KASPERSKY lab

# VIRTUALIZATION SECURITY: UNDERSTANDING THE DIFFERENCE

www.kaspersky.com

# VIRTUALIZATION SECURITY: UNDERSTANDING THE DIFFERENCE

Are you already converting your hardware assets to virtual? Then your business goal is almost certainly to gain maximum efficiency from IT infrastructure. Running several virtual machines (VMs) together on a single computer instead of using dedicated servers, all demanding their own power, cooling and maintenance, makes for a convincing argument. Multiple virtualized nodes powered by a single physical server creates business savings. The economic effect of virtualization can be amazingly powerful: according to survey performed by Forrester in 2011, the implementation of VMware VDI infrastructure yielded as much as 255% of risk-adjusted ROI over a 4-year period, with a break-even point at 17 months after deployment.

The question is, how many VMs can you squeeze into that hardware configuration without a significant impact on performance? This is what's known as the "consolidation ratio", and this is the really tricky part, with the multitude of factors to consider. What sort of tasks are your virtual machines supposed to carry out? What hypervisor software do you employ? What are the risks of putting all your eggs into so few baskets? And how do you reliably secure your new virtual infrastructure, making sure you're not vulnerable to cybercriminals, without going to extremes and slowing everything to a crawl? To make the right decision, you need to understand several concepts, and to look at how they work together.

## Virtualization Models

The industry has defined several virtualization models. This paper considers three:

- **Server Virtualization** - allowing several instances of an operation system to run together on a single server. This is the best way to increase your resource utilization - by up to 80% compared to an average utilization rate of 10-20% for common single-role physical servers[1].
  **Hardware Server Virtualization**, providing only one intermediate layer (hypervisor) between virtual machine (VM) and bare metal, offers greater value than **Software Server Virtualization**, where the underlying operating system involves some additional resource consumption. So for most business applications, Hardware Virtualization is preferred.

1 Ruest D. Virtualization.A Beginners Guide. McGraw-Hill,2010, Page 4

- **Desktop Virtualization** - offers a different value scenario by replacing an army of physical desktops with Virtual Desktop Infrastructure (**VDI**). Cost-effective 'thin clients', role-based remote desktops, remote branches with no need for a dedicated IT service and all the maintenance for hundreds of workplaces limited to a handful of physical servers.
- **Application Virtualization** - here, unlike a role-based remote desktop infrastructure; a virtual environment is adopted only for a single application. For increasingly popular Software-as-a-Service approaches, this is a natural - and efficient - choice.

All virtualization models have many uses - and every use carries some relevant risks. Among these, the risk of cyber-threats is one of the most significant, making it absolutely necessary to employ some kind of security solution. This task becomes even more challenging when you realize that all three approaches may be employed within a single IT network. And, yes, you'll also need to cope with additional resource consumption.

However, there are ways to lessen the impact on your newly built highly efficient virtual infrastructure.

# A SPECIALIZED SECURITY SOLUTION FOR VIRTUAL ENVIRONMENTS IS ESSENTIAL

Of course, you can install familiar Endpoint Protection agents on your virtual machines. But there's a number of major shortcomings that can make your experience with virtualized IT infrastructure less than satisfying.

1. **Duplication.** Every VM will carry an identical set of security components, including an isolated anti-malware engine and signature databases, each of which will need to update independently. So a significant proportion of your precious resources - processing power, RAM and disk storage – is consumed quite pointlessly, significantly reducing the resulting consolidation ratio.
2. **"Storms".** This term is used for simultaneous anti-malware scanning or database updating activity by multiple machines, which can lead to a sudden peak in resource consumption and a consequent drop of performance, and even to a denial of service. Manual configuration can help partially solve this issue, but with scores and hundreds of VMs, manual intervention may be extremely time-consuming.
3. **"Instant-on gap".** Some virtual machines remain dormant until called to service when the need arises. Unfortunately, it is not possible to update security solution components or databases on an inactive VM. So immediately after booting and before the security update is completed, the VM is vulnerable to attack.
4. **"Panic attacks".** It is a common practice among system administrators to pre-define the reaction to a virus outbreak as a tightening of security parameters, switching to "paranoid" mode and triggering an unscheduled scanning process. Such a policy, which may have value for physical nodes, can easily bring a virtual environment to a grinding halt.
5. **Incompatibility problems.** Virtual machines are in many ways similar to their physical counterparts – but there are some major differences to bear in mind, such as the use of non-persistent disks or the live VM migration process. Standard anti-malware, having been designed for physical endpoints, does not make allowance for the many nuances characteristic of virtual environments, and so may cause unexpected lags and glitches, or even fail to run at all.

