KASPERSKY lab

LIGHT AGENT OR AGENTLESS

A Features Guide to Kaspersky Security for Virtualization

www.kaspersky.com

With virtualization becoming ever more widespread, the need for adequate security solutions is self-evident. Although just as susceptible to cyber-attack as any physical system, virtual environments present unique features which need consideration when assessing different security solutions.

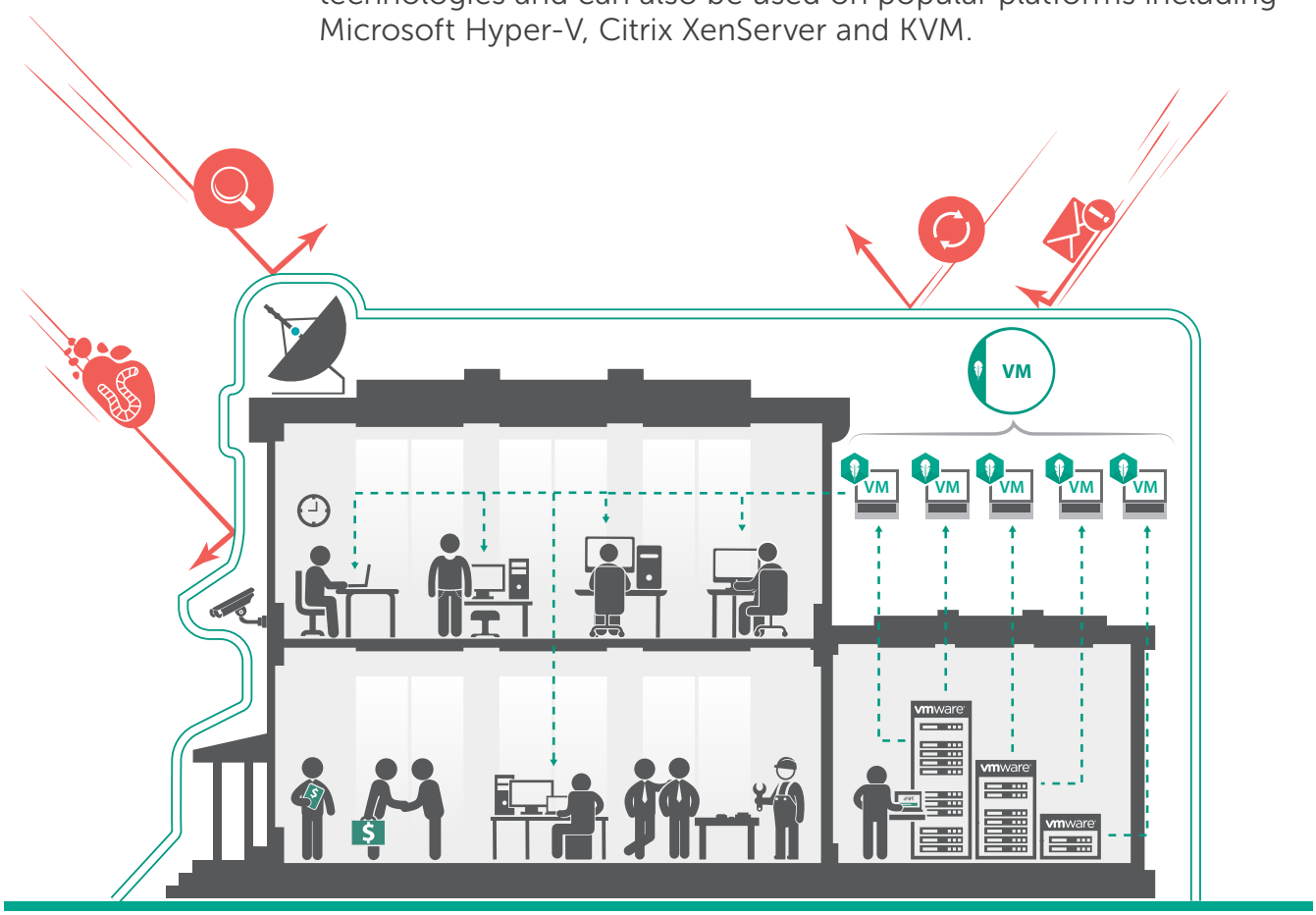
Businesses can use the same security software to protect both their physical and virtual machines. But while providing a good level of protection, standard solutions which are not designed specifically for virtual environments can cause problems, including:

1. **Excessive resource consumption** due to the replication of signature databases and active anti-malware engines on each protected Virtual Machine (VM).
2. **"Storms"**– simultaneous database updates and/or anti-malware scanning processes on each VM, leading to an avalanche-like increase in resource consumption, causing drastic loss of performance and even denial of service. Attempts to mitigate the problem by scheduling these processes generates "vulnerability windows" – time periods when postponed malware scans leave the VM vulnerable to attack.
3. **"Instant-on gaps".** Signature databases cannot be updated on inactive VMs. So from machine startup until the update process completes, the VM is vulnerable to attack.
4. **Incompatibilities.** Because standard solutions are not built to handle virtualization-specific features, like migrating VMs or non-persistent storage, their use can cause instabilities and even system lockups.

Recognizing the importance of virtual systems security, and the unique features virtualization presents, market leader VMware developed vShield endpoint technology, a specific defensive layer for its vSphere virtualization platform. This layer creates an integrated security space for third-party solutions, natively integrated with VMware APIs such as vShield Endpoint and NSX Guest Introspection, enveloping all virtualized assets and allowing easy and efficient access by appropriately designed security solutions. Only one Security Virtual Appliance (SVA) – a specialized virtual machine carrying an anti-malware scanning engine and signature databases – is needed per host, removing this burden from individual VMs and so greatly reducing resource consumption. The biggest benefit of this approach for Enterprise businesses is smooth and native integration with the

VMware ecosystem.

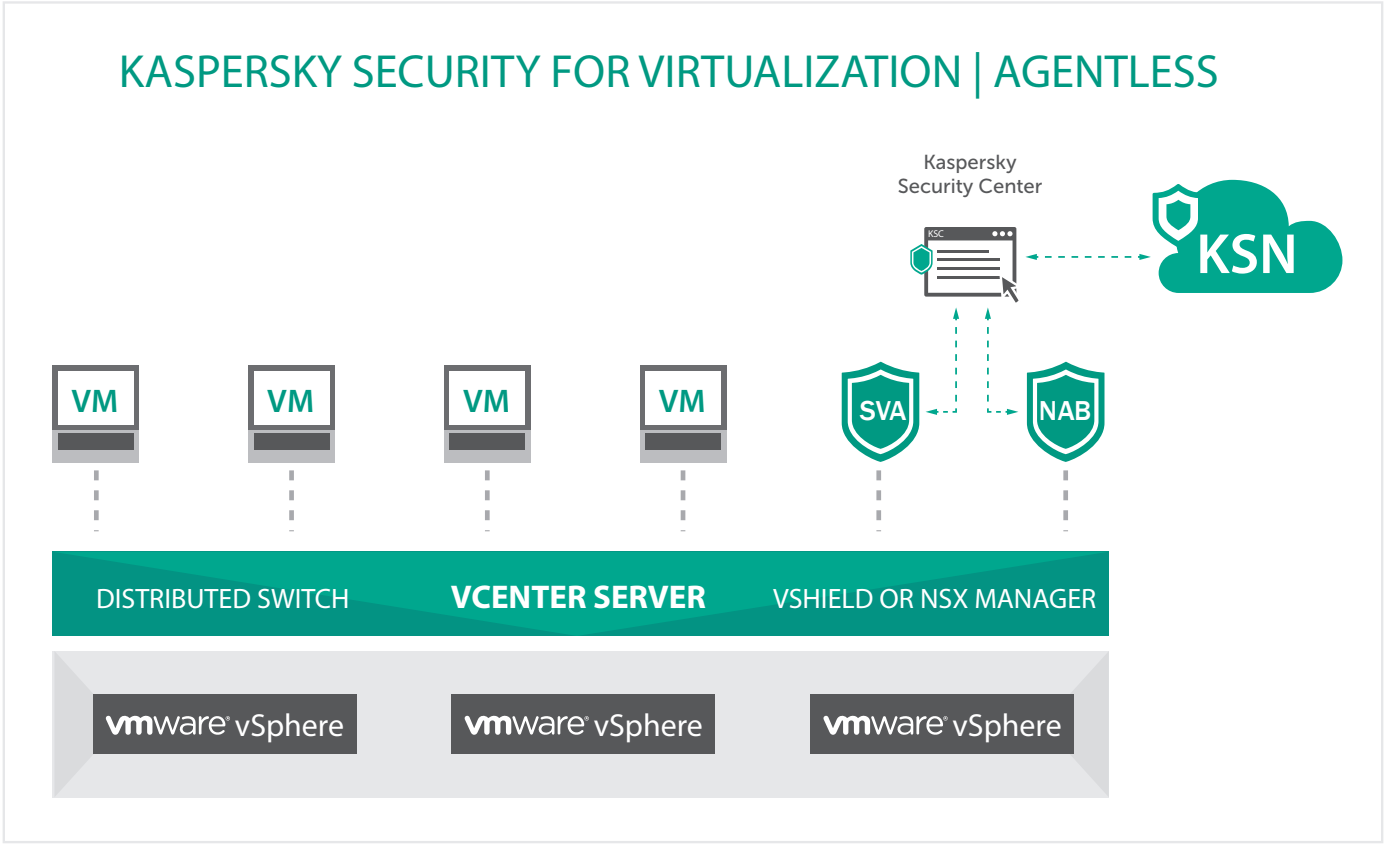
Another approach is an API-independent or, rather, a virtualization-platform-independent solution, which utilizes a lightweight agent optimized to operate inside the OS of each VM being protected. With the file scanning engine and databases still held centrally on the SVA, 'light agent' technology delivers a dramatically smaller resource footprint than a traditional full agent solution. The solution sits between "agentless" and traditional full agent solutions in terms of resource consumption, but is not tied to or limited by VMware technologies and can also be used on popular platforms including Microsoft Hyper-V, Citrix XenServer and KVM.



KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Kaspersky Security for Virtualization | Agentless was specifically designed to utilize all the advantages of vShield Endpoint technology. The Security Virtual Appliance (SVA), ready for deployment out-of-the-box, is powered by Kaspersky Lab's award-winning anti-malware engine, benefiting from superior detection rates and performance. Support for the cloud-assisted Kaspersky Security Network service ensures the fastest possible reaction times and, importantly, identifies new malware threats in as little as 0.02 seconds. This enables Kaspersky Security for Virtualization to protect your virtualized environment against even zero-day threats.

VMware NSX-enabled environments benefit from integration between Kaspersky Security for Virtualization | Agentless and VMware's native NSX Guest Introspection, so your infrastructure will scale with no limitations while your security solution seamlessly follows topology and infrastructure changes.



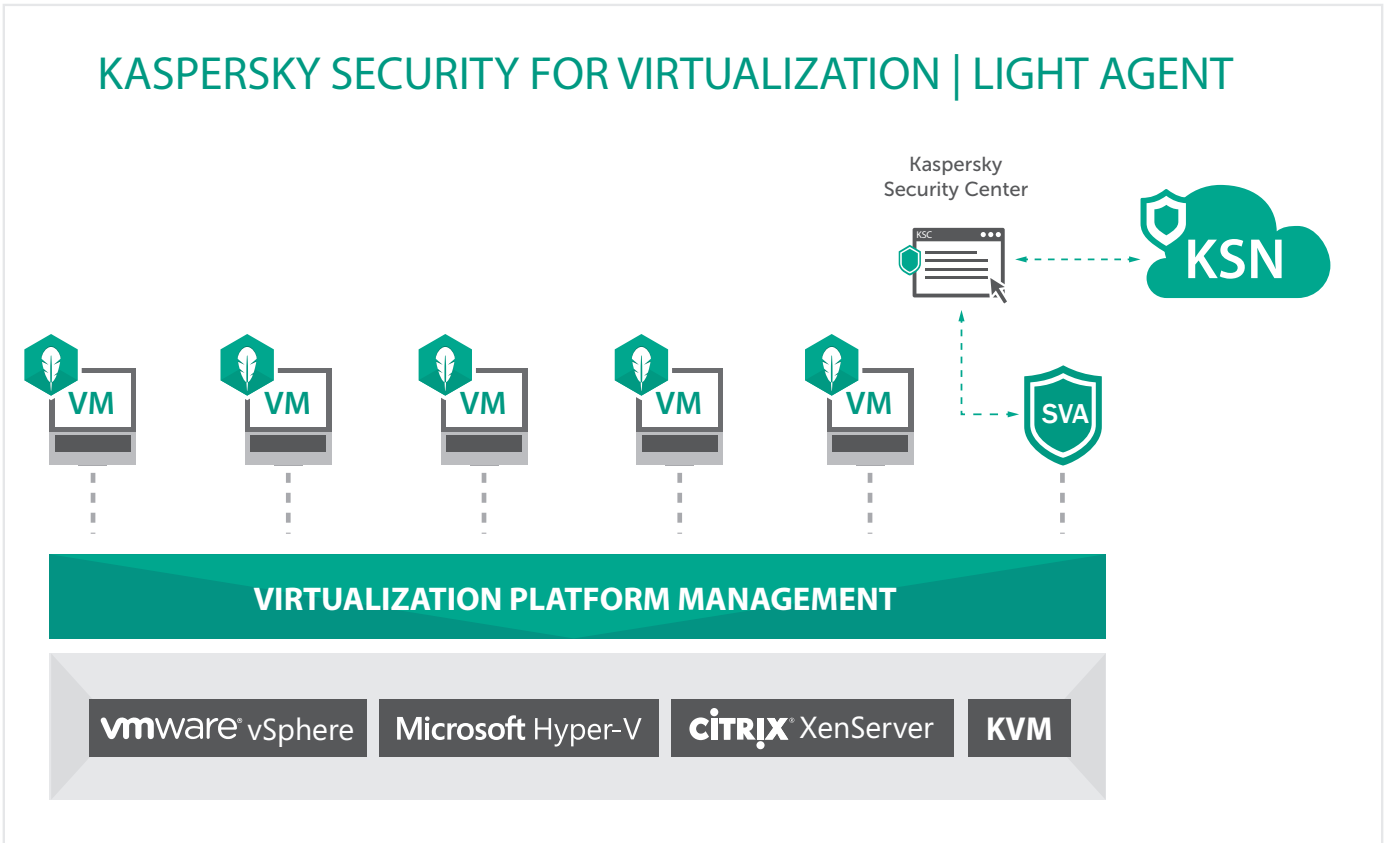
For advanced network protection, a second SVA may be used to deliver Kaspersky Network Attack Blocker functionality, in close integration with VMware's vCloud Networking & Security component.

There are shortcomings to an 'agentless' approach. First, VMware vSphere is the only virtualization platform with an intermediate security layer - vShield endpoint. For other virtualization platforms, the security solution must install some form of agent inside the guest OS of individual VMs to perform file-scanning tasks at machine level. Secondly, due to VMware's design, native technologies like vShield Endpoint and NSX Guest Introspection don't provide access to the VM's internal processes, applications or web traffic, or to virtualized devices. Infrastructure protection is limited to file level scanning, which significantly decreases the solution's ability to provide deep protection against advanced malware at individual VM level.

KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

A 'light agent' approach overcomes these limitations. With the file scanning engine and databases still held centrally on the SVA, this application has a dramatically smaller resource footprint than traditional full agent solutions. The light agent on each VM provides access to individual machine memory, application and internal processes, as well as to web traffic and virtualized devices. This access allows advanced security techniques to be deployed at machine level, while preserving overall virtualization platform efficiency and performance.

Kaspersky Security for Virtualization | Light Agent has been specifically designed for virtual environments and supports most popular platforms: Citrix XenServer, Microsoft Hyper-V, VMware and most recently KVM.



In virtualized server environments, Kaspersky Security for Virtualization | Light Agent users benefit from valuable technologies like HIPS (Host-Based Intrusion Prevention System) and a proprietary Firewall, giving protection from network attacks. For VDI environments, security is extended with comprehensive network protection capabilities and a full set of endpoint controls - allowing you not just to protect your systems from malware, but to limit the use of untrusted applications, devices or web resources. The solution architecture significantly reduces the attack surface, saving precious computing resources. A powerful multi-layered defensive perimeter, capable of eliminating sophisticated malware and even zero-day threats, is supplemented by Automatic Exploit Prevention (AEP) technology.

