Kaspersky® Security for Virtualization

Neuheiten in Kaspersky Security for Virtualization 4.0 für noch mehr Schutz

Immer mehr Unternehmen nutzen die Vorteile softwarezentrierter Rechenzentren. Der Bedarf an verlässlicher IT-Sicherheit ohne Produktivitätseinbußen ist daher so hoch wie nie. Mit Kaspersky Security for Virtualization 4.0 definieren wir die Interaktion Ihres softwaredefinierten Rechenzentrums und der zugehörigen Sicherheitslösung neu, um beide Komponenten intelligenter, schneller und effizienter denn je zu gestalten.

Top-5:

- Unterstützung für VMware vSphere 6.5
- Unterstützung für VMware NSX 6.2 und 6.3
- Unterstützung für Windows 10 (einschließlich RS1)
- Unterstützung für Linux Server OS
- Umfassende Überprüfung der Infrastruktur

Native agentenlose Integration in VMware NSX 6.2 und 6.3

Agentenloser Malware-Schutz

Der auf unserer vielfach ausgezeichneten Engine basierende Malware-Schutz wird sofort für jede von VMware NSX verwaltete VM (Virtual Machine) bereitgestellt, sodass Sie keinen Client mehr auf der Maschine installieren müssen.

Blockieren von Netzwerkangriffen

Funktionen zur Angriffserkennung und -überwachung (Intrusion Detection and Prevention; IDS/IPS) werden ebenfalls den von der VMware NSX-Plattform verwalteten virtuellen Hosts bereitgestellt. So schützen Sie Ihre virtualisierte Infrastruktur selbst vor den ausgefeiltesten netzwerkbasierten Bedrohungen sowie Zero-Day-Schwachstellen.

Automatisierte Bereitstellung

Die enge Integration in VMware NSX ermöglicht eine vollständig automatisierte Bereitstellung von Sicherheits-Appliances (Security Virtual Machine oder Network Attack Blocker). Diese Funktionen werden automatisch basierend auf den Sicherheitsrichtlinien jeder einzelnen VM „eingeblendet".

Sicherheitsrichtlinien

Dank der engen Integration in VMware NSX stehen Ihnen auf jeder VM präzise und fein abgestufte Sicherheitsfunktionen zur Verfügung. So erstellen und skalieren Sie ein perfekt ausbalanciertes softwarezentriertes Rechenzentrum.

Security Tags

Kaspersky Security for Virtualization und die VMware NSX-Plattform tauschen jetzt Sicherheitsmarkierungen aus (die so genannten Security Tags). Diese können basierend auf speziellen Regeln (z. B. bei auf einer VM erkannten Malware) geändert werden. Dank dieser fortlaufenden Interaktion zwischen der Infrastruktur und ihrer Sicherheitslösung kann das softwarezentrierte Rechenzentrum in Echtzeit auf Sicherheitsvorfälle reagieren und bei Bedarf automatisch eine Neukonfiguration der gesamten virtualisierten Infrastruktur einleiten.

vmware PARTNER TECHNOLOGY ALLIANCE

vmware READY NETWORKING AND SECURITY

Verbesserungen der Produktarchitektur

Agentenloses Überprüfen inaktiver VMs

Bedarfsorientierter Scan aktiver und inaktiver virtueller Maschinen. Keine „herkömmliche" Lösung kann einen agentenlosen Scan nach Malware für eine VM durchführen, die derzeit offline ist. Die neue Version von Kaspersky Security for Virtualization verfügt über eine neuartige Funktion, die alle VMs scannt – ob offline oder online. So erreichen Sie einen effektiveren bedarfsorientierten Scan und eine bessere Sicherheitsabdeckung in Ihrer gesamten Infrastruktur.

vShield Endpoint-API weiterhin unterstützt

Ein großer Teil der Unternehmen migriert zu VMware NSX oder hat eine derartige Migration bereits geplant. Viele nutzen jedoch weiterhin die bisherige Technologie vShield Endpoint. Security for Virtualization Agentless 4.0 unterstützt vShield Endpoint weiterhin im vollen Umfang. Zudem planen wir, diese Technologie so lange zu unterstützen, wie sie von unseren Kunden eingesetzt wird. So können Sie den Wechsel aus der Sicherheitsperspektive reibungslos und flexibel nach Ihrem eigenen Zeitplan durchführen.

Agentenlos und Light Agent für Linux OS

Wir schützen Windows- und Linux-Server mit Kaspersky Security for Virtualization. Außerdem können wir dies nun agentenlos und mit Light Agent anbieten. Kaspersky Security for Virtualization ist die wahrhaft perfekte Cybersicherheitslösung für hybride Rechenzentren. Sie stellt ungeachtet des Betriebssystems fortschrittliche Sicherheitsfunktionen für alle virtuellen Server bereit.

KSV in der agentenlosen Version unterstützt:

- RHEL 7 GA (64 Bit)
- SLES 12 GA (64 Bit)
- Ubuntu 14.04 LTS (64 Bit)

KSV Light Agent unterstützt:

- Red Hat Enterprise Linux Server 6.7, 7.2
- SUSE Linux Enterprise Server 12 SP1
- CentOS 6.8, 7.2
- Debian 8.5
- Ubuntu Server 14.04, 16.04 LTS

Light Agent für KVM auf RHEL

Wir werden die Liste der unterstützten Virtualisierungsplattformen weiter ausbauen. Eine neue Version von Kaspersky Security for Virtualization Light Agent unterstützt den KVM-Hypervisor auf Basis des Betriebssystems RHEL-Server (Red Hat Enterprise Linux Server).