Given all of the above, the overall need for a specialized solution becomes obvious. Such a product should be created with awareness of all the above considerations in mind – while providing the highest possible level of protection with the minimum impact on overall performance. Kaspersky Lab – the world's technological leader on the field of cybersecurity – is well up to the task, offering a solution for all three most popular virtualization platforms – VMware, Microsoft Hyper-V and Citrix.

# PLATFORMS AND MODES OF PROTECTION

## Agentless approach

VMware, one of the oldest and still the most popular virtualization platform, provides a solution called vShield, which allows the burden of carrying identical databases and doubling anti-malware scanning agents to be offloaded from the VM. This is being called "agentless" approach.

Kaspersky Lab offers a specialized security solution for VMware platforms, **Kaspersky Security for Virtualization | Agentless**. Here, scanning functions are transferred to a single Security Virtual Appliance (SVA), a specialized virtual machine holding both the scanning engine and the security databases, providing protection for all the VMs running on the hypervisor.

The benefits are clear:

- The native interface provided by VMware vShield offers efficient access to VMs, freeing up individual machines resources and ensuring compatibility with other VMware technologies
- The resources freed up due to the concentration of anti-malware functions and the signature database onto a single Virtual Appliance can now be used to deploy additional VMs, increasing the consolidation ratio.
- As new VMs are booted up protection is provided instantly through the SVA, with no 'instant on-gap' or the need for installation of any additional software.
- The ever-awake Kaspersky SVA keeps its signature database continuously updated, and, even more importantly, it maintains connection with the Kaspersky Security Network (KSN), a worldwide infrastructure that processes information from millions of voluntary participants and provides protection from the most recent threats even before it is deployed via the database updates.
- The problem of "storms" is eradicated as a single SVA is updated, and the SVA automatically scans the VMs, following a randomly set schedule with and limiting the number of used threads.

In addition, with the help of basic network security functions provided through vCloud Networking and Security, the Kaspersky solution is capable of detecting and preventing incoming attacks on VMs, efficiently blocking the attacker with Network Attack Blocker technology[2].

2 Setting up network protection in KSV | Agentless requires deployment of a secondary SVA

Unfortunately, vShield capabilities are limited, providing access to protected VMs only at file systems level. So processes that occur within the VM's memory itself cannot be monitored and controlled by agentless anti-malware. This also means that other endpoint protection technologies, like Application Control with Dynamic White listing, designed to provide powerful additional layers of security, cannot be implemented.

It should be noted that, as vShield is proprietary VMware technology, the agentless principle for securing a virtual infrastructure can also only be applied to the VMware platform at this time.

## Light Agent approach

Mindful of the limitations outlined above, **Kaspersky Lab** offers another variant of solution for Virtualization, an approach that sits midway between agentless and full agent: **Kaspersky Security for Virtualization | Light Agent**.

As with the agentless approach, databases and the file-scanning anti-malware engine are located on the SVA. But there's a difference: a lightweight resident module is deployed to each VM being protected.

Kaspersky Security for Virtualization | Light Agent is not limited by the security capabilities of vShield technology, but has full direct access to every VM, including everything that's happening within each operative memory. So the full range of Kaspersky Lab's leading edge technologies can be employed to defend the virtualized infrastructure.

Key benefits of Kaspersky Security for Virtualization | Light Agent include:

- Less resource consumption compared with a full agent-based solution, as the file system-scanning engine and databases are moved to the dedicated SVA.
- Support for all three most popular virtualization platforms - VMware, Microsoft Hyper-V and Citrix*
- The highest possible level of protection, provided by full access to VM resources, including the operative memory.
- Additional proactive security layers, such as HIPS armed with Automatic Exploit Prevention, and Application Control with Dynamic White listing, become available. It is easy to deploy even the tightest security scenarios, including 'Default Deny'.
- Being initially designed with virtualization in mind, the solution works with the unique features of the virtual environment, not against them.

