Kaspersky®
Security
for Virtualization

Superior, flexible and resource-efficient protection for virtual servers and VDI

With more businesses exploiting the benefits of software-defined data centers, the need for outstanding protection without compromising on productivity has never been greater.

This is exactly what Kaspersky Security for Virtualization delivers – outstanding multi-layered, granular and powerful protection for VDI and virtual servers and environments – enhanced by tight integration with the most popular virtualization platforms and technologies, including VMware vSphere with NSX, Microsoft Hyper-V, Citrix XenServer and KVM, as well as VMware Horizon and Citrix XenDesktop.
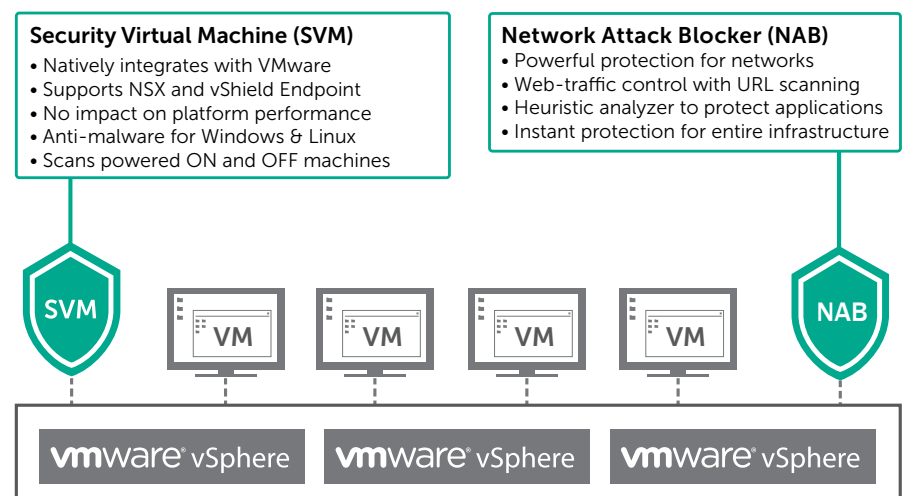
With Kaspersky Security for Virtualization featuring agentless and lightweight security options, we redefine how your software-defined data center and its security solution interact, empowering one another to become even smarter, faster and more efficient.

How You Benefit From Natively Integrated Agentless Security:

- **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.

Agentless security for VMware NSX

Kaspersky Security for Virtualization Agentless natively integrates with VMware NSX. With no additional agent required on each VM, thrimpact on virtual platform performance is near-zero, administrative tasks consume fewer resources, and all VMs across your entire infrastructure are protected instantaneously.

Security Virtual Machine (SVM)
- Natively integrates with VMware
- Supports NSX and vShield Endpoint
- No impact on platform performance
- Anti-malware for Windows & Linux
- Scans powered ON and OFF machines

Network Attack Blocker (NAB)
- Powerful protection for networks
- Web-traffic control with URL scanning
- Heuristic analyzer to protect applications
- Instant protection for entire infrastructure

Kaspersky Security for Virtualization Agentless not only delivers anti-malware protection, but also shields your entire infrastructure from network based attacks by leveraging a dedicated virtual network IDS/IPS (Network Attack Blocker, NAB).

More security layers with Light Agent

Kaspersky Security for Virtualization Light Agent provides a single solution to secure both virtual servers and VDI. Because it supports most popular platforms – including VMware vSphere, Citrix XenServer, Microsoft Hyper-V and KVM – the solution is ideal for hybrid software-defined data centers. A powerful but lightweight security agent supports industry-leading VDI platforms such as Citrix XenDesktop and VMware Horizon and significantly boosts protection while preserving the performance of each VM.

Light Agent
- Enhanced security for servers and VDI
- Memory and Processes protection
- Apps, Device, Web and Mail control
- Exploit Prevention & Anti-ransomware
- For Windows and Linux servers

Security Virtual Machine (SVM)
- Full scanning engine
- Complete full-sizes AV databases
- Scan task orchestration
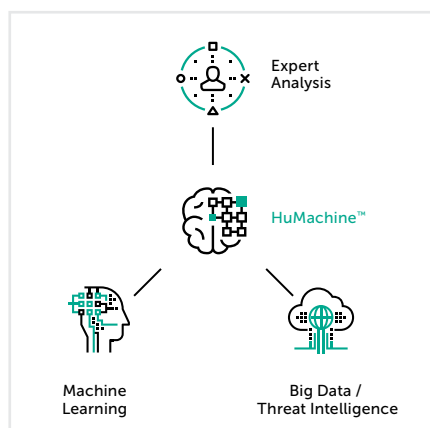- Redundancy and fault-tolerance
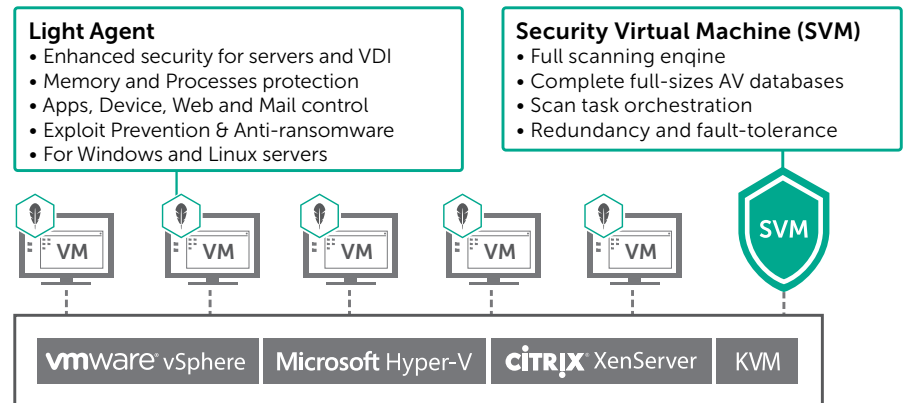
A Security Virtual Machine (SVM) on each host scans all VMs centrally, while a powerful but lightweight agent deployed onto each VM allows advanced security features, including application, device and web controls, anti-malware protection for mail and web traffic, plus advanced heuristics, to be activated. Peaks in resource consumption are reduced via Intelligent Scan Task Orchestration, automating queues by grouping and prioritizing scan tasks on multiple protected VMs.

- **System Watcher** technology leverages behavior stream signatures to preserve the consistency of every VDI and protect from crypto-lockers and ransomware.

- **Application Startup and Privilege Control**, including Default Deny, controls user activity so only trusted applications can launch on a protected VM.

- **Network Attack Blocker empowered with Host-Based Intrusion Prevention System**, protects the virtualized environment from network-based attacks.

- **URL protection** shields every VM from malware and malicious Internet resources that might do harm or don't meet corporate security policies.

- **Mail and Web-traffic protection** ensures that all communication within your corporate environment flows safely, rather than acting as a conduit for malware.

- **Device Control** guarantees secure access to virtualized devices that are connected to a virtual desktop.

Whatever virtualized platform or platforms you use, Kaspersky Security for Virtualization, with its perfectly engineered technologies and unique architecture, provides greater security capabilities. VMware vSphere with NSX, Microsoft Hyper-V, Citrix XenServer, and KVM are all supported in a single security solution. Regardless of your platform configuration and hybridization, on-premise or off-premise, all security management is through one unified console, and full systems efficiency is retained.

Kaspersky Security for Virtualization Light Agent and Agentless. Two security approaches in one solution, both delivering outstanding protection powered by Kaspersky Lab's unique HuMachine Intelligence.