

# ► KASPERSKY SECURITY FOR VIRTUALIZATION

Zuverlässiger, flexibler und effizienter Schutz für virtualisierte Server- und Desktop-Umgebungen

## WICHTIGSTE VORTEILE

### UMFASSENDE SCHUTZ

- Unterstützt VMware-, Microsoft Hyper-V- und Citrix Xen-Plattformen.
- Die vielfach ausgezeichnete Technologie schützt virtuelle Maschinen (VMs) vor komplexer Malware.
- Die Integration in das Cloud-basierte Kaspersky Security Network (KSN) schützt proaktiv vor allen aufkommenden Bedrohungen weltweit.
- Der erweiterte Malware-Schutz umfasst einen automatischen Exploit-Schutz und bietet leistungsstarke Sicherheit auf mehreren Ebenen.
- Programmkontrolle (mit Integration dynamischer Whitelists) sowie Web- und Gerätekontrolle ermöglichen dem Administrator die Durchsetzung von Sicherheitsrichtlinien.
- Eine leistungsstarke Kombination aus Network Attack Blocker, Firewall, Host-basiertem System zur Angriffsüberwachung (Host-based Intrusion Prevention System, HIPS) und Anti-Phishing-Technologien schützt VMs vor Netzwerkbedrohungen.
- Agentenlose VMs und alle nicht-persistenten VMs werden sofort und automatisch durch eine kontinuierlich aktualisierte Security Virtual Appliance (SVA) geschützt.\*

### MEHR LEISTUNG

- Das innovative Design gewährleistet die Schonung der Systemressourcen und optimiert Konsolidierungsraten für maximale Virtualisierungsdichte.
- Die Shared-Cache-Technologie reduziert doppelten Scanaufwand.
- AV-Update- und Scan-Stürme sowie „Instant-on“-Lücken werden vermieden.

### HÖHERE EFFIZIENZ

- Schnelles und unkompliziertes Deployment, kein Neustart oder Wartungsmodus erforderlich.
- Eine umfassende Konsole ermöglicht es, physische, virtualisierte und mobile Endpoints gemeinsam zu verwalten.
- Vereinfachte Administration und verbessertes Deployment bieten höhere Effizienz und weniger Risiken für Konfigurationsfehler.
- Flexible Lizenzierung – wählen Sie zwischen der Lizenzierung nach Anzahl der virtualisierten Maschinen (Desktops oder Server) oder der Ressourcen (Anzahl der Kerne).

\*Persistente VMs mit Light-Agent-Funktion sind geschützt, sobald der Light Agent installiert wurde.

# **KASPERSKY SECURITY FOR VIRTUALIZATION IST EINE FLEXIBLE LÖSUNG, DIE SOWOHL SCHUTZ ALS AUCH LEISTUNG FÜR IHRE VIRTUALISIERTE UMGEBUNG GARANTIERT.**

## **WICHTIGE PRODUKTFUNKTIONEN**

- Zentralisierte Verwaltung über das Kaspersky Security Center
- Zentralisierter VM-Schutz über eine einzige SVA
- Verbesserter Malware-Schutz
- Host-basierte Angriffsüberwachung (Host-based Intrusion Prevention System, HIPS) und Firewall
- Endpoint-Kontrolle für Programme, Internetzugriff und Peripheriegeräte
- Cloud-basierte Sicherheit über das Kaspersky Security Network
- Network Attack Blocker
- Anti-Phishing
- Anti-Virus für IM-, Mail- und Internetdatenverkehr
- Keine zusätzliche Installation oder Neustarts für neue VMs\*

## **SECURITY VIRTUAL APPLIANCE (SVA)**

Kaspersky Lab bietet in diesem Bereich zwei herausragende Lösungen, die beide auf einer Security Virtual Appliance basieren.

Die Security Virtual Appliance (SVA) von Kaspersky Lab scannt alle VMs in der Host-Umgebung zentral. Diese Architektur bietet effizienten VM-Schutz, schont gleichzeitig die Ressourcen des Endpoints und verhilft Ihnen zu besseren Konsolidierungsraten. AV-Scan- und Update-Stürme sowie „Instant-on“-Lücken werden vermieden.

