Virtualization security with Kaspersky Hybrid Cloud Security - a features guide

Light Agent or Agentless?

kaspersky

Virtual environments present unique challenges which need consideration when assessing different security solutions.

Executive summary

Virtualization continues to be widely adopted throughout the corporate world, with good reason. Dramatic resource savings can be made by being able to spin up virtual machines (VMs) as and where needed. However, applying a 'traditional' security approach to virtual environments, with a full-function security agent on each machine, takes up valuable space and can seriously erode the ROI generated by your move to virtualization.

The answer lies in reducing the computational and memory footprint of the agent on the virtual device. Kaspersky Hybrid Cloud Security achieves this through two different approaches – Agentless and Light Agent.

This guide explains how each of these two approaches works, and the features and benefits of each.

Securing virtualized environments – the challenge

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 challenges 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:

- **Excessive resource consumption** due to the replication of signature databases and active anti-malware engines on each protected Virtual Machine (VM).
- **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.
- **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.
- **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.

Meeting the challenge – two approaches

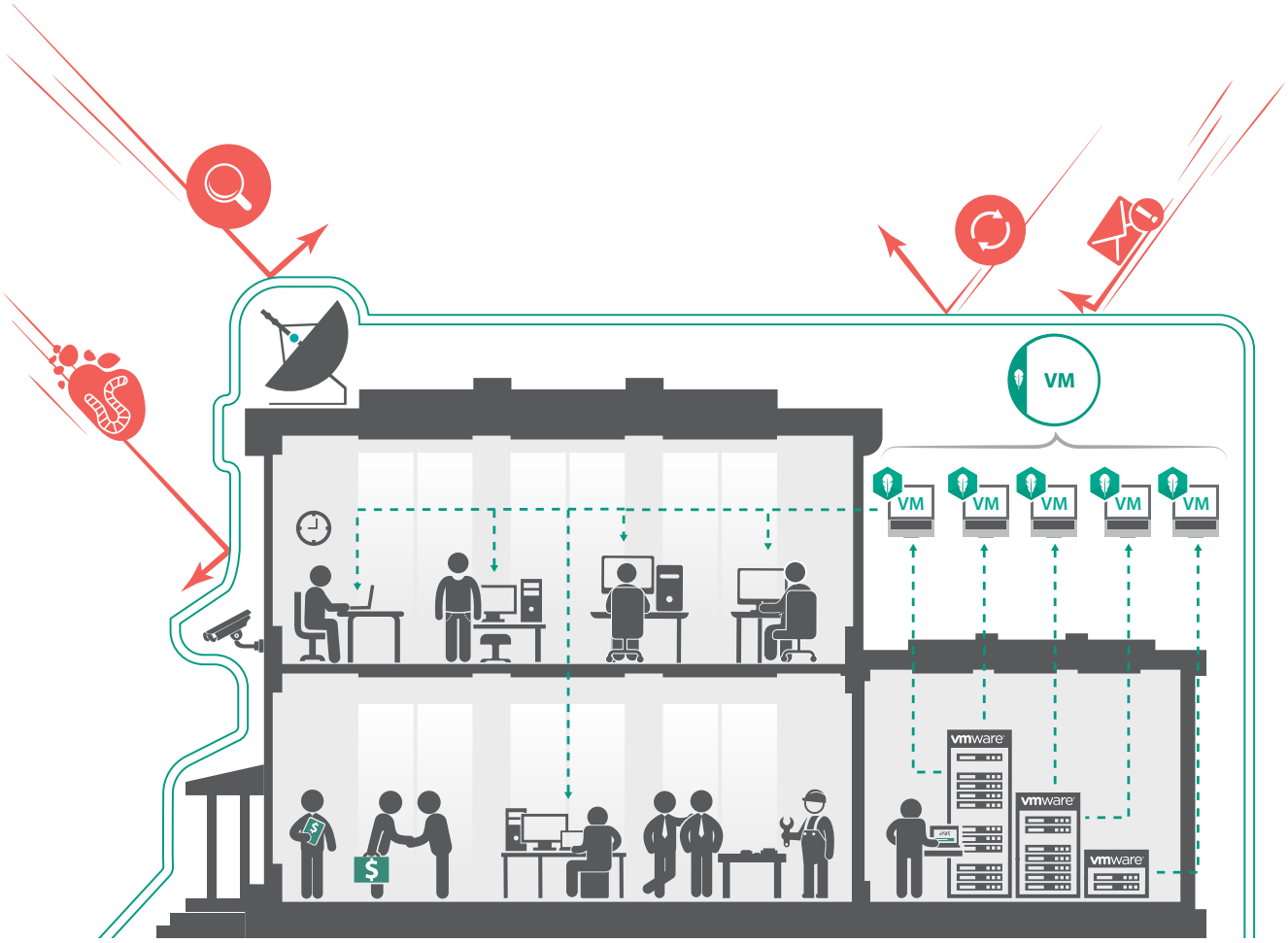
Kaspersky's Light Agent solution covers numerous platforms, including:

- **Microsoft Hyper-V**
- **Citrix Hypervisor**
- **Citrix Virtual Apps and Desktops,**
- **KVM**
- **VMware vSphere**
- **VMware NSX**
- **VMware Horizon**

Recognizing the importance of virtual systems security, and the unique features virtualization presents, leading virtualization technology vendor VMware developed vShield endpoint technology, a specific defensive layer for its vSphere virtualization platform. This layer creates a security connector for third-party solutions that's 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 greatly reducing resource consumption. The biggest benefit of this approach for enterprises 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, more importantly, limited by VMware technologies, and can be used on other popular platforms.



It's your choice
Kaspersky Hybrid Cloud Security incorporates both Agentless and Light Agent applications - so you choose which to deploy and where.

The solution - providing both on-prem and in the cloud

Kaspersky Hybrid Cloud Security provides unified protection and control for an organization's complete virtualized estate, both on-prem and in public clouds, through a single-pane-of-glass console.

One of the main ways we protect our customers' ROI on virtualization, as well as their resources and workloads, is through minimizing the security agent 'footprint' on each VM.

Kaspersky Hybrid Cloud Security does this in two different ways, both of which are offered as part of the solution:

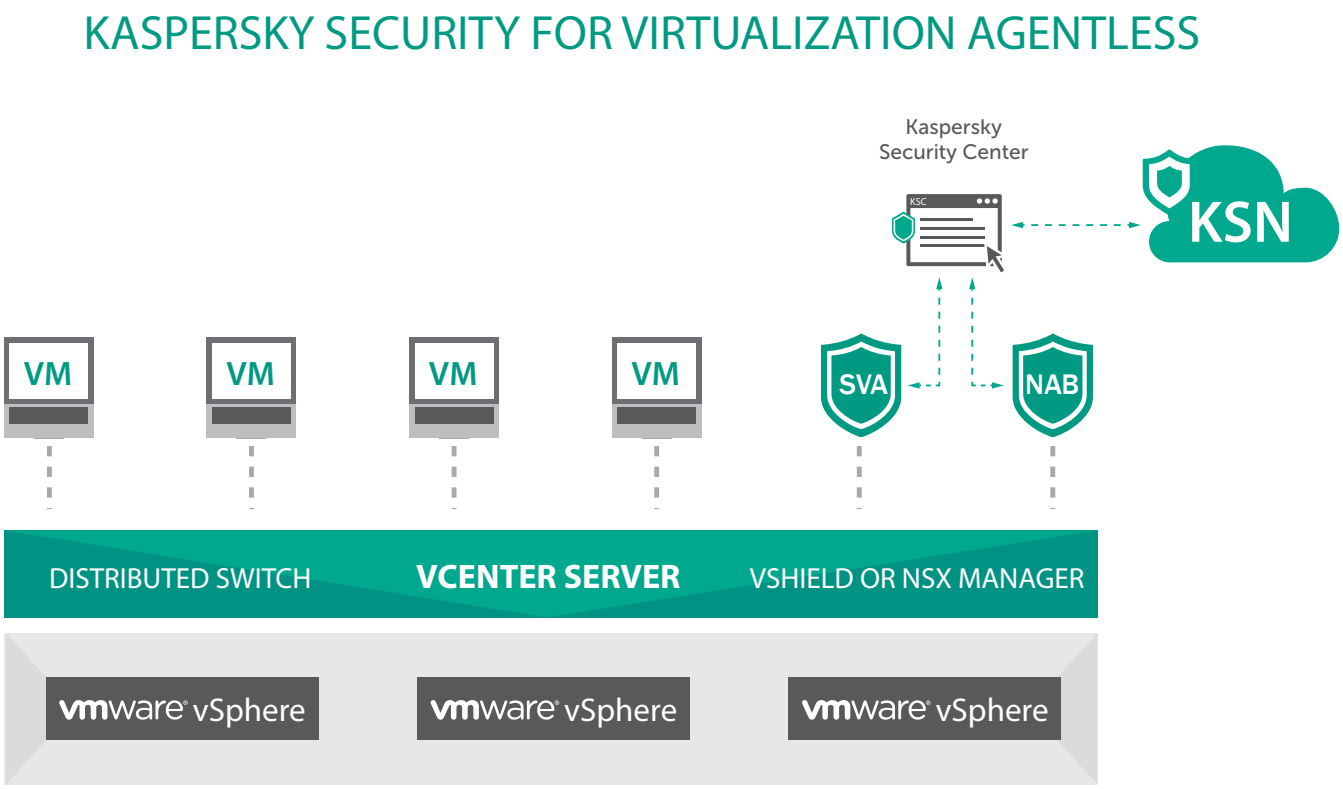
- Our Agentless solution provides significant performance benefits, together with simplified deployment, by leveraging the security architecture offered by VMware environments.
- Our unique Light Agent architecture offers comprehensive multi-layered protection for virtual environments with a much lower resource 'footprint' than traditional security agents, and is compatible with all major virtualization platforms.

Kaspersky Security for Virtualization Agentless

Kaspersky Security for Virtualization Agentless was specifically designed to utilize all the advantages of VMware vShield Endpoint technology. The Security Virtual Appliance (SVA), ready for deployment out-of-the-box, is powered by Kaspersky's award-winning anti-malware engine, benefiting from superior detection rates and performance.

Support for the cloud-assisted Kaspersky Security Network (KSN) service ensures the fastest possible reaction times and, importantly, identifies new malware threats in as little as 0.02 seconds. This enables Kaspersky Hybrid Cloud Security to protect your virtualized environment against even the very latest 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.

Two important considerations

There are some shortcomings in the agentless approach.

First, VMware vSphere is the only virtualization platform offering an intermediate security layer - vShield endpoint. For other virtualization platforms, the security solution must install some sort of an agent inside the guest OS of an individual VMs to perform file-scanning tasks at machine level.

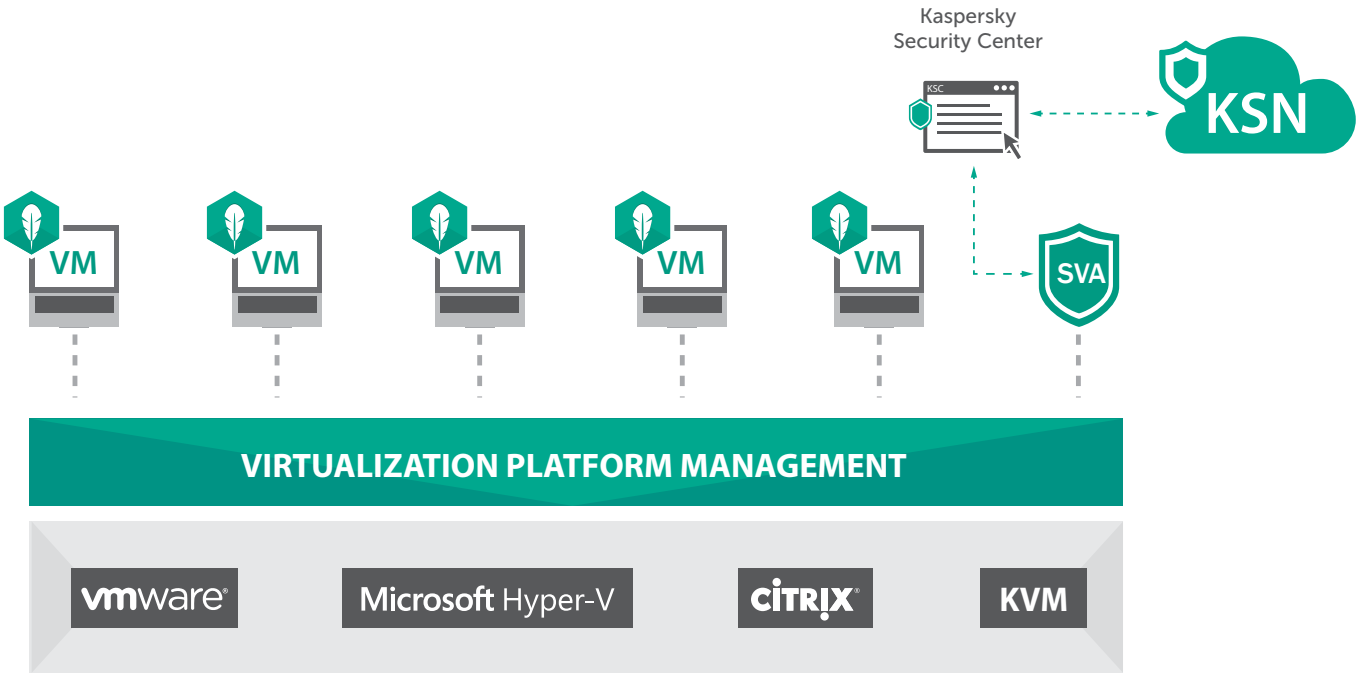
Second, due to VMware's design, native technologies like vShield Endpoint and NSX Guest Introspection don't provide access to the VM internal processes, applications or web traffic, or to virtualized devices. As a result, infrastructure protection is limited to file level scanning, which significantly 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 held centrally on the SVA, this application still has a much smaller resource footprint than traditional full agent solutions. The light agent on each VM provides access to individual VM memory, applications and internal processes, as well as to web traffic and virtualized devices. This access allows advanced security techniques to be deployed at VM 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 Hypervisor, Citrix Virtual Apps and Desktops, Microsoft Hyper-V, VMware vShield, NSX, Horizon, KVM and others.

KASPERSKY SECURITY FOR VIRTUALIZATION LIGHT AGENT



Kaspersky Security for Virtualization Light Agent provides a powerful multi-layered defensive perimeter, capable of eliminating sophisticated malware and even the very latest threats. Users benefit from technologies like HIPS (Host-Based Intrusion Prevention System), a personal firewall, Automatic Exploit Prevention, and a full set of endpoint controls. The solution architecture significantly reduces the attack surface, while saving precious computing resources.

This 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 which specifically addresses advanced threats. Below, we examine the technologies used to counteract potential threats to virtual systems.

Application Control and Whitelisting

When only trusted software is allowed to run on a VM, malware has no chance of executing. This is how Application Control and Dynamic Whitelisting prevents malware from harming your virtualized assets. Kaspersky Security for Virtualization Light Agent allows endpoint controls, including Application Control, to be enabled on individual VMs.

Exploit Prevention

Independent tests performed by the MRG Effitas institute found that, even with all other protective components switched off, Kaspersky's AEP technology remained 100% effective against exploit-using attacks.

The exploitation of vulnerabilities found in systems components and popular applications remains a highly effective attack mechanism. Though it's possible to thwart these incursions, 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.

Vulnerability Assessment and Patch Management

Kaspersky Vulnerability & Patch Management provides comprehensive information about the endpoints and applications running on your network. It gathers data about software versions and ascertains whether updates are required and vulnerabilities need to be patched. The detected vulnerabilities can be automatically prioritized so that the most critical patches are applied first and the most important updates deployed with priority. You get a complete view of what you have, the risks involved, and the tools to mitigate them.

Systems Integrity Assurance

Working alongside application control and exploit prevention technologies, these systems can be used to monitor VMs for state changes and configuration drift. They are also often required for compliance reasons.

System Integrity Assurance technologies include File Integrity Monitoring (FIM), Registry Integrity Monitoring and Baseline Management for virtualized Windows Servers.

Network Security

Network-based cyberthreats 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, and 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.

Behavioral Protection

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 applications 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.

Protection from fileless malware

Fileless malware is malware that does not store its body directly onto a disk. This type of malware became more popular in 2017 because of the increasing complexity of its detection and remediation. Although such techniques were limited to targeted attacks in recent years, today they proliferate more and more in the current threat landscape, and Kaspersky registers new families of trojan-clickers or even adware with fileless components.

Advanced anti-malware techniques, which can monitor processes in the memory and immediately block programs engaged in any suspicious or dangerous activity, are required.

Protection from 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'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.

Blocking 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 to 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.

Anti-rootkit and remediation technologies

Rootkit is a malicious program that applies different techniques of concealing malicious code and activities from detection and counteracts against attempted remediation by antivirus. Anti-Rootkit technology, part of Kaspersky's multi-layered, next generation protection, detects active infection by these rootkit programs and remediates systems from this type of infection.

Kaspersky Security for Virtualization 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.

Agentless or light agent: which is better?

The answer depends on which virtualization platform or platforms you utilize, your specific infrastructure and your security targets. Regardless of the hypervisor used to build your virtualized environment. You can protect your virtual servers and VDI with Kaspersky Security for Virtualization Light Agent. But you may also consider Kaspersky Security for Virtualization Agentless for non-critical VMware-based servers.

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. Even better - flexible licensing also allows to activate traditional endpoint agents, providing a way to gradually migrate from physical infrastructure to virtual server or desktop infrastructure and take as much time or as many steps back as needed without a need to juggle with different sets of licenses for physical and virtual deployments.

Whatever combination of virtualization platforms, and whichever approach you are using, all your virtual and physical machines, as well as public cloud workloads, can be managed simply and centrally through a single unified management interface – Kaspersky Security Center. And utilizing our cloud-based security service – Kaspersky Security Network – allows for almost instant detection of advanced threats.

Kaspersky Hybrid Cloud Security:
www.kaspersky.com/hybrid
Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
Cybersecurity for SMB: kaspersky.com/business
Cybersecurity for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Known more at kaspersky.com/transparency

Proven.
Transparent.
Independent.