A 'light agent' approach means you can secure your virtual environment – including virtual servers and VDI - with no significant impact on hypervisor performance. So you fully protect your systems and sensitive corporate data while preserving machine density and quality of user experience.

KASPERSKY PROTECTIVE TECHNOLOGIES VS. THREATS TO YOUR VIRTUAL INFRASTRUCTURE

VMs are every bit as vulnerable as their physical counterparts – perhaps even more so: in lightning-fast virtualized networks, the spread of infection can be devastating. So it's important to identify the security weaknesses in your virtual infrastructure, and to deploy an efficient security solution with specific protection to fight advanced threats. Below, we examine potential threats to virtual systems, and the technologies used to counteract them.

Malware executables

Whether it's an insidiously crafted attachment received via email, infected leisureware or a temporary malware-created executable – anti-malware protection is essential deal with basic threats. Our powerful malware-fighting engine is the core of both our Agentless and Light Agent configurations of Kaspersky Security for Virtualization, though different means are used to reach into the protected VM's file.

Another way to prevent malware agents from harming your virtualized assets is through Application Control with Dynamic Whitelisting. When only trusted software is allowed to run on a VM, malware has no chance of executing. Kaspersky Security for Virtualization | Light Agent allows endpoint controls, including Application Control, to be enabled on individual VMs.

Bodiless malware

Some sophisticated malware does not have a 'body' – so there's nothing to be found in the file system. Spawned by a previously launched executable, or injected via an exploit, this malware can rarely be detected by traditional anti-malware solutions. Advanced anti-malware techniques, which can monitor processes in the memory and immediately block programs engaged in any suspicious or dangerous activity, are required.

Kaspersky Security for Virtualization | Light Agent is armed with a range of technologies able to block incursions into the VM's memory. These include:

- System Watcher, which monitors program behavior, tracing system events.
- Behavioral Stream Signatures, identifying behavior patterns characteristic of malware activity.

- Privilege Control, restricting application from making unsolicited changes, including process injection.

These tools allow the Host-based Intrusion Protection System (HIPS) to track down and stop rogue processes in the VM memory.

Exploits

The exploitation of vulnerabilities found in systems components and popular applications remains a highly effective attack mechanism. Though it is possible to thwart these incursions using the technologies above, the affected program may operate at a high privilege level, limiting control over its activities.

The most effective method of tackling this form of threat is to prevent exploits from exploiting their targeted vulnerabilities. To swiftly overcome the dangers posed by unpatched vulnerabilities, Kaspersky Security for Virtualization | Light Agent offers Automatic Exploit Prevention (AEP) technology. AEP specifically monitors the most frequently targeted applications in critical environments like VDI – including Adobe Reader, Internet Explorer, Microsoft Office, Java and many more – delivering an extra layer of security monitoring and protection against unknown threats.

The efficiency of this technology has been proven in independent tests performed by MRG Effitas institute, which found that, even with all other protective components switched off, Kaspersky's AEP technology remained 100% effective against exploit-using attacks (see Real World Enterprise Security Exploit Prevention, MRG Effitas, March 2015 for details). Even unknown, zero-day exploits are blocked by this superior technology.

Rootkits

Sophisticated malware is often capable of hiding itself, preventing detection by traditional anti-malware with the help of so called "bootkits" and "rootkits". These insidious tools try to boot or execute the malware as early as possible, so that it gains high privileges within the guest operating system, helping it remain undetected.

Operating both in memory and at file system level, Kaspersky Security for Virtualization | Light Agent uses Kaspersky Lab's Anti-Rootkit technology to detect and eradicate even this deeply hidden malware.