Of course, everything comes at a price. The Light Agent must be present on every newly deployed VM - a process easily automated by including the LA in the pre-generated VM image. Due to the presence of the Light Agent itself, Kaspersky Security for Virtualization | Light Agent has somewhat larger footprint in memory than the agentless application; but it should be said that, under certain conditions, the Light Agent solution can actually outrun the vShield-based Agentless application.

One more fact to remember is that the number of supported hypervisors is limited by three most popular platforms. And, at the time of writing, the Microsoft Windows family is the only guest OS supported by both Agentless and Light Agent applications.

But that certainly doesn't mean you are defenseless if you do not employ one of these three platforms. There is still full agent based security, as designed by Kaspersky Lab, to be considered.

## Full agent approach

**Kaspersky Endpoint Security**, despite being a full-agent solution, is actually capable of doing a remarkably decent job in virtual environments. Though requiring more resources than Kaspersky Security for Virtualization, it can be adopted for use in virtual environments. So, if there's a need to secure some peculiar configuration, be it a set of Linux servers or Windows guests on some exotic hypervisor, you're still armed.

The benefits of deploying Kaspersky Endpoint Security over your virtual infrastructure including:

- Support for the most contemporary Operating Systems
- Incorporates the most comprehensive set of Kaspersky Lab advanced technologies
- Completely familiar management principles, as with any regular physical machine
- It's efficiency is recognized by three world leading consulting agencies - Gartner, IDC and Forrester, naming one of the best available Endpoint Protection Platforms; a "triple crown".

Table 1: Comparative feature list

| Feature | Kaspersky Security for Virtualization \| Agentless | Kaspersky Security for Virtualization \| Light Agent | Kaspersky Endpoint Security for Business |
|---|---|---|---|
| Virtualization Platforms Supported | VMware | VMware, Microsoft Hyper-V, Citrix | Any except OS-level[3] |
| Guest OS supported | MS Windows | MS Windows | MS Windows, Mac OS X, Linux |
| Consolidation ratio within a single host | * * * | * */* * *[4] | * |
| Centralized Management via Kaspersky Security Center | + | + | + |
| KSN functionality | + | + | + |
| Protection of new VM without additional installations | + | +/-[5] | - |
| Anti-ma lwa re | * * | * * * | * * * |
| Firewall | - | + | + |
| Host-based Intrusion Prevention (HIPS) | - | + | + |
| Network Attack Blocker | + | + | + |
| Application Control with Dynamic Whitelisting and support for Default Deny | - | + | + |
| Web Control | - | + | + |
| Device Control | - | + | + |
| Systems Management | - | +[6] | +[6] |
| Encryption | - | - | + |

So, after all the tedious calculations, the question is raised once again: how to obtain maximum efficiency without becoming vulnerable to cyberthreats? Well, there is an approach, which may be used as a rule of thumb, and it is called **role-based security**.

3 OS-level virtualization, also called zone-based or container-based, employs a mechanism where many user-space "containers" share single OS kernel. Parallels and Proxmox offer examples of such platforms.

4 Depends on hypervisor and type of virtualization.

5 For non-persistent VMs, instant protection is available after including the Light Agent into the VM's image. For persistent VMs, the administrator must deploy LA manually.

6 Vulnerability Assessment/Patch management technology, while being nominally available in Kaspersky Security for Virtualization | Light Agent, is very resource-intensive and, therefore, is not recommended to be employed in virtual environments.

# PARRY ONLY THE INCOMING BLOWS; A ROLE-BASED APPROACH TO SECURITY

Every cyber-menace threatening physical endpoints can also threaten your virtual infrastructure. But what is absolutely necessary for an attacker is a method of penetrating your security perimeter to perform an attack. For example, to infect a working PC, a cybercriminal may need to lure the employee to the malicious website, where infection occurs through exploiting a vulnerability in the victim's browser. But to infect, say, a database server which is hidden deep in the IT infrastructure which may not even have Internet connectivity, some other attack vector must be found. So, if you are sure that the only threats possible are those attacking at file system level, or that the data in question has low value in itself , or you're using strictly policed VDI without access to the Web, you may opt for an agentless solution offering the benefits of instant protection and absence of "instant on gaps".

