Cloud Security

Kaspersky Security for Virtualization Integrated with VMware NSX platform

Data is your business's most important asset. So how and where that data is stored, processed and transmitted is critical not just to achieving a greater competitive advantage, but also to increasing operational efficiency and maintaining business continuity. There are many superior data processing, storage and networking solutions out there. But networking solutions in particular can be complex, inflexible and all too often tied to, and limited by, the hardware platform they're built on. This in turn impedes your data center's agility, and your ability to satisfy rapidly changing business requirements.

Traditional security solutions do not meet your private cloud needs

- Not elastic enough for your clouds
- Cannot inter-operate via native API
- Lack in providing full visibility on IT
- Cause 'update and scanning storms'
- Eat your private cloud resources

How You Benefit From Natively Integrated Agentless Security for VMware NSX:

- **Fully automated deployment** of SVM, a specialized security appliance, based on the security polices applied to each protected VM on the hypervisor host.
- **Integration with NSX Security Policies** allows each protected VM to receive precise, granular security capabilities to let you scale corporate software-defined data center with no borders.
- **Integration with NSX Security Tags** allows your software-defined data center detect and react to most advanced threats in real-time fashion, and even reconfigure the entire infrastructure if necessary.
- **Full infrastructure scanning** protects all VMs, whether they are on- or offline, for even better cybersecurity coverage right across your entire virtual infrastructure.
- **Proactive defense against cyberthreats** through use of the cloud-based Kaspersky Security Network.

vmware PARTNER TECHNOLOGY ALLIANCE

vmware READY NETWORKING AND SECURITY

VMware® and Kaspersky Lab together address these issues through a joint solution built around a highly efficient Software-Defined Data Center, armed with advanced security capabilities to ensure high-level protection from internal or external threats, allowing you to work with different pools of network resources, dynamically creating or reconfiguring your entire network topology in a matter of seconds, using a "zero trust" security approach.

Kaspersky Security for Virtualization Agentless has been specifically designed to protect private clouds built on VMware NSX for vSphere. This joint solution delivers advanced security capabilities to each VM within your private cloud with near-zero impact on systems efficiency.

Built-in VMware NSX Services	
Distributed Firewall	Virtual networks (VXLAN)
Server Activity Monitoring	VPN (IPSec, SSL L2VPN)

Kaspersky Security for Virtualization	
Agentless Anti-malware	Virtual Network IDS/IPS
Automated Deployment	Security Policies integration
Security Tags integration	Scans even powered-off VMs

Native interaction between your virtualization platform and its security solution means your private cloud can react in real time to any security incident across your entire infrastructure. Unified orchestration console lets your teams centrally manage the security of all your VMs, together with the Kaspersky Lab security products running on your physical servers, endpoints and even mobile devices, so it becomes easier for your team to manage entire hybrid cloud environment, with less pressure on IT resources, and less scope for human error.

A perfectly balanced combination, so you can implement, orchestrate and scale security regardless of the size and complexity of your private cloud.

Preserves the private cloud ROI

Because Kaspersky Security for Virtualization has been specifically developed to protect virtual machines (VMs), it helps businesses maintain a high machine density and high perfomance – preserving your virtualization ROI while eliminating update and scanning 'storms', together with Windows of Vulnerability or 'instant-on' gaps.

Designed For Any Virtualizations

Kaspersky Security for Virtualization is more than just 'designed for' virtualization platforms: it utilizes the core technologies of those platforms to optimize the security capabilities of both platform and security solution.

From now on, your infrastructure and its security solution work in harness for maximum effectiveness.

Shields Entire Virtual Network

Kaspersky's Network Attack Blocker monitors network traffic for signs of activity typical of network attacks.

Kaspersky Security for Virtualization Agentless provides this network-level functionality together with support for both VMware vCloud Networking and Security and VMware NSX platforms.

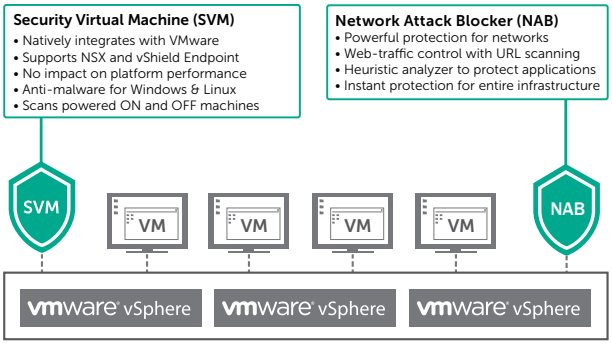
For Windows and Linux VMs

Kaspersky Security for Virtualization is truly a perfectly engineered solution for hybrid data centers that delivers advanced security capabilities to any virtual server regardless of the operating system running inside it.

We protect both Windows and Linux servers, including RHEL 7GA, SLES 12 GA and Ubuntu 14.04 LTS.

Specifically Designed for VMware NSX Security

- Interoperability with VMware NSX lets infrastructure and security layers work together in close co-operation, bringing new levels of automation and protection.
- Automated deployment for VMware NSX allows the SVM (Security Virtual Machine) to 'pop up' automatically on the hypervisor, based on the requirements of the protected VMs sitting on that host.
- Security Policy integration means each VM receives precise security capabilities, as defined by your corporate policies based on the VM's individual role.
- Integration with NSX Security Tags allows your private cloud to react in real-time to security incidents, automatically reconfiguring the entire infrastructure if necessary.



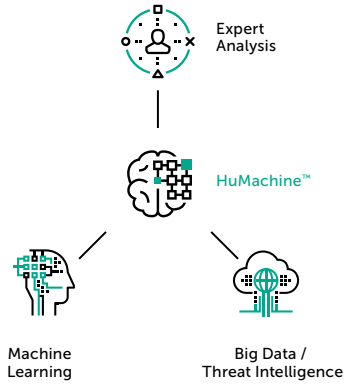
Automated Security and Monitoring

- Full infrastructure scanning protects all VMs, whether they are on- or offline, for even better security coverage right across your infrastructure.
- 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 guaranties that SVMs are always up and running, and able provide extensive information to 3rd-party monitoring tools for extra control.
- Advanced protection will be never interrupted, even if a workload is moved through the cloud – VMware vMotion and Disaster Recovery's own capabilities are fully supported.

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 – no 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 platform efficiency.
- Feature-rich reporting and monitoring makes it easier to manage and supervise security throughout your organization.

The result is a powerful, elastic and fully secure private cloud environment. Learn more at 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