Network attacks

Network-based cyber threats may allow the attacker to obtain crucial information about the network, gaining access to the targeted system's resources, interfering with critical processes and affecting its smooth operation. These threats include malicious actions like port scanning, denial-of-service attacks, buffer under-run attacks. Both our 'agentless' and 'light agent' solutions have network protection technologies built-in. Kaspersky Security for Virtualization | Light Agent extends network protection capabilities with built-in HIPS (Host-based Intrusion Prevention System) and additional proprietary technologies to fight external and internal network attacks – including threats that may be hidden in non-transparent virtualized traffic.

Kaspersky Security for Virtualization | Agentless also addresses this issue, leveraging VMware integration to provide a Network Attack Blocker – a dedicated virtual appliance designed to monitor network traffic for signs of typical attack activity.

Malicious websites

One of the most common sources of infection is a malicious, or infected, website. Though this rarely affects virtualized servers, it may pose a serious threat to VDI, a fact not always fully appreciated by corporate users. This is where Kaspersky Lab's web protection technologies come into play.

Anti-phishing prevents users from accessing websites reported as dangerous, using information obtained via the Kaspersky Security Network (KSN) and continuously updated with the help of millions of KSN's voluntary participants around the globe. As yet undiscovered phishing sites are also blocked, thanks to a heuristic engine that analyzes the source text of the loaded page, detecting signs of malicious code. Web Control lets you manage Internet usage, so you can block access to social networks, music, video, non-corporate web email and any websites that contain inappropriate content or are against your corporate policy. You can deploy different policies reflecting different responsibilities, and choose between applying a complete block or just blocking access during specific periods.

Peripherals-based attacks

Traditionally, one of the most effective methods of introducing an infection into an IT network is through external storage. While network-delivered infections now appear the greater threat in terms of sheer numbers, external storage remains a significant danger – especially when it's part of a carefully planned targeted attack. It is worth mentioning that ungoverned non-storage peripherals can also pose a threat - external storage drives are one of the most popular methods of stealing your confidential data. While it may not be easy for an unauthorized person to access the physical machines hosting your virtual infrastructure, it is possible.

So hardware connecting to your virtualized environment should be a concern. For example, using thin-clients is a best practice for VDI deployments, and even simplest thin-clients have USB ports. Controlling peripherals can be nightmare – or can be done seamlessly using Kaspersky Lab's Device Control technology. This technology allows you to specify which removable devices are granted access to individual VMs, so it's easy to apply control policies covering a range of devices, including removable drives, printers and non-corporate network connections.

Data leakage

Secrets leaking from a corporate IT environment may harm not only business-critical processes or systems but the entire business, including reputational damage that may have long-lasting and painful consequences. So restricting the number of ways information is shared is a good option to protect your business.

Both Kaspersky Lab's Application Control and Device Control are useful here. Application Control can prevent dangerous applications, such as instant messengers or file hosting and P2P client apps, from executing on the secured VM, while Device Control restricts the use of external storage, which could be used to steal sensitive data. Both technologies are included in Kaspersky Security for Virtualization | Light Agent.

Agentless or light agent: which is better?

The answer depends on which virtualization platform or platforms you utilize, and specific deployments. Regardless of the hypervisor used to build your virtualized environment – VMware vSphere, Citrix XenServer, Microsoft Hyper-V or KVM – you can protect your critical virtual servers and fast-growing VDI with Kaspersky Security for Virtualization | Light Agent. But you may also consider Kaspersky Security for Virtualization | Agentless for non-critical VMware-based servers which do not require strong multi-layered security.

Luckily, Kaspersky Security for Virtualization licensing policy allows you to deploy the most appropriate approach to each part of your virtualized environment – 'agentless', 'light agent' or a combination of both - under single license.

Whatever combination of Citrix XenServer, VMware vSphere, KVM or Microsoft Hyper-V virtualization platforms, and whichever approach you are using, all your virtual and physical machines, as well as mobile security, can be managed simply and centrally through a single unified interface – Kaspersky Security Center. And utilizing our cloud-based security service – Kaspersky Security Network – allows for almost instant detection of advanced threats.


Twitter.com/
Kaspersky


Facebook.com/
Kaspersky


Youtube.com/
Kaspersky

Kaspersky Lab, Moscow, Russia
www.kaspersky.com

All about Internet security:
www.securelist.com

Find a partner near you:
www.kaspersky.com/buyoffline

KASPERSKY lab