A SINGLE SOLUTION FOR YOUR HYBRID DATA CENTER

Corporate data centers are increasingly becoming software-defined. Network interaction is moving from the physical to the virtual realm, opening up a new range of possible attack scenarios. You need a security solution designed to deliver optimum protection while preserving systems performance by harnessing the software-defined data center's own capabilities and infrastructure.

Kaspersky Security for Virtualization has been designed to protect software-defined data centers built on VMware vSphere®, including VMware NSX® for vSphere. Kaspersky Security for Virtualization delivers advanced security capabilities with almost zero impact on the efficiency of either compute or networking platform processes.

Infrastructure and Security Working in Harness

VMware and Kaspersky Lab together address cyber-security threats with a joint solution built upon the software-defined data center (SDDC), armed with advanced security capabilities to deliver high-level protection from internal or external threats.

Kaspersky Security for Virtualization has been designed specifically to protect enterprise-level infrastructure built on VMware vSphere technologies and the VMware NSX network virtualization platform. Customers benefit from an industry-leading* anti-malware solution while retaining high consolidation ratios.

BUILT-IN VMWARE NSX SERVICES	
Distributed Firewall	**Virtual Networks (VXLAN)**
Server Activity Monitoring	**VPN (IPSec, SSL L2VPN)**
KASPERSKY SECURITY FOR VIRTUALIZATION	
Anti-Malware	**Intrusion Prevention (IPS)**
Security Policies Integration	**Security Tags Integration**
Automated Deployment	**...Multi-Layered Security for Software-Defined Data Centers**

Kaspersky Security for Virtualization, interoperating with VMware vSphere and the NSX network virtualization platform means infrastructure and security layers work in harness, bringing new levels of automation and protection to software-defined data centers, regardless of size or complexity.

VMWARE NSX®

VMware NSX is the leading network virtualization platform that delivers the operational model of a virtual machine for the network.

KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization delivers permanent protection for VMware infrastructures through native integration with NSX:

- Agentless anti-malware security for VMware compute and networking platforms
- Virtual network IDS/IPS fight against network threats
- Continuous protection even for powered-off VMs
- Enterprise level manageability and flexibility
- Retains full systems efficiency and performance

Whether you are running a public or private virtualized infrastructure, or a combination, you can increase your efficiency and security by utilizing VMware NSX interoperating with Kaspersky Security for Virtualization.

KASPERSKY LAB

Kaspersky Lab is a global cybersecurity company founded in 1997. Kaspersky Lab's deep threat intelligence and security expertise is constantly transforming into security solutions and services to protect businesses, critical infrastructure, governments and consumers around the globe. The company's comprehensive security portfolio includes leading endpoint protection and a number of specialized security solutions and services to fight sophisticated and evolving digital threats. Over 400 million users are protected by Kaspersky Lab technologies. They help 270,000 corporate clients protect what matters most to them.

FITS ANY ENTERPRISE

Integrated solution makes sure that ROI of your virtualization projects remains on high levels.

- Improved operations through the automated deployment of security appliances
- Granular security capabilities delivered fast through security policies and security tags.
- Protective scanning even for powered-off VMs, thanks to the Full Infrastructure Scanning option.

See this solution in the VMware Solution Exchange.

www.solutionexchange.vmware.com/store/companies/kaspersky-lab

Kaspersky Security for Virtualization – Complementing VMware NSX Security

- Infrastructure and security layers work together, allowing for new levels of automation for corporate software-defined data centers.
- Automated deployment for VMware NSX allows Kaspersky Lab's Security Virtual Machine (SVM) to 'pop up' automatically on the hypervisor.
- Security policy alignment means each VM receives precise security capabilities, as defined by corporate policies based on the VM's role.
- Integration with NSX Security Tags allows your software-defined data center to react in real time to security incidents, automatically reconfiguring the virtual infrastructure as necessary.

Automated Security and Monitoring

- Full infrastructure scanning protects all VMs, whether they are online or offline, for even better security coverage right across your IT estate.
- Routine scanning of all VMs can be pre-scheduled at a granular level, so security tasks can be orchestrated according to your needs.
- Self-protection and advanced SNMP-based monitoring guarantees that the solution is always available, and able to provide detailed information for extra control.
- Native support for VMware vCenter Server® as well as NSX Manager means the security layer is always aware of any infrastructure changes.

The Right Balance of Protection and Performance

- Award-winning anti-malware protection* engineered for virtualization allows the offloading of file-scanning tasks from VMs onto a dedicated SVM for greater efficiency.
- Virtual Network Intrusion Detection and Prevention (IDS/IPS) works in agentless mode, shielding your entire virtualized infrastructure from network-based threats.
- Cache based optimization ensures that recently scanned files are not re-scanned during routine scanning.
- Security solution designed to scan both powered-on and powered-off virtual machines utilizing resource efficient approach.

Superior Reliability and Manageability

- A single unified management console for virtual, physical and mobile devices means you can enforce consistent security policies across your entire IT estate.
- Deployment with no downtime allows installing security solution without a need to reboot any VMs or put the host server into maintenance mode.
- Intelligent scan task orchestration and automation eliminates any peaks in hypervisor resource consumption to preserve overall efficiency.
- Feature-rich reporting and monitoring makes it easier to manage and supervise security throughout the organization.

* www.usa.kaspersky.com/files/pdf/Kaspersky_Lab_TOP3_2016.pdf

"With Kaspersky Lab's security solution now natively working with our virtual environment, we can also easily offer automated protection for each virtual machine across the entire infrastructure. Security tags and policy-based operation allows us to deliver security capabilities in a faster and more efficient way."

LURIE TURCANU
CHIEF TECHNOLOGY OFFICER
E-GOVERNMENT CENTER OF
THE REPUBLIC OF MOLDOVA

LEARN MORE

To learn more about how Kaspersky Security for Virtualization and VMware NSX can provide superior protection for your software-defined data center, visit www.kaspersky.com/enterprise-security/virtualization or contact your Kaspersky Lab or VMware partner or sales representative.

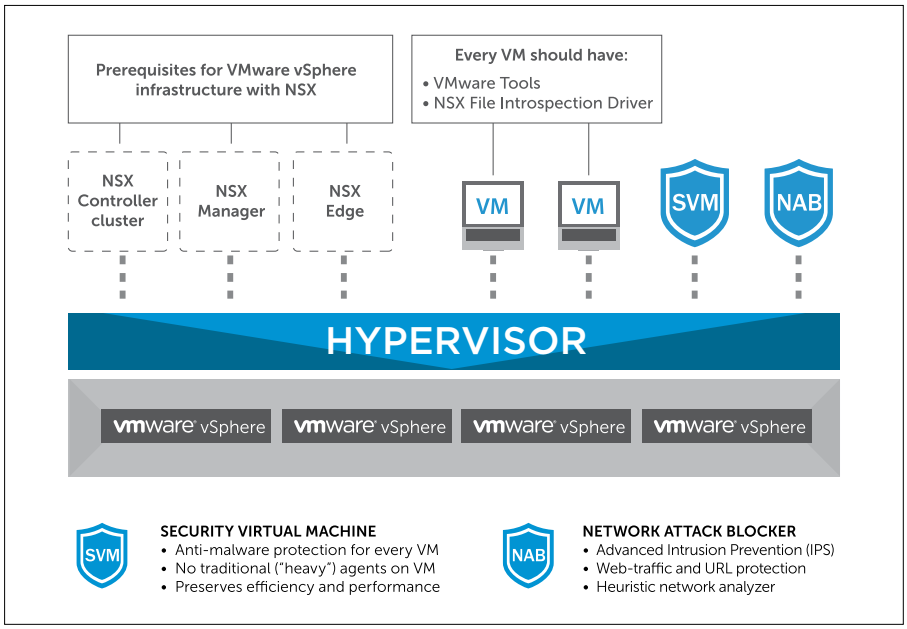
Technological Excellence

Kaspersky Security for Virtualization has been engineered specifically to work with virtualization platforms, while traditional security solutions consume too many resources. Technological benefits for servers include:

- **Security Automation** allowing bidirectional policy-based communications between the infrastructure and its security layer.
- **Full infrastructure scanning** of both powered-on and powered-off virtual machines in your software-defined data center.
- **Efficiency is conserved** by offloading all resource-intensive tasks to dedicated security appliances and leveraging security task orchestration.
- **No more 'update storms'** and **'scanning storms'**, or 'windows of vulnerabilities" as there are fewer databases to update.
- **Virtual network IDS/IPS** fights against network-based attacks.

How It Works

Just as server virtualization transforms physical nodes into virtualized pools of computing resources, the VMware NSX network virtualization platform transforms the data center network into a pool of network resources which can be created, changed, utilized and redistributed dynamically. Kaspersky Security for Virtualization interoperates with VMware NSX allowing for more efficient and secure operations. With no agent required on each VM, impact on virtual platform performance is near-zero, administrative tasks consume fewer resources, and all VMs within the infrastructure are protected instantaneously.



The joint solution delivers advanced security capabilities to every VM running on VMware vSphere infrastructure. While Kaspersky Lab's solution is focused on identifying and blocking known and unknown threats, resource efficiency of the infrastructure remains paramount.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com