KASPERSKY SECURITY FOR WINDOWS SERVER™

Speziell entwickelt für hochleistungsfähige Unternehmensserver

Durch die immer weiter zunehmende Komplexität von IT-Netzwerken in Unternehmen muss auch der größtmögliche Schutz für die Server gewährleistet werden. Eine einzelne infizierte Datei auf Ihrem Unternehmensserver kann sich auf jeden Computer innerhalb Ihres Netzwerks ausbreiten und beträchtlichen Schaden anrichten. Eine geeignete und spezielle Serversicherheitslösung sorgt nicht nur dafür, dass geschäftskritische Daten vor aktuellen Malware-Bedrohungen geschützt sind. Sie wehrt außerdem die Gefahr ab, dass Malware Sicherungskopien von Dateien befällt, was wiederum zu Mehrfachausbrüchen führen kann.

Kaspersky Security for Windows Server bietet kosteneffektiven, zuverlässigen und skalierbaren Schutz für freigegebenen Dateispeicher, der gleichzeitig die Systemressourcen schont.

Wichtigste Vorteile

SCHUTZ VOR BEKANNTER, UNBEKANNTER UND HOCH ENTWICKELTER MALWARE
Unsere vielfach ausgezeichnete Anti-Malware-Engine bietet schnellere Scans, schont Systemressourcen und kann dank cloud-basierter Sicherheit (Kaspersky Security Network) hohe Erkennungsquoten aufweisen.

ZUSÄTZLICHE SICHERHEIT FÜR UNTERNEHMENSKRITISCHE SERVER
Die leistungsstarke Programmstart-Kontrolle in Kombination mit den Global Security Intelligence- und Anti-Cryptor-Funktionen bieten zusätzlichen Schutz für Ihre Unternehmensspeicher und -server.

ZERTIFIZIERTE LÖSUNG
Das Programm ist für die Kompatibilität mit Virtualisierungsplattformen und Betriebssystemen zertifiziert.

Programmfunktionen

WIRKSAMER SCHUTZ VOR SCHÄDLICHEN PROGRAMMEN

Dauerhafter Malware-Schutz und bedarfsgesteuerte Scans: Das Programm scannt jede aufgerufene oder geänderte Datei. Verdächtige Objekte werden behandelt, gelöscht oder in Quarantäne verschoben. Wenn eine neue Software installiert wird oder der Verdacht auf eine infizierte Datei besteht, kann der Administrator auch einen gezielten Malware-Scan des verdächtigen Bereichs starten.

Cloud-basierter Serverschutz: Kaspersky Security Network (KSN) reagiert schneller als jemals zuvor auf neue Bedrohungen, verbessert die Leistung von Schutzkomponenten und minimiert das Risiko von Fehlalarmen (False-Positives).

Leistungsstarke Programmstart-Kontrolle auf den Servern: Beispiellose Sicherheit durch konfigurierte Regeln, die zulassen bzw. unterbinden, dass ausführbare Dateien, Skripte und MSI-Pakete gestartet oder DLL-Module auf dem Server geladen werden.

Schutz freigegebener Ordner vor Crypto-Malware (Anti-Cryptor): Wenn Dateiverschlüsselungsvorgänge erkannt werden, verhindert das Programm den Zugriff des Ursprungscomputers auf sämtliche Dateifreigaben des geschützten Servers.

Zugriffsverweigerung für Hosts mit verdächtigen Aktivitäten: Eine Funktion, die den Computerzugriff auf freigegebene Netzwerkordner auf einem geschützten Server blockiert, wenn im Rahmen von Echtzeit-Dateischutz- oder Anti-Cryptor-Aufgaben schädliche Aktivitäten bei diesen Computern erkannt werden.

Proaktiver Schutz vor Malware: Fortschrittliche Technologien zum Schutz vor Malware, z. B. ein heuristisches Analyseprogramm, das Schadprogramme mit sehr hohem Präzisionsgrad erkennt, selbst wenn die Programmsignatur noch nicht den Malware-Datenbanken hinzugefügt wurde.

Scans der kritischen Bereiche des Betriebssystems: Im Rahmen einer zielgerichteten Aufgabe lassen sich die Bereiche eines Betriebssystems überprüfen, die dem größten Infektionsrisiko ausgesetzt sind. So kann beispielsweise mit einem Scan von Autorun-Dateien verhindert werden, dass Malware beim Hochfahren des Systems gestartet wird. Auch versteckte Prozesse lassen sich auf diese Weise erkennen.

Flexible Scaneinstellungen: Die Einstellungen für Dateiscans geben dem Administrator folgende Möglichkeiten:

- Ausschließen bestimmter Prozesse vom Scan-Vorgang
- Einstellen des Virenschutzumfangs
- Festlegen, welche Dateitypen immer gescannt und welche komplett ausgeschlossen werden sollen
- Vorabfestlegen von Reaktionen auf verdächtige und infizierte Objekte je nach Art der Bedrohung.

Dieser Ansatz sorgt für eine bessere Verteilung der Serverlast und für flexibles Sicherheitsmanagement in Unternehmensnetzwerken.

Schutz von Terminal- und virtuellen Servern: Das Programm schützt Microsoft Terminal Services- und Citrix XenApp-Server. Endbenutzer, die im Desktop-/Application-Publishing-Modus arbeiten, bleiben durchgehend geschützt und werden über Ereignisse informiert. Hyper-V-, XenDesktop- und VMware™-Umgebungen werden ebenfalls unterstützt.

