Kaspersky® Security for Virtualization

Kaspersky Security for Virtualization 4.0 New features for even greater protection

With more businesses exploiting the benefits of software-defined data centers, the need for outstanding protection without compromising on productivity has never been greater. And now, with Kaspersky Security for Virtualization version 4.0, we redefine how your software-defined data center and its security solution interact, empowering one another to become even smarter, faster and more efficient.

Top 5

- VMware vSphere 6.5 support
- VMware NSX 6.2 & 6.3 support
- Windows 10 (including RS1) support
- Linux Server OS support
- Full Infrastructure Scanning

Native Agentless Integration with VMware NSX 6.2 & 6.3

Agentless anti-malware

Anti-malware protection based on our award-winning engine is delivered instantly to every VM (Virtual Machine) managed by VMware NSX, with no need to install any agent on the machine.

Network attack blocking

Intrusion Detection and Prevention (IDS/IPS) capabilities are also delivered to virtual hosts managed by the VMware NSX platform, helping you protect your virtualized infrastructure from the most advanced network-based threats and zero-day vulnerabilities.

Automated deployment

Tight VMware NSX integration enables the fully automated deployment of security appliances (Security Virtual Machine or Network Attack Blocker). These 'pop up' on the hypervisor automatically, based on the security polices applied to each VM.

Security policies

This tight integration with VMware NSX also means that each VM now receives precise, granular individual security capabilities. This feature fully supports the building and scaling of perfectly balanced software-defined data centers.

Security tags

vmware PARTNER TECHNOLOGY ALLIANCE

vmware READY NETWORKING AND SECURITY

Kaspersky Security for Virtualization and the VMware NSX platform now exchange security tags, which can change based on specific rules (e.g. malware detected inside a VM). This constant interaction between the infrastructure and its security means that the software-defined data center can react in real time to any security incident, automatically kicking off the reconfiguration of whole virtual infrastructure if necessary.

Product Architecture Improvements

Agentless Scanning for Powered-OFF VMs

On-demand scanning of powered-on and powered-off virtual machines. No 'traditional' solution can perform an agentless anti-malware scan of a VM that's offline. The new release of Kaspersky Security for Virtualization introduces advanced functionality which scans all VMs, whether they are on- or offline. The result is more effective on-demand scanning and better security coverage right across your entire infrastructure.

vShield Endpoint API Still Supported

Many businesses are migrating, or planning to migrate, to VMware NSX. But many are still using the previous technology – vShield Endpoint. Security for Virtualization Agentless version 4 fully supports vShield Endpoint, and we are absolutely committed to continuing to support this technology for as long as required by any of our customers. So, from a security perspective, you can transition smoothly and flexibly, at your own pace.

Agentless and Light Agent for Linux OS

We protect both Windows and Linux servers with Kaspersky Security for Virtualization. Moreover, now we do that in both Agentless and Light Agent modes. Kaspersky Security for Virtualization is truly a perfectly engineered cybersecurity solution for hybrid data centers that delivers advanced security capabilities to any virtual server regardless of the operating system running inside it.

KSV Agentless supports:

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

KSV Light Agent supports:

- 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 for KVM on RHEL

We continue to extend our list of supported virtualization platforms. A new version of Kaspersky Security for Virtualization Light Agent supports KVM hypervisor based on the RHEL Server (Red Hat Enterprise Linux Server) OS.

Light Agent in Silent Mode

The Kaspersky Security for Virtualization Light Agent UI can now be disabled (by offloading it) on any VM across the software-defined data center. This can be of benefit with, for example, desktop virtualization on Windows Server OS when Remote Desktop or Terminal Services are enabled, or for application virtualization based on Citrix XenApp.

Single KSV Integration Server for Multiple vCenter Servers

Kaspersky Security for Virtualization's dedicated Integration Server can be connected to several VMware vCenter Servers, obtaining more information from your VMware based virtual infrastructure.

Advanced SNMP-Agent on SVM

Kaspersky Security for Virtualization can be installed with an SNMP-agent. This monitors and sends extensive information about the SVM's "Health Status" to 3rd-party SNMP monitoring tools like Zabbix and Nagios. SNMP counters include general SVM metrics (CPU, RAM, etc.), as well as specific metrics.

Exceptions or Enforcement Management

Kaspersky Security for Virtualization Light Agent now offers a wider list of applications from different software vendors for use when specifying exceptions or configuring an enforced scanning policy.

Unified Installation of Plug-in and Integration Server

There is now a single unified procedure for installing the Kaspersky Security for Virtualization administration plug-in and Integration Server. The plug-in and the Integration Server Management Console are installed and configured using the Installation Wizard for Kaspersky Security Management Components. You can also start installation from the command line.

Supporting More From Microsoft

Windows Server 2016

Kaspersky Security for Virtualization Light Agent and Agentless both, now enable the most advanced security capabilities of Microsoft Windows Server 2016, for even more flexibility.

Windows 10 Red Stone 1 (RS1)

Kaspersky Security for Virtualization Light Agent and Agentless already support Windows 10, which is popular in VDI environments. We are now adding support for Windows 10 Red Stone 1 (RS1).

Full Mode and Server Core Mode

Kaspersky Security for Virtualization version 4.0 Light Agent and Agentless support Windows Server operating systems running both in Full and in Server Core mode. This is particularly important now that businesses are deploying more and more critical infrastructure servers with no user interface in Server Core mode (e.g., Domain Controllers, DHCP, DNS).

Windows Hyper-V 2016

Kaspersky Security for Virtualization Light Agent also supports Microsoft's latest virtualization platform, allowing businesses to secure their Hyper-V 2016 based software-defined data centers using our award-winning anti-malware and network protection capabilities.

Deployment via SCVMM

Now, Kaspersky Security for Virtualization Light Agent can be deployed simultaneously onto a number of Microsoft Windows Hyper-V hosts via the System Center Virtual Machine Manager (SCVMM).

Full List of Supported platforms and OS

VMware virtualization

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

Microsoft virtualization

- MS Windows Server 2016 Hyper-V
- MS Windows Server 2012 R2 Hyper-V
- Deployment via SCVMM 2016, 2012 R2

Citrix virtualization

- Citrix XenServer 7.0, 6.5 SP1

KVM virtualization

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

VDI platforms

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

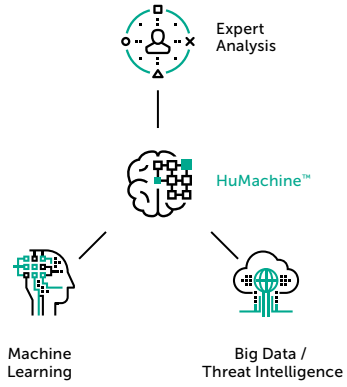
MS Windows OS

- Windows 10 (RS1), 8.1, 8, 7, XP SP3
- Windows Server 2016, 2012 R2, 2012 (Full or Server Core modes)
- Windows Server 2008 R2, 2008, 2003 R2 (Full or Server Core modes)

Linux OS

- 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

To learn more about security capabilities of Kaspersky Security for Virtualization version 4.0, please visit www.kaspersky.com/enterprise.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com