Practical Guide

VIRTUALIZATION SECURITY

Tips to help you protect your systems and sensitive corporate data

kaspersky.com/business

KASPERSKY lab

CONTENTS

VIRTUALIZATION BENEFITS . . .

For Businesses of All Sizes

In today's competitive environment – with businesses trying to boost efficiency and cut costs – virtualization is no longer the preserve of multinational enterprises and large-scale data centers. Virtualization promises to:

- Run more applications and services – on fewer servers.
- Cut hardware acquisition costs.
- Reduce operational costs related to maintenance, space and energy.

Virtualization is often an important element in the IT department's efforts to meet the business's demand to do more and spend less.

However, whether you're running applications on physical or virtual machines, you still need to guard against the constant increase in the volume and sophistication of malware and other cyberthreats that could jeopardize your day-to-day operations by:

- Disrupting your business processes – and increasing your operational costs.
- Stealing and exposing your confidential business information.
- Compromising the security of your suppliers' and customers' data.
- Destroying the competitive advantage that your business gains from its intellectual property.

MEET MAX, THE INTREPID IT & SECURITY SPECIALIST

As the IT Manager for a business with 150 employees, Max devotes his working life to managing every aspect of the company's IT systems and services – physical, virtual and mobile. He's also responsible for keeping all servers, desktops and mobile devices up and running – plus ensuring sensitive corporate data is safe and secure.

With so many tasks to juggle – and tight budget constraints to comply with – Max is always looking for IT solutions that simplify support, automate everyday tasks and help control costs.

Max's bosses may not totally understand the day-to-day challenges that Max faces – they just know everything has to run smoothly. However, with each passing year, they also realize that the company's ongoing success is increasingly reliant on IT . . . and Max's ability to introduce new technologies and IT services that enable improved business processes, while he also continues to ensure valuable information is protected.

Although the company's IT infrastructure has enabled business-critical processes – that weren't possible in the past – Max is constantly being asked to do more with less. Furthermore, with the growing number of security threats, plus constant battles to avoid service disruptions and downtime, Max is buried in day-to-day routine, and he's got no time left to perfect his IT strategy.

A Message From Max

"For our first virtualization projects, I migrated some of our less important applications to a virtual environment. At that stage, we were keen to delay migration of mission-critical applications."

"This approach meant we gained invaluable experience and built up our confidence levels – before moving our most important business processes and applications to a virtual environment."

"The lessons we learned on those first few projects helped to ensure later projects went really smoothly."

ARE VIRTUAL ENVIRONMENTS MORE SECURE . . . OR LESS SECURE?

It's a myth that virtualized environments are somehow more secure than their physical counterparts. Unfortunately, even though there is absolutely no truth or logic behind this belief, it can lull some organizations into a false sense of security when they consider security requirements for any virtualization projects.

From the point of view of everything that interfaces with or interacts with a virtual machine, the machine "looks" and acts exactly like any physical machine. Generally, the only thing that is aware that the machine is virtual is the hypervisor (plus the IT administration team!).

So it's a simple statement of fact that virtualized environments still have to contend with all of the potential security risks that physical environments have to deal with.

FIREWALLS AREN'T ENOUGH

Just because a virtual machine is behind a firewall – within the organization's data center – doesn't mean it's safe from many different types of threats that can be launched from outside the company perimeter.

Attackers that have already breached the company's security perimeter will regard unprotected virtual machines as easy targets.

USING YOUR EXISTING SECURITY POLICIES

The services and applications that your IT department delivers to the business are obviously important – regardless of whether those services and applications are being run on physical or virtual machines.

If your business has recognized the need to protect applications and data running on physical servers, that same need for security applies to applications or business processes that you run in a virtualized environment.

The majority of the policies that you applied to those applications and processes – when they were running on physical servers or desktops – are still just as valid.

Your first steps toward a secure virtualized environment can be as simple as taking your current security and operational policies – that you already apply to your physical servers and desktops – and replicating them across your new virtualized environment.

However, here's a note of caution – while replicating security policies may make perfect sense, replicating the same security technologies could:

- Introduce security gaps.
- Greatly increase your IT costs.
- Introduce system inefficiencies.

Your choice of virtual machine security technologies will need to be carefully considered. Traditional agent-based security software can bring some highly undesirable side effects.

CYBERCRIMINALS FOCUS ON ATTACKING YOUR WEAK LINKS

With cybercriminals always looking to maximize their ill-gotten gains and minimize the effort necessary to implement their illegal activities, the fact that some businesses fail to apply adequate security measures to their virtual environments has not gone unnoticed.

Criminals recognize that – for many organizations – virtualized components within the corporate IT infrastructure can be the weak link in a business's defenses . . . and can make it easy for criminals to gain access to corporate systems and confidential, highly valuable information.

AGENT-BASED SECURITY SECURITY SOFTWARE

This is basically the same type of package that you would install on a physical machine. In a non-virtualized environment, the full security software agent and anti-malware database are installed on the machine (server or desktop).

Generally, using these agent-based products within a virtualized environment is not a good idea. Each virtual machine will require the full agent and full anti-malware signature database to be installed on it. Therefore, if you have 100 virtual machines running on one virtual host, you'll have 100 instances of the security agent and 100 instances of the malware signature database on that virtual host.

Obviously, this high level of duplication of the antivirus database wastes storage capacity. In addition, with multiple instances of the security application running, performance will suffer – especially in cases where the security software is running intensive processes on multiple virtual machines on the host.

If one of the motivations behind undertaking a virtualization project is doing more with less hardware, anything that adversely affects consolidation ratios will severely handicap your virtualization project's ability to generate a good return on investment.

In addition to wasteful duplication of the security software and databases, agent-based security can also result in phenomena that further degrade performance or lead to potential gaps in security, including:

- Scanning storms.
- Panic attacks.
- Update storms.
- Instant on gaps.

SCANNING STORMS

Because there are multiple instances of the security agent installed on each virtual host, if several – or even all – virtual machines simultaneously start to run a routine security scan, the other applications that are running on that host will be affected. In the event of a virus outbreak, the resulting malware scanning processes could mean that key applications will almost grind to a halt.

These scanning storms can be avoided if you choose a security solution that has been optimized for virtualized environments.

PANIC ATTACKS

IT administrators often set up policies whereby security will tighten up during a virus outbreak – so that scanning processes simultaneously run on all virtual machines and heuristic analysis is set to maximum. Obviously, this leads to each virtual machine consuming high levels of the host's resources – including memory and CPU power – and can severely affect the performance of the host machine.

UPDATE STORMS

With the virtual host storing the anti-malware databases for multiple instances of the security agent, all of those databases will be subject to regular updates. Simultaneous updates of each virtual