Cluster-Unterstützung: Das Programm eignet sich ideal für komplexe Architekturen mit Server-Clustern und schützt lokale Festplatten sowie freigegebene Cluster-Festplatten, die derzeit dem geschützten Node zugeordnet sind.

Hohe Leistung

Skalierbarkeit: Für Server mit mehreren Prozessoren kann der Administrator die Anzahl der Anti-Malware-Threads festlegen und damit sicherstellen, dass Serveranfragen schneller verarbeitet werden.

Performance-Steuerung: Die Zuteilung von Ressourcen an Kaspersky Security for Windows Server und andere Programme erfolgt auf Grundlage vorab festgelegter Prioritäten: Malware-Scans können auch im Hintergrundmodus ausgeführt werden.

Auswahl vertrauenswürdiger Prozesse: Der Administrator hat die Möglichkeit, sichere Prozesse wie Datensicherungen oder Festplattendefragmentierungen vom Scanvorgang auszuschließen, um eine optimale Leistung des Systems zu gewährleisten.

Ununterbrochener Serverbetrieb: Wenn der Malware-Schutz installiert oder aktualisiert wird, benötigt Kaspersky Security for Windows Server keinen Neustart.

Flexible Verwaltung

Auswahl von Verwaltungstools: Das Programm kann entweder direkt oder per Fernzugriff über die Microsoft Management Console, das Kaspersky Security Center oder die Befehlszeile gesteuert werden. Die neueste Produktversion enthält eine intuitiv bedienbare, grafische Benutzeroberfläche für die Microsoft Management Console.

Einfach zu bedienende Installations- und Verwaltungstools: Kaspersky Security Center ist eine Verwaltungskonsole, die die gleichzeitige Remote-Installation und -Konfiguration des Programms auf mehreren Servern ermöglicht. Zudem bietet sie Unterstützung während des Betriebs sowie beim Empfang von Updates und Benachrichtigungen.

Kontrolle über Administratorrechte: Das Programm ermöglicht das Einrichten unterschiedlicher Rechteebenen, die den Administratoren der verschiedenen Server zugewiesen werden können. So können die Anforderungen einzelner IT-Abteilungen sowie interne Sicherheitsanforderungen erfüllt werden.

Flexible Einstellung der Scan-Zeiten: Um Unterbrechungen zu vermeiden und die Verfügbarkeit von Serverressourcen zu steigern, lassen sich Scans ganz einfach zeitlich planen.

Benachrichtigungssystem: Das Programm unterstützt Administratorbenachrichtigungen per Nachrichtendienst oder E-Mail für ein umfangreiches Ereignisspektrum. Das Programm ist in das Simple Network Management Protocol (SNMP) integriert und kann zusammen mit dem Microsoft Operations Manager (MOM) eingesetzt werden. Alternativ kann der Administrator die Arbeit des Programms durch eine Überprüfung der Microsoft-Windows- oder Kaspersky-Security-Center-Ereignisprotokollen überwachen.

Kaufen

Kaspersky Security for Windows Server ist erhältlich als Bestandteil von:
- Kaspersky Endpoint Security for Business – Select (inkl. Anti-Cryptor und untrusted Host Blocker, ohne Applications Launch Control)
- Kaspersky Endpoint Security for Business – Advanced (inkl. Anti-Cryptor, untrusted Host Blocker und Applications Launch Control)
- Kaspersky Total Security for Business

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

Eine Liste der Partner von Kaspersky Lab finden Sie unter: www.kaspersky.com/de/partner_finden

Weitere Informationen finden Sie auf: www.kaspersky.de

SYSTEMANFORDERUNGEN

- Kaspersky Security for Windows Server wurde für Server entwickelt, die auf 32- oder 64-Bit-Versionen von Microsoft Windows ausgeführt werden:
  - Microsoft Windows Server 2008/2008 R2 x86/x64 Standard/ Enterprise/Datacenter SP1 oder höher (einschließlich Core-Modus)
  - Microsoft Windows Hyper-V Server 2008 R2 SP1 oder höher
  - Microsoft Windows Server 2012/2012 R2 Essentials/Standard/ Foundation/Datacenter (einschließlich Core-Modus)
  - Microsoft Windows Hyper-V® Server 2012/2012 R2

- Kaspersky Security for Windows Server kann auf den folgenden Terminalservern installiert werden:
  - Microsoft Remote Desktop Services basierend auf Windows 2008 Server
  - Microsoft Remote Desktop Services basierend auf Windows 2008/2012/2012 R2 Server
  - Citrix® XenApp® 6.0, 6.5, 7.0, 7.5, 7.6
  - Citrix XenDesktop® 7.0, 7.1, 7.5, 7.6.

Verwaltungskonsole:
- Microsoft Windows XP SP2/ Vista®/7/8/10 Enterprise/ Professional x86/x64
- Microsoft Windows Server 2008/2008 R2 Standard/Enterprise/ Datacenter SP1 oder höher x64
- Microsoft Windows Server 2012/2012 R2 Essentials/Standard/ Foundation/Datacenter x64
- Microsoft Windows Hyper-V Server 2008 R2 SP1/2012/2012 R2 oder höher x64

Hardware-Anforderungen:
- Prozessor – Intel® Pentium® IV
- Prozessorgeschwindigkeit: 2,4 GHz
- RAM: 512 MB
- Festplattensubsystem: 1 IDE

CITRIX READY

vmware PARTNER TECHNOLOGY ALLIANCE

Windows Server 2012 R2 Certified

Kaspersky Security for Windows Server/Version 3/Februar 2016/Global

KASPERSKY lab