenden Targeted Solutions erworben werden: Kaspersky Security for File Server und Kaspersky Security for Storage.

www.kaspersky.de

© 2018 Kaspersky Labs GmbH. Alle Rechte vorbehalten. Eingetragene Handelsmarken und Markenzeichen sind das Eigentum ihrer jeweiligen Rechtsinhaber.