KASPERSKY SECURITY FOR VIRTUALIZATION

Superior, flexible and efficient protection for virtual server and desktop environments

HIGHLIGHTS

OUTSTANDING PROTECTION

- Supports VMware, Microsoft Hyper-V* and Citrix Xen* platforms and core technologies.
- Powerful, multi-layered anti-malware, including Automatic Exploit Prevention.
- Integration with the cloud-based Kaspersky Security Network (KSN) proactively defends against emerging global threats.
- Application controls (incorporating dynamic whitelisting) plus web and device controls allow the administrator to enforce policies, keeping users safe and productive.
- A powerful combination of network attack blocker, firewall, Host-based Intrusion Prevention (HIPS) and anti-phishing technologies protect VMs from network threats.
- VMs are instantly and automatically protected by a Security Virtual Appliance (SVA) which is continuously updated.

BETTER PERFORMANCE

- Innovative design ensures a light resource footprint, optimising consolidation ratios for maximum density.
- Shared cache technology eliminates duplication of scanning effort.
- Anti-virus update and scanning ‘storms’ as well as ‘instant-on’ gaps are eliminated.

GREATER EFFICIENCY

- Fast, straightforward deployment to new VMs, with no reboot or maintenance mode required.
- A single console allows physical, mobile and virtual endpoints to be managed together.
- Simplified administration and deployment delivers greater efficiency and less opportunity for configuration error.

OUTSTANDING FLEXIBILITY

- Citrix, Microsoft and VMware platform security are all included in a single cost.
- Flexible licensing — choose from licensing based on number of machines (desktops or servers) or resources (number of cores).

KASPERSKY SECURITY FOR VIRTUALIZATION IS A FLEXIBLE SOLUTION WHICH DELIVERS BOTH PROTECTION AND PERFORMANCE FOR YOUR ENVIRONMENT.

KEY PRODUCT FEATURES

- Centralized management via Kaspersky Security Center
- Centralized SVA based VM protection
- Advanced threat protection including Automatic Exploit Prevention
- Virtual network protection including HIPS, firewall and Network Attack Blocker
- Endpoint controls for applications, web access and peripherals
- Cloud-assisted security via Kaspersky Security Network
- Antivirus and anti-phishing for IM, mail and Internet traffic
- No additional installation or reboots for new VMs*

SECURITY VIRTUAL APPLIANCE (SVA) AND LIGHTWEIGHT AGENT

Kaspersky Lab's Security Virtual Appliance (SVA) centrally scans all VMs in the host environment. This architecture provides efficient VM protection without sacrificing endpoint resources, resulting in greater consolidation ratios than are achievable using traditional antivirus solutions. AV scanning and update storms are eliminated, together with 'instant-on' gaps.

Kaspersky Security for Virtualization also includes a powerful but lightweight agent which is deployed on each virtual machine. This allows for the activation of advanced endpoint security features including vulnerability monitoring, application, device and web controls, anti-virus protection for instant messaging, mail and web, plus advanced heuristics. The result is powerful, multilayered security combined with efficient performance.

Kaspersky Security for Virtualization supports VMware, Microsoft Hyper-V and Citrix Xen platforms and their core technologies.

Optional agentless configuration for VMware environments

For VMware based internal environments where zero downtime with no reboots is a mandatory requirement, Kaspersky Security for Virtualization can be deployed in an agentless configuration. Please ask your reseller or Kaspersky Lab sales representative for more details.

* For non-persistent VMs, instant protection is available after the agent is executed on the VM image. For persistent VMs, the administrator must deploy the light agent during installation.

For more information about Kaspersky Security for Virtualization, contact your local Kaspersky partner or visit **www.kaspersky.com**

KSV/Version 3.1/April 14/Global

KASPERSKY lab