

# KASPERSKY SECURITY FOR VIRTUALIZATION

*Superior, flexible and efficient protection for virtual servers and VDI*

As businesses continue to roll out virtualized environments across more of their IT estate, there is an increasing need for security designed specifically for virtualization. But finding a solution which provides security capabilities both for your growing Virtual Desktop Infrastructure (VDI) and your virtual server environment, while retaining all the benefits of virtualization, is not easy.

Virtual and physical machines face the same security threats - cybercrime makes no distinctions. And as security breaches affecting a virtual infrastructure can be particularly costly, you cannot afford to compromise on security. Nor on performance.

Kaspersky Security for Virtualization delivers outstanding multi-layered, granular protection for VDI and virtual server environments. We do this in a way nobody else does, quite straightforwardly, without wasting resources or compromising performance, resulting in significantly higher consolidation ratios than are achievable with traditional anti-malware solutions. Kaspersky Security for Virtualization is a right balance between performance and protection.

## Highlights

### OUTSTANDING PROTECTION

- Real-time protection for all your VMs on leading platforms including VMware vSphere, Microsoft Hyper-V, KVM and Citrix XenServer.
- Enhanced functionality including application, web and device controls, keeping VDI users safe and business critical systems productive.
- Award-winning protection from sophisticated threats and vulnerabilities via Advanced Exploit Prevention (AEP) technology.
- Proactive defense against emerging threats through integration with the cloud-based Kaspersky Security Network (KSN).
- Powerful IDS/IPS recognizes and blocks known, unknown and advanced exploit-based threats.

### BETTER PERFORMANCE

- Our innovative patented design<sup>1</sup> ensures a very light resource footprint, optimizing consolidation ratios for maximum density.
- Security designed specifically for virtualization saves precious hypervisor resources.
- Lightweight yet powerful protection off-loads file scanning tasks and uses intelligent orchestration to preserve overall platform efficiency.
- Multi-layered protection for VMware Horizon and Citrix XenDesktop, with no adverse impact on VDI end-user experience or platform performance and responsiveness.



<sup>1</sup> US Patents N°9009836 and N°9088618

## GREATER EFFICIENCY

- File scanning tasks are off-loaded to a dedicated Security Virtual Appliance (SVA) per host. For deeper protection, deploying a Light Agent on each VM is straightforward, with no reboots.
- Update and scanning 'storms' and Windows of Vulnerability or 'instant-on' gaps are eliminated.
- A powerful combination of network attack blocker, application firewall, Host-based Intrusion Prevention (HIPS) and anti-phishing protects VMs from network threats.
- Support for VMware NSX and vCNS means the solution seamlessly follows infrastructure and network topology changes.

## SUPERIOR FLEXIBILITY & VISIBILITY

- Specifically designed to protect virtual servers and desktops, so your protection solution of choice also best fits your business needs.
- Flexible licensing options — based on the number of VMs (desktops or servers) or hardware resources (number of cores).
- A single console means physical and virtual machines and mobile devices can all be managed together.
- Feature-rich reporting and monitoring makes it easier to manage and supervise security within your organization.

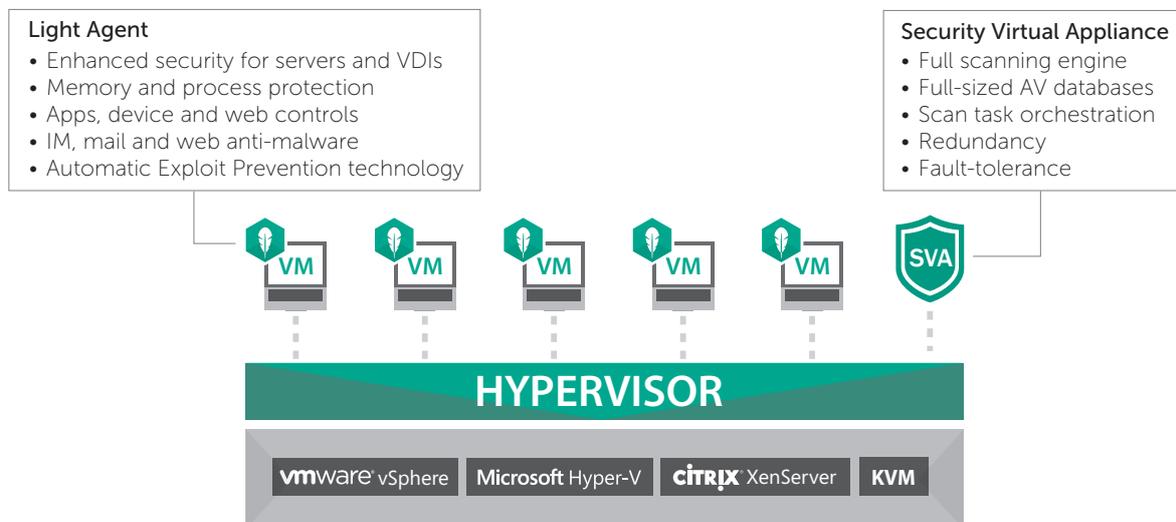
## Using an agentless approach

Kaspersky Security for Virtualization integrates with native VMware technologies like vShield Endpoint and NSX. With no additional agent required on each VM, systems impact on virtual platform performance is near-zero, administration is reduced, and each powered-on VM is protected instantaneously.

This approach is most appropriate for VMware based infrastructures simply requiring strong file-level security and network protection. For business-critical virtual servers and desktops, an agent on the VM delivers further advanced security capabilities.

## Unique Light Agent Technology

### HOW IT WORKS AND WHAT IT DOES



A Security Virtual Appliance (SVA) on each host scans all VMs centrally, while a powerful but lightweight agent deployed on each VM allows advanced security features, including application, device and web controls, anti-malware protection for IM, mail and web, plus advanced heuristics, to be activated.

Kaspersky Security for Virtualization is tightly integrated with most popular platforms - VMware vSphere, Microsoft Hyper-V, Citrix XenServer and KVM. Your business critical infrastructure benefits from optimized performance that fully exploits your hypervisor's own core technologies – complementing and enhancing security in, for example, VMware Horizon and Citrix XenDesktop VDI environments.

**Kaspersky Security for Virtualization Light Agent and Agentless. Two approaches in one solution, delivering powerful protection combined with efficient performance for your virtual environment.**

For more information about Kaspersky Security for Virtualization, visit [www.kaspersky.com/enterprise](http://www.kaspersky.com/enterprise)