# ▶ LIGHT AGENT OR AGENTLESS

## A Feature Guide to Kaspersky Security for Virtualization

**With virtualization becoming widespread, the need for adequate security solutions is self-evident. Although just as susceptible to cyber-attacks as any physical system, virtual environments present unique features which need to be considered when looking at security solutions.**

While providing a certain level of protection, standard solutions not designed specifically for virtual environments can introduce issues 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 several VMs leading to an avalanche-like increase of 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 start-up 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.

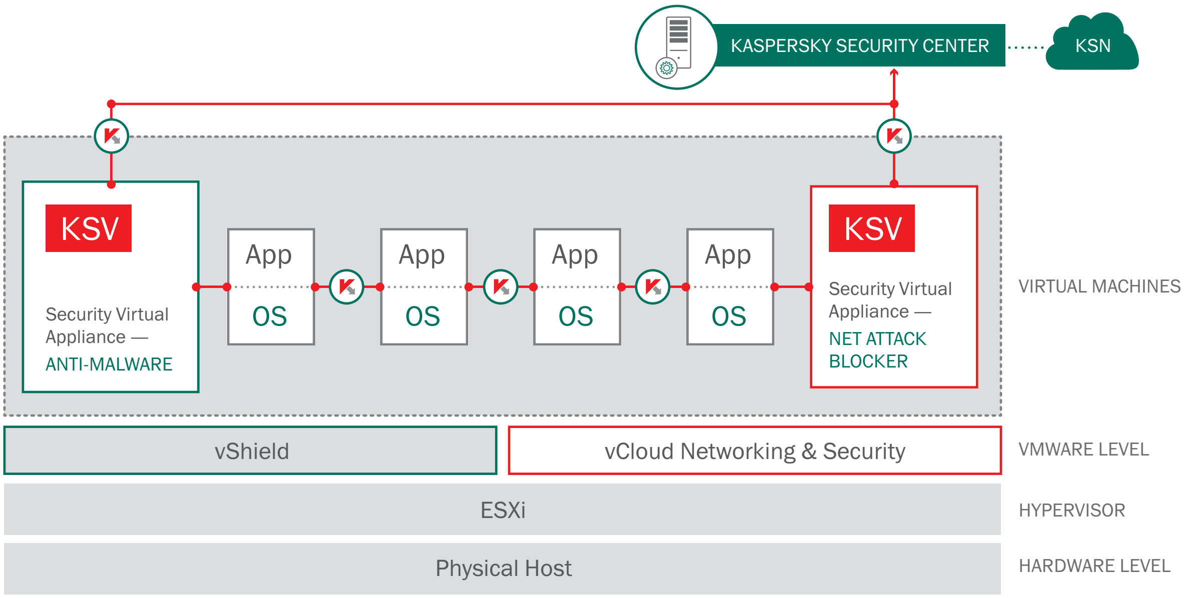
Recognizing the importance of virtual systems security, and the unique features virtualization presents, market leaders VMware developed vShield, a specific defensive layer for its vSphere platform. This layer creates an integrated security space enveloping all virtualized assets and allowing easy and efficiently access by appropriately designed security solutions. One obvious benefit of this approach is that "agentless" protection of virtualized endpoints becomes an option. Only one Security Virtual Appliance (SVA) – a specialized virtual machine carrying an anti-malware scanning engine and signature databases – is needed, removing this burden from individual VMs and so greatly reducing resource consumption. vShield-compatible security solutions fully able to leverage all the features VMware's environment offer, can gain many benefits for users through this approach.

## KASPERSKY SECURITY FOR VIRTUALIZATION I AGENTLESS

Kaspersky Security for Virtualization I Agentless was specifically designed to utilize all the advantages of vShield. A Security Virtual Appliance (SVA), ready for deployment out-of-the-box, is powered by Kaspersky Lab's award-winning anti-malware engine and so benefits from superior detection rates. Support for the cloud-assisted Kaspersky Security Network service ensures the fastest possible reaction times and, importantly, significantly reduces the number of false positives. A second SVA may be used to deliver Kaspersky Network Attack Blocker technology, in conjunction with VMware's vCloud Networking & Security component.

However, there are shortcomings to an 'agentless' approach.

For a start, VMware is the only vendor providing an intermediate security layer; for other platforms, the security solution must find another way to access individual VMs. Secondly, vShield does not provide access to the virtual machines' internal processes, significantly decreasing any solution's ability to provide deep protection against advanced malware at this level.



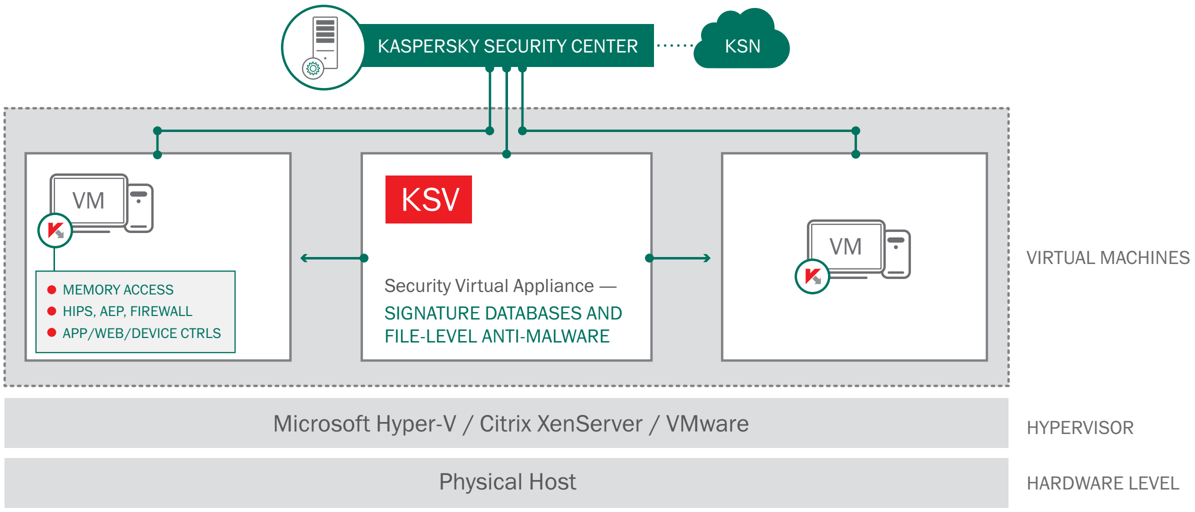
To overcome these limitations, another approach was introduced, deploying a small light-weight application to the VM being protected in addition to the SVA. This application is known as a “light agent”. With the file scanning engine and databases still held centrally, this application has very much smaller footprint on the VM memory than a full agent solution, while providing access not just to the VM’s file system, but to its memory and internal processes. As a result,  additional, more advanced security techniques can be employed.

## KASPERSKY SECURITY FOR VIRTUALIZATION I LIGHT AGENT

**Kaspersky Security for Virtualization I Light Agent** was created for all three of the most popular virtualization platforms; Citrix, Microsoft Hyper-V and VMware. The anti-malware scanner and the signature databases reside on a dedicated SVA, just as with agentless technology, freeing up resources for the deployment of additional VMs so consolidation ratios are optimized. And, with a light agent operating inside each guest OS, it becomes possible to employ most of the advanced technologies available to physical machines through **Kaspersky Endpoint Security for Business.** A full set of endpoint controls can be deployed, as well as HIPS (Host-Based Intrusion Prevention System), a proprietary Firewall and a Systems Management toolset. A powerful multi-layered defensive perimeter,  capable of dealing with the most sophisticated examples of malware and even with zero-day threats, is created.

Of course, while providing a higher level of protection, the **Light Agent** solution may appear ‘heavier’ than its **Agentless** counterpart, and it does require a little more attention when deploying new VMs. But even these issues are not as straightforward as they appear.

For a better understanding, we need to look deeper into the functionality of both **Agentless** and **Light Agent** solutions, and the threats they are designed to counter.


KASPERSKY SECURITY CENTER
KSN
VM
MEMORY ACCESS
HIPS, AEP, FIREWALL
APP/WEB/DEVICE CTRLS
KSV
Security Virtual Appliance —
SIGNATURE DATABASES AND FILE-LEVEL ANTI-MALWARE
VM
VIRTUAL MACHINES
Microsoft Hyper-V / Citrix XenServer / VMware
HYPERVISOR
Physical Host
HARDWARE LEVEL

# THREATS VS. FEATURES

Virtual machines 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 adequate measures in proportion to the potential 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 is essential to deal with these basic threats. The malware-fighting engine is the core technology of both **Agentless** and **Light Agent** configurations of **Kaspersky Security for Virtualization**, though it reaches into the protected VM's file systems through different means in each case.

Another way to prevent malware agents from harming your virtualized assets is through Application Control with Dynamic Whitelisting. When only legitimate and safe software is allowed to run, malware is stopped in its tracks. Kaspersky Security for Virtualization | Light Agent allows Application Control to be enabled on VMs, although Kaspersky Security for Virtualization | Agentless, operating through vShield, is not able to support endpoint controls.

## BODILESS MALWARE

Some sophisticated malware does not have a 'body' – which means there's nothing to be found in the file system. Spawned by a previously launched executable or injected via an exploit, this malware cannot be detected by traditional anti-malware. Advanced anti-malware counter-measures, able to watch over processes in the memory and immediately block programs engaged in any suspicious or outright 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. This is supported by
- BSS – Behavioral Stream Signatures, identifying behavior patterns characteristic to 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 VM memory.

**Kaspersky Security for Virtualization | Agentless** is only capable of tracing changes at file system level, due to vShield API limitations.

## EXPLOITS

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

The most effective method of tackling this threat is to prevent the exploits from doing what their name implies – exploiting the vulnerabilities in the first place. This is achieved through recognizing the sequence of actions characteristic to exploits as they take place; as performed by Kaspersky's Automatic Exploit Prevention (AEP). The efficiency of this technology was proved by a series of independent tests performed by MRG Effitas institute. These tests found that, even with all other protective components switched off, Kaspersky's AEP technology remained 100% effective against exploit-using attacks. Even unknown, zero-day exploits are blocked by this proactive technology.

**Kaspersky Security for Virtualization | Light Agent** is equipped with this advanced feature, which makes it particularly useful in Virtual Desktop Infrastructures (VDI) employed to replace physical desktops – with their commensurately higher risks of drive-by infections.

**Kaspersky Security for Virtualization | Agentless** must rely on vShield capabilities, which lack features similar to Kaspersky AEP.

## 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 load malware as early as possible, so it remains undiscovered through gaining high privileges within the system. Kaspersky's Anti-Rootkit technology is able to detect and eradicate even such deeply hidden malware. It operates both in memory and at file system level, requiring access to the guest machine's RAM and processes to operate.

**Kaspersky Security for Virtualization | Light Agent** can offer this technology, because it has full access to guest machine resources.

**Kaspersky Security for Virtualization | Agentless** can only access the file system, so lacks full anti-rootkit capability.

## NETWORK ATTACKS

There are threats that take advantage of networking system features, allowing the attacker to obtain crucial information about the network under attack, gain access to the targeted system's resources or interfere with its smooth operation. These include port scanning, denial-of-service attacks, buffer-underrun attacks and other malicious actions. Such attacks require specialized counter-measures of the sort provided by Kaspersky's Network Attack Blocker. As the name suggests, this technology stops incoming network attacks, with the help of an IDS (Intrusion Detection System), by utilizing heuristic algorithms to discern even the most complex attack patterns.

Both **Kaspersky Security for Virtualization | Agentless** and **Kaspersky Security for Virtualization | Light Agent** have these network technologies in their arsenals.

## 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 desktop-replacement VDI if users are allowed full Internet access. This is where Kaspersky's web technologies come into play. Anti-phishing prevents users from accessing websites reported as dangerous, using information obtained via **Kaspersky Security Network** 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** technology has the added benefit of restricting access to non-work-related websites, such as gaming or social networks, preventing users from wasting precious time on non-working activities.

**Kaspersky Security for Virtualization | Agentless** does not possess these host-based features, but **Kaspersky Security for Virtualization | Light Agent** does, making it more suitable for VDIs with access to the Internet.

## 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 still remains a significant danger – especially so when part of carefully planned targeted attack. It's worth mentioning that ungoverned non-storage peripherals can also pose a threat; known cases include, for example, infected printer firmware. And external storage drives remain among the leading methods for your confidential data to leave the building.

While it is not usually easy for an unauthorized person to gain access to the physical machines hosting the virtual infrastructure, it is still possible – and there are business cases where such a possibility is considered too high a risk. And, in terms of desktop-replacement VDI, even the most simple thin-clients may have USB ports.

So controlling peripherals becomes a sensible precaution – and is easily accomplished through **Kaspersky's Device Control** technology. This allows the prevention or restriction in use of specific device and bus types. And of course exceptions can be configured, so that peripherals essential for work can still be used.

As with other Control technologies, Device Control is offered in **Kaspersky Security for Virtualization | Light Agent**, but not in **Kaspersky Security for Virtualization | Agentless.**

## DATA LEAKAGE

Corporate secrets leaking from an IT network may inflict great harm on a business, including reputational damage that may have long-lasting and painful consequences. So restricting the number of ways in which information is shared may become necessary. Both **Kaspersky'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 running, while device control restricts the use of external storage, which may be used to ship out sensitive data.

As above, these two technologies are included in **Kaspersky Security for Virtualization | Light Agent** but cannot be offered in **Kaspersky Security for Virtualization | Agentless.**

## AGENTLESS VS LIGHT AGENT: WHICH IS BETTER?

For some readers the answer may seem very clear: **Kaspersky Security for Virtualization | Light Agent** is packed with advanced features which are not included in **Kaspersky Security for Virtualization | Agentless** – so the light agent solution is obviously the better. But don't jump to conclusions; it's a little more complicated than this.

First, there's the matter of instant protection offered by **Kaspersky Security for Virtualization | Agentless.** Virtual machines become protected from the very moment of startup, which may be critical if you already have infection running amok in your virtualized network (and your VM cannot be raised from an image containing the **Light Agent** app).

Then again, in some cases **Kaspersky Security for Virtualization | Light Agent** may yield to **Kaspersky Security for Virtualization | Agentless** in the terms of performance. To choose the best security option for your virtual installation and to gain the most from your virtualization project, you'll need to weigh up carefully the potential threats, the value of data being protected and the different layers of protection required.*

Please note that any combination of agentless protection for VMware and light agent based security for any or all three platforms is covered by a single **Kaspersky Security for Virtualization** license. Whether you're employing Citrix, VMware or Microsoft, all are under your control within the comfortable "single pane-of-glass" interface of **Kaspersky Security Center.**

* Read "Kaspersky Security for Virtualization: Understand the Difference" whitepaper for more details on choosing the best combination of Kaspersky solutions for securing your virtual infrastructure.