Kaspersky Security for Virtualization unterstützt VMware-, Microsoft Hyper-V- und Citrix Xen-Plattformen und ihre Kerntechnologien.

## **FLEXIBLE LIZENZIERUNG**

Kaspersky Security for Virtualization steht, abhängig von Ihren Anforderungen, mit folgenden Lizenzoptionen zur Verfügung:

- Maschinenbasierte Lizenzierung
  - Pro Desktop
  - Pro Server
- Ressourcenbasierte Lizenzierung
  - Pro Kern

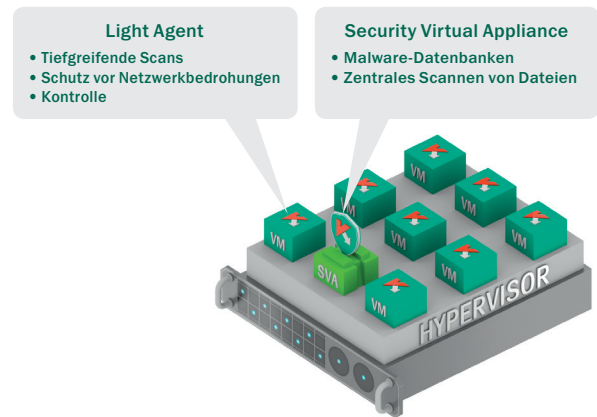
## **VIELE PLATTFORMEN, EIN PREIS**

Eine Einzellizenz von Kaspersky Security for Virtualization umfasst die Unterstützung für virtualisierte Citrix-, Microsoft- und VMware-Umgebungen.

\* Bei nicht-persistenten VMs ist ein sofortiger Schutz verfügbar, sobald der Light Agent im Image der VM integriert ist. Bei persistenten VMs muss der Administrator den Light Agent bei der Installation manuell einrichten.

## LIGHT AGENT FÜR ERWEITERTEN SCHUTZ

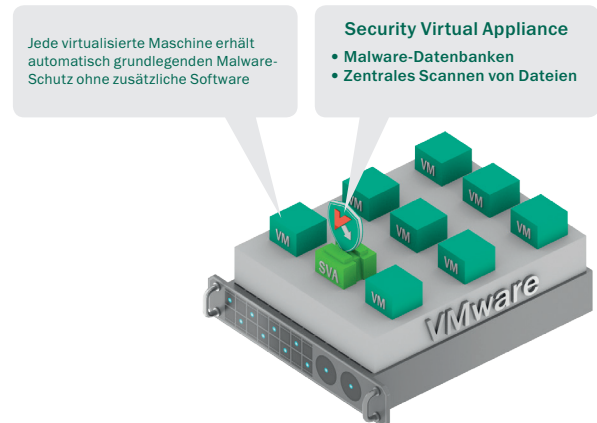
Kaspersky Security for Virtualization umfasst einen leistungsstarken Light Agent, der auf jeder virtualisierten Maschine bereitgestellt wird. Dies ermöglicht die Aktivierung erweiterter Endpoint-Sicherheitsfunktionen. Dazu zählen Vulnerability Monitoring, Programm-, Geräte- und Web-Kontrolle, Virenschutz des Instant-Messaging-, E-Mail- und Internet-Datenverkehrs sowie erweiterte Heuristik. Das Ergebnis ist leistungsstarke Sicherheit auf mehreren Ebenen in Kombination mit effizienter Leistung.



Kaspersky Security for Virtualization  
Light-Agent-Konfiguration

## AGENTENLOSE KONFIGURATION – VMWARE-UMGEBUNGEN

Tiefere Integration in VMware-Technologien bedeutet, dass Kaspersky Security for Virtualization auf dieser Plattform auch in einer agentenlosen Sicherheitskonfiguration sehr einfach bereitgestellt und verwaltet werden kann. Die gesamte Sicherheitsaktivität ist in der Security Virtual Appliance vereint und interagiert mit Schnittstellen von vShield – für sofortigen automatischen Schutz virtualisierter Maschinen – und vCloud für den Netzwerkschutz.



Kaspersky Security for Virtualization  
Agentenlose Konfiguration

Erweiterte Sicherheitsfunktionen wie Datei-Quarantäne, HIPS, Vulnerability Scanning und Endpoint-Kontrolle stehen bei dieser Konfiguration nicht zur Verfügung.

 <b>Agentenbasierte Sicherheit</b>	 <b>Agentenlose Sicherheit</b>	 <b>Light-Agent-Sicherheit</b>
<ul style="list-style-type: none"> <li>• Funktioniert auf jedem Hypervisor</li> <li>• Wenn VM-Dichte nicht entscheidend ist</li> <li>• Windows-, Linux- oder Mac-Gast-VMs</li> </ul>	<ul style="list-style-type: none"> <li>• Nur VMware</li> <li>• Ermöglicht hohe VM-Dichte</li> <li>• Windows-Gast-VMs</li> <li>• Minimaler Aufwand für die IT bei Installation und Verwaltung</li> <li>• Kommt typischerweise bei einer Server-Virtualisierung mit kontrollierter Internetkonnektivität (kein Surfen) zum Einsatz</li> </ul>	<ul style="list-style-type: none"> <li>• VMware, Citrix oder Hyper-V</li> <li>• Ermöglicht hohe VM-Dichte</li> <li>• Windows-Gast-VMs</li> <li>• Erweiterte Sicherheit und Richtliniendurchsetzung</li> <li>• Wird für gewöhnlich bei VDI und Servern mit kritischen Rollen genutzt</li> </ul>

## UNTERSTÜTZTE PLATTFORMEN:

- Microsoft Hyper-V Server 2008 R2/2012
- Citrix XenServer 6.0.2/6.1
- VMware ESXi 4.1, 5.0, 5.1 und 5.5

## UNTERSTÜTZTE GASTBETRIEBSSYSTEME:

Bereitstellungsmethode	Light Agent			Agentenlose
	Windows Server 2008 R2 Hyper-V und Windows Server 2012 Hyper-V	XenServer 6.0.2 und 6.1	VMware ESXi 5.1 und 5.5	
Auf der virtuellen Maschine installiertes Gastbetriebssystem				
Windows XP Professional SP3 (32 Bit)	Ja	Ja	Nein	Ja
Windows XP Professional SP2 (64 Bit)	Ja	Nein	Nein	Nein
Windows 7 Professional/Enterprise/Ultimate SP1 oder höher (32/64 Bit)	Ja	Ja	Ja	Ja
Windows 8 Pro/Enterprise (32/64 Bit)	Ja	Ja	Ja	Nein
Windows Vista Business/Enterprise/Ultimate SP2 (32 Bit)	Ja	Nein	Nein	Ja
Windows Server 2008 R2 Standard/Enterprise SP1 (64 Bit)	Ja	Ja	Ja	Ja
Windows Server 2008 Standard/Enterprise SP2 (32/64 Bit)	Ja	Ja	Ja	Ja
Windows Server 2003 R2 Standard/Enterprise SP2 (32/64 Bit)	Ja	Nein	Ja	Ja
Windows Server 2003 Standard SP2 (32/64 Bit)	Ja	Ja	Nein	Ja
Windows Server 2012 (64 Bit)	Ja	Ja	Ja	Nein
Windows Small Business Server 2008 Standard (64 Bit)	Ja	Nein	Nein	Nein
Windows Small Business Server 2011 Essentials/Standard (64 Bit)	Ja	Nein	Nein	Nein

Weitere Informationen zu Kaspersky Security for Virtualization erhalten Sie von Ihrem lokalen Kaspersky-Partner oder unter [www.kaspersky.de/business-security](http://www.kaspersky.de/business-security).

KSV/Version 3.1/April 14/Global

© 2014 Kaspersky Lab ZAO. Alle Rechte vorbehalten. Eingetragene Markenzeichen und Handelsmarken sind das Eigentum ihrer jeweiligen Rechtsinhaber. Windows Server ist ein eingetragenes Markenzeichen der Microsoft Corporation in den USA und anderen Ländern.