Light Agent im Ruhemodus

Die Benutzeroberfläche von Kaspersky Security for Virtualization Light Agent kann jetzt auf jeder VM im gesamten Rechenzentrum deaktiviert werden (durch Auslagerung). Dies ist beispielsweise für die Desktop-Virtualisierung unter Windows Server nützlich, wenn Remote Desktop oder Terminal Services aktiviert sind, oder bei der Virtualisierung von Anwendungen basierend auf Citrix XenApp.

Ein KSV-Integrationsserver für mehrere Multiple vCenter-Server

Der dedizierte Integrationsserver von Kaspersky Security for Virtualization kann mit mehreren VMware vCenter-Servern verbunden werden, um mehr Informationen aus Ihrer VMware-basierten virtualisierten Infrastruktur abzurufen.

Erweiterter SNMP-Agent auf SVM

Kaspersky Security for Virtualization kann mit einem SNMP-Agent installiert werden. Dieser überwacht und sendet umfassende Informationen zum Zustand der SVM an SNMP-Überwachungstools von Drittanbietern wie Zabbix und Nagios. SNMP-Zähler stellen allgemeine SVM-Kennzahlen (CPU, RAM usw.) sowie spezielle Metriken zur Verfügung.

Ausnahmen für das Durchsetzungsmanagement

Kaspersky Security for Virtualization Light Agent bietet jetzt eine umfassendere Liste von Anwendungen unterschiedlicher Softwarehersteller, die bei der Angabe von Ausnahmen oder Konfiguration durchgesetzter Scanrichtlinien verwendet werden kann.

Einheitliche Installation von Plug-in und Integrationsserver

Die Installation des Verwaltungs-Plug-ins und Integrationsservers von Kaspersky Security for Virtualization wurde zu einem einzigen Vorgang zusammengefasst. Das Plug-in und die Verwaltungskonsole des Integrationsservers werden nun mithilfe des Installationsassistenten für Kaspersky Security Management-Komponenten installiert und konfiguriert. Sie können die Installation auch über die Befehlszeile durchführen.

Unterstützung für weitere Microsoft-Lösungen

Windows Server 2016

Kaspersky Security for Virtualization Light Agent und Agentless umfassen jetzt beide erweiterte Sicherheitsfunktionen für Microsoft Windows Server 2016.

Windows 10 Red Stone 1 (RS1)

Kaspersky Security for Virtualization Light Agent und Agentless unterstützen bereits das Betriebssystem Windows 10, das in VDI-Umgebungen häufig eingesetzt wird. Jetzt fügen wir auch Unterstützung für Windows 10 Red Stone 1 (RS1) hinzu.

Vollmodus und Server-Core-Modus

Kaspersky Security for Virtualization 4.0 Light Agent und Agentless unterstützen Windows Server-Betriebssysteme im Vollmodus und im Server-Core-Modus. Dies ist besonders wichtig, da Unternehmen immer häufiger kritische Infrastrukturserver ohne Benutzeroberfläche im Server-Core-Modus bereitstellen (z. B. Domain Controller, DHCP, DNS).

Windows Hyper-V 2016

Kaspersky Security for Virtualization Light Agent unterstützt zudem die neueste Virtualisierungsplattform von Microsoft. Unternehmen können jetzt auch Hyper-V 2016-basierte Rechenzentren mit Kaspersky Lab schützen.

Bereitstellung über SCVMM

Kaspersky Security for Virtualization Light Agent kann über System Center Virtual Machine Manager (SCVMM) auf mehreren Microsoft Windows Hyper-V-Hosts gleichzeitig bereitgestellt werden.

Vollständige Liste unterstützter Plattformen und Betriebssysteme

VMware-Virtualisierung

- VMware NSX 6.3, 6.2
- VMware vSphere 6.5, 6.0, 5.5, 5.1

Microsoft-Virtualisierung

- MS Windows Server 2016 Hyper-V
- MS Windows Server 2012 R2 Hyper-V
- Bereitstellung über SCVMM 2016, 2012 R2

Citrix-Virtualisierung

- Citrix XenServer 7.0, 6.5 SP1

KVM-Virtualisierung

- RHEL Server 7 Update 1
- Ubuntu Server 14.04
- CentOS 7.2

VDI-Plattformen

- VMware Horizon View 7
- Citrix XenDesktop 7.12, 7.11, 7.9
- Citrix PVS 7.12, 7.11, 7.9

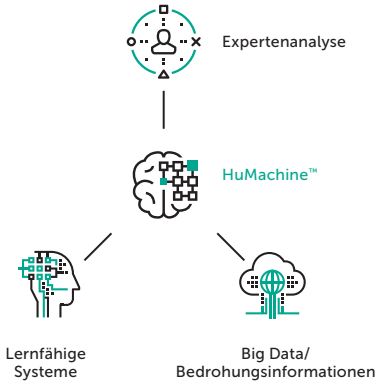
MS Windows-Betriebssysteme

- Windows 10 (RS1), 8.1, 8, 7, XP SP3
- Windows Server 2016, 2012 R2, 2012 (Voll- und Server-Core-Modus)
- Windows Server 2008 R2, 2008, 2003 R2 (Voll- und Server-Core-Modus)

Linux-Betriebssysteme

- Debian GNU/Linux 8.5
- Ubuntu Server 16.04 LTS, 14.04 LTS
- CentOS 7.2, 6.8
- RHEL 7.2, 6.7
- SUSE LES 12 SP1

Weitere Informationen zu den Sicherheitsmerkmalen von Kaspersky Security for Virtualization Version 4.0 finden Sie unter www.kaspersky.com/enterprise.



Kaspersky Lab
Cybersicherheit für Unternehmen: **www.kaspersky.de/enterprise**
Neues über Cyberbedrohungen: **www.viruslist.de**
IT-Sicherheitsnachrichten: **https://www.kaspersky.de/blog/b2b/**

#truecybersecurity
#HuMachine

www.kaspersky.de