Table 2: Role-based security approach

| Role | External access | Data* Value | Service** Value | Ext. conditions | Solution (Why certain solution is to be used) |
|---|---|---|---|---|---|
| **Backend database Servers** | No | Low to Med | Medium to High | Regular backups | KSV \| Agentless (short living data, less attack vectors) |
| **Frontend webservers** | Yes | Low | High | Have trust relationships with several backends | KSV \| Light Agent (Exposed to dangers of public access, after successful attack exploitation of trusts is possible) |
| **Limited purpose VDI or virtualized application** | No | Med to High | Med | Highly restricted, no apps installation, no use of removable storage | KSV \| Agentless (predictable environment, less attack vectors) |
| **Desktop replacement VDI** | Yes | Medium | Medium | Personal removable storage in use, privileged users with installation rights | KSV \| Light Agent (The need for higher security is bigger than the need for faster response. more attack vectors due to exposure to public Internet) |
| **Corporative intranet webservers** | Yes | Low to Med | Low to Medium | *External access only from authorized users using hardware tokens | KSV \| Agentless (Little business value of data, very limited exposure to public internet ) |

| Role | External access | Data* Value | Service** Value | Ext. conditions | Solution (Why certain solution is to be used) |
|---|---|---|---|---|---|
| **Client data processing infrastructure** | Yes | High | High | Need for stable, unchanging environment; Application Control w.Default Deny recommended | KSV \| Light Agent (Need for compliance makes additional protection layers an absolute necessity.) |
| **Web developers test infrastructure** | Yes | Low to Med | Med | Linux-based hypervisor and heterogeneous guest VMs | KESB for Linux, KESB for Windows (constantly renewed short-living data, variety of OSes) |

The table given above contains some examples that provide a general understanding of role-based defenses, though it's not a direct recommendation for the roles listed and should not be used as such. Every usage case is unique; there are always more conditions to be taken into account than can be summarized in a single table. However, to make the concept more clear, we'd like to provide the classification for the Data Value and the Service Value in more details:

- **Low Value Data**- This data is usually depersonalized, contains no valuable personal, commercial or governmental secrets, and perhaps short-lived and subject to constant renewal. Its loss or exposure doesn't lead to significant commercial losses and can never cause any reputation damage. A good example would be a working database where transitional data is temporarily stored.
- **Medium Value Data** - This data may contain some personal or commercial information with the exception of data directly connected with finances and personal well-being. It would not contain classified information. Its loss may cause some financial damage to the enterprise. Its exposure may lead to noticeable monetary impact and it may be capable of harming the enterprise's reputation in some non-critical way. Example - data on the customers of an internet retailer.
- **High Value Data** - May contain sensitive personal and/or financial information or commercial secrets that constitute a significant part of enterprise's market advantage. They may also contain classified information. Its loss may result in significant commercial and reputational losses. Its exposure may lead to heavy financial penalties including lawsuits, and irrevocable reputational damage. Example - blueprints of some critical infrastructure or confidential correspondence at executive level.

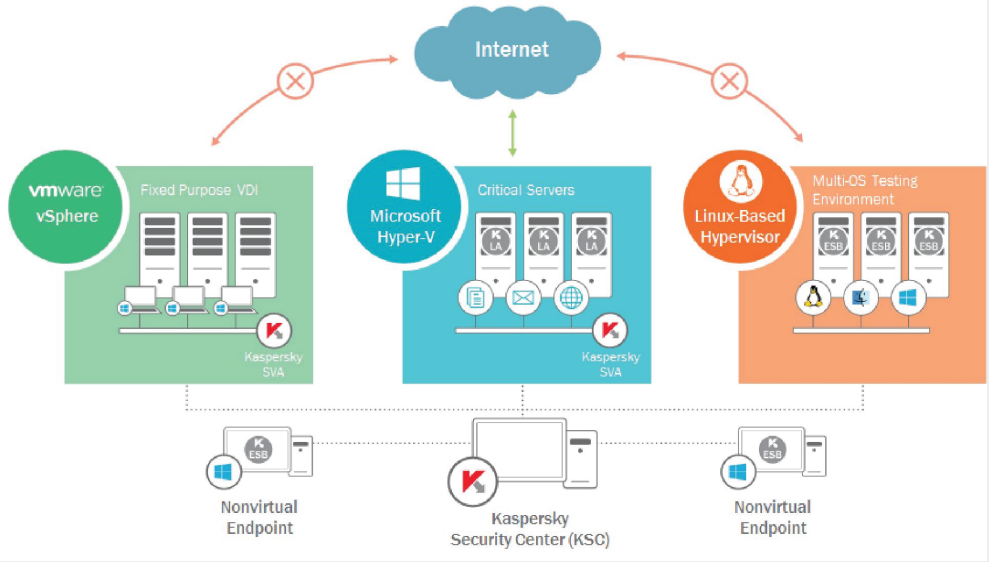
- **Low Value of Service** - No third parties are affected, speed of recovery is of little significance. Little or no financial consequences in case of its malfunctioning. Probability of reputation damage is extremely low. Example - corporate information portal.
- **Medium Value of Service** - Third parties may be affected if the service malfunctions. The loss of such data may lead to noticeable financial damage. Reputational damage is noticeable as well, and it is directly connected to social significance of the service: the more well-known and popular the service (or a product relying on it), the heavier the reputational consequences. The data may be a part of governmental infrastructure but its condition has little influence on national well-being. Expeditious recovery is of primary importance. Example - VDI infrastructure of a systems integrator providing desktop-replacing environment among its services.
- **High Value of Service** - Third parties are almost certainly affected. The service is key element of the business and may be a critical element of third parties businesses as well. Influence on national well-being is possible. Reputational losses are extremely painful and may be irrevocable. Recovery is of utmost importance; failure to perform a successful recovery in shortest time period may result in further dramatic consequences. Example - government video surveillance system infrastructure.

You who know your infrastructure best, so you can best decide what your security is going to look like; the guidelines provided here are just that - a basic methodology for making a decision. But yes, it is quite possible to enhance your resource utilization efficiency and save some money for your company while keeping your virtual infrastructure safe. Remember though, that before deploying any kind of specialized security solution, you should check and adjust basic security settings of your IT network. A properly administered network means less attack vectors for criminals and fewer consequences for you to reap if anything goes wrong.

# EFFICIENCY MEANS INTEGRITY

Efficient resource utilization is fine, but it's nothing without effective control. Certainly you may deploy an agentless solution for your back-ends from one vendor, a light-agent solution for your VDI from another and throw in third-party Application Control for some critical area. As a result you'll have three management consoles, three sets of policies to configure and maintain, and some excessive update traffic to pump through your data channel. Surely it's much better to have everything coming from a single vendor, with all the gauges and controls neatly organized within a single console. All the Kaspersky Security products were designed to be controlled centrally, via Kaspersky Security Center. This means you can manage your virtualized assets from the same console you employ for controlling your physical endpoint security.

Another benefit is centralized updating. There's no need to download the same updates set for every SVA on every hypervisor; they are automatically deployed after being downloaded into KSC storage.




One more distinctive feature of Kaspersky Lab's solutions is their availability for different virtualization platforms. Therefore, you're free to operate a well-protected multi-hypervisor environment – and still enjoy all the controls brought together within the same KSC.

Figure 1: Multi-hypervisor environment may be solidly and efficiently protected

For example, your Active Directory core (Domain Controllers, Domain Name Systems, etc.) may be hosted on Microsoft Hyper-V virtual servers, employ a Cirtix-based VDI and include some database servers running on VMware ESXi. Or, as pictured on the figure above, you may operate mixed environment containing more than one hypervisor platform as well as physical endpoints.

In this case, for the most efficient performance/security balance leading to optimum consolidation ratios:

- Isolated fixed-purpose VDI can be protected by KSV | Agentless
- Server infrastructure which is critical to business and contains valuable data, should be protected by robust security layers of KSV | Light Agent
- The testing environment, featuring Linux hypervisor and a zoo of guest OSes, as well as physical endpoints, is best shielded by Kaspersky Endpoint Security.

In every case, Kaspersky Lab's products provide you with the best protection the industry has to offer - and allow you to choose between the easy deployment and ROI efficiency of KSV | Agentless solution, the robust protection of KSV | LA, or any combination within a single IT infrastructure.

Because Kaspersky Lab can offer customers agentless, light agent and agent-based virtualizations solutions, we are able to make completely objective recommendations to our customers. We do not feel we have to promote any specific technology, but can put forward the best option, or combination of options, for a specific customer environment. And because all our solutions are based on the same powerful anti-malware engine, and all are designed by us as part of a single integrated security platform, we know that whatever you decide will work efficiently to keep your virtual system secure.


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