

Segurança para centrais de dados

KASPERSKY SECURITY FOR VIRTUALIZATION 4.0

Novos recursos — para proporcionar ainda mais segurança, eficiência e velocidade

Cada vez mais empresas estão explorando os benefícios das centrais de dados baseadas no software; por isso, nunca foi tão necessário ter uma proteção excelente sem comprometer a produtividade.

E é exatamente isso que o Kaspersky Security for Virtualization oferece — ótima proteção multicamadas, granular e eficiente para infraestruturas de áreas de trabalho virtuais (VDIs, Virtual Desktop Infrastructures) e ambientes de servidores virtuais, aprimorada com a forte integração com as plataformas e tecnologias de virtualização mais conhecidas — como VMware vSphere com NSX, Microsoft Hyper-V, Citrix XenServer e KVM, além do VMware Horizon e Citrix XenDesktop.

E, agora, com o Kaspersky Security for Virtualization versão 4.0, redefinimos a forma de interação entre a central de dados baseada no software e sua solução de segurança, que têm autonomia para ser ainda mais inteligentes, rápidas e eficientes.

Estes são alguns dos novos recursos disponíveis na versão 4.0:

Integração nativa sem agentes com o VMware NSX *****EXCELENTE NOVIDADE*****

ANTIMALWARE SEM AGENTES

A proteção antimalware baseada em nosso premiado mecanismo é disponibilizada imediatamente para todas as máquinas virtuais (VMs, Virtual Machines) gerenciadas pelo VMware NSX, sem a necessidade de instalar agentes nos computadores.

BLOQUEIO DE ATAQUES DE REDE

As funcionalidades de detecção e prevenção de invasões (IDS/IPS) também são fornecidas para os hosts virtuais gerenciados pela plataforma VMware NSX, ajudando na proteção de sua infraestrutura virtualizada contra as ameaças de rede mais avançadas e as vulnerabilidades de dia zero.

IMPLEMENTAÇÃO AUTOMATIZADA

A forte integração com o VMware NSX possibilita a implementação totalmente automatizada de dispositivos de segurança (máquina virtual de segurança ou bloqueio de ataque de rede). Eles são exibidos no hipervisor automaticamente, de acordo com as políticas de segurança aplicadas a cada VM.

POLÍTICAS DE SEGURANÇA

A forte integração com o VMware NSX também faz com que cada VM tenha acesso a funcionalidades de segurança individuais e granulares. Esse recurso dá suporte total à criação e ao dimensionamento de centrais de dados baseada no software perfeitamente balanceadas.

MARCAS DE SEGURANÇA

O Kaspersky Security for Virtualization e a plataforma VMware NSX agora conseguem trocar marcas de segurança que, por sua vez, são alteradas com base em regras específicas (por exemplo, a detecção de malware em uma VM). Essa interação contínua entre a infraestrutura e sua segurança permite que a central de dados baseada no software responda em tempo real a qualquer incidente de segurança. Se necessário, a reconfiguração de toda a infraestrutura virtual é iniciada automaticamente.



Verificação de toda a infraestrutura no modo sem agentes *****EXCELENTE NOVIDADE*****

VERIFICAÇÃO POR DEMANDA DE MÁQUINAS VIRTUAIS LIGADAS E DESLIGADAS

Nenhuma solução 'tradicional' é capaz de fazer a verificação antimalware sem agentes de uma VM off-line. A nova versão do Kaspersky Security for Virtualization apresenta funcionalidades avançadas que verificam todas as VMs, tanto on-line quanto off-line. O resultado é a verificação por demanda mais eficiente e uma cobertura de segurança maior de toda a infraestrutura.

Agentes leves para servidores Linux *****EXCELENTE NOVIDADE*****

PROTEÇÃO DE SERVIDORES WINDOWS E LINUX COM O AGENTE LEVE

O Kaspersky Security for Virtualization Light Agent é a solução perfeita para centrais de dados híbridas, pois fornece funcionalidades avançadas de segurança para qualquer servidor virtual, independente do sistema operacional executado nele. As plataformas Linux compatíveis incluem:

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

Agente leve para virtualização baseada no RHEL

SUORTE PARA O KVM BASEADO NO SISTEMA OPERACIONAL RHEL

Continuamos ampliando nossa lista de plataformas de virtualização compatíveis, com a inclusão do suporte para o KVM baseado no sistema operacional RHEL Server (Red Hat Enterprise Linux Server).

Suporte para mais soluções da Microsoft

WINDOWS SERVER 2016

O Kaspersky Security for Virtualization Light Agent e Agentless agora possibilita o uso das funcionalidades de segurança mais avançadas do Microsoft Windows Server 2016 para proporcionar uma flexibilidade ainda maior.

WINDOWS 10 RED STONE 1 (RS1)

O Kaspersky Security for Virtualization Light Agent e Agentless dá suporte ao Windows 10, que já é comum em ambientes de VDI. Estamos incluindo também o suporte ao Windows 10 Red Stone 1 (RS1).

MODO COMPLETO E MODO SERVER CORE

O Kaspersky Security for Virtualization versão 4.0 Light Agent e Agentless dá suporte ao sistema operacional Windows Server tanto no modo completo quanto no modo Server Core. Isso é especialmente importante agora que as empresas estão implementando cada vez mais servidores de infraestrutura essencial sem interface do usuário no modo Server Core (por exemplo, controladores de domínio, DHCP, DNS).

WINDOWS HYPER-V 2016

O Kaspersky Security for Virtualization Light Agent também dá suporte à mais recente plataforma de virtualização da Microsoft, o Hyper-V 2016, permitindo que as empresas protejam centrais de dados baseadas no software com o nosso premiado antimalware e nossas funcionalidades de proteção de redes.

IMPLEMENTAÇÃO DO SYSTEM CENTER VIRTUAL MACHINE MANAGER (SCVMM)

Agora, o Kaspersky Security for Virtualization Light Agent pode ser implementado simultaneamente em vários hosts Microsoft Windows Hyper-V via SCVMM.

Agente leve no modo silencioso

DESATIVAÇÃO DA INTERFACE DO USUÁRIO DO AGENTE LEVE

Agora é possível desativar a interface do usuário do Kaspersky Security for Virtualization Light Agent (descarregando-a) em qualquer VM da central de dados baseada no software. Isso pode ser uma vantagem, por exemplo, no caso da virtualização de áreas de trabalho no sistema operacional Windows Server quando a Área de Trabalho Remota ou os Serviços de Terminal estão ativados, ou da virtualização de aplicativos com base no Citrix XenApp.

Servidor de Integração aprimorado

VÁRIOS SERVIDORES VMWARE VCENTER EM UM SERVIDOR DE INTEGRAÇÃO

O Servidor de Integração dedicado do Kaspersky Security for Virtualization pode ser conectado a vários servidores VMware vCenter para obter mais informações de sua infraestrutura virtual baseada no VMware.

Monitoramento automático das máquinas virtuais de segurança (SVMs, Security Virtual Machines)

AGENTE SNMP AVANÇADO NO SVM

É possível instalar o Kaspersky Security for Virtualization usando um agente SNMP. Ele monitora e envia informações abrangentes sobre o "status de integridade" do SVM para ferramentas de monitoramento SNMP de terceiros, como o Zabbix e o Nagios. Os contadores SNMP incluem métricas gerais das SVMs (CPU, RAM, etc.), além de métricas específicas.

Outros aprimoramentos

GERENCIAMENTO DE EXCEÇÕES OU IMPOSIÇÃO

O Kaspersky Security for Virtualization Light Agent agora oferece uma lista mais ampla de aplicativos de vários fornecedores de software que podem ser usados para especificar exceções ou configurar uma política de verificação obrigatória.

INSTALAÇÃO UNIFICADA DO PLUG-IN E DO SERVIDOR DE INTEGRAÇÃO

Agora temos um procedimento unificado para instalar o plug-in de administração e o Servidor de Integração do Kaspersky Security for Virtualization. O plug-in e o Console de Gerenciamento do Servidor de Integração são instalados e configurados pelos Assistente de Instalação de Componentes de Gerenciamento da Segurança da Kaspersky. Também é possível iniciar a instalação pela linha de comando.

CONTINUIDADE DO SUPORTE À API DO VSHIELD ENDPOINT

Várias empresas estão migrando ou planejando migrar para o VMware NSX. Porém, muitas ainda usam a tecnologia anterior, o vShield Endpoint. O Security for Virtualization Agentless versão 4 é totalmente compatível com o vShield Endpoint, e temos o compromisso de continuar com o suporte a essa tecnologia pelo tempo necessário para todos os nossos clientes. Assim, considerando a perspectiva da segurança, você pode fazer essa transição de modo tranquilo e flexível, em seu ritmo.

Kaspersky Security for Virtualization versão 4.0 — ainda mais proteção, eficiência e velocidade.

Plataformas compatíveis:



vCenter Server NSX
6.2.4* vSphere 6.5**
vSphere 6.0 vSphere 5.5
vSphere 5.1 **



MS SCVMM 2016**
MS SCVMM 2012 R2**
Hyper-V 2016**
(completo + server core)
Hyper-V 2012 R2**
(completo + server core)



XenServer 6.5 SP1**
XenServer 7.0**



CentOS 7.2**
Ubuntu Server 14.04
LTS**
RHEL Server 7u1**

SISTEMAS OPERACIONAIS DE SERVIDOR:

Windows Server 2016
(completo + server core)
Windows Server 2012 R2
(completo + server core)
Windows Server 2012
(completo + server core)
Windows Server 2008 R2
(completo + server core)
Windows Server 2008**
(completo + server core)
Windows Server 2003 R2*
Debian 8.5
Ubuntu Server 14.04, 16.04 LTS**
CentOS 6.8, 7.2**
RHEL Server 6.7, 7.2**
SUSE LES 12 SP1**

SISTEMAS OPERACIONAIS DE ÁREA DE TRABALHO:

Windows 10 (inclusive RS1)
Windows 8.1
Windows 8*
Windows 7
Windows XP SP3 (32 bits)*

PLATAFORMAS DE VDI:

Citrix XenDesktop 7.9, 7.11**
Citrix Provisioning Services 7.9, 7.11**
VMware Horizon View 7**

* Com suporte apenas na solução KSV Agentless

** Com suporte apenas na solução KSV Light Agent

SAIBA MAIS EM:

kaspersky.com/enterprise

ENCONTRE UM PARCEIRO PERTO DE VOCÊ EM:

kaspersky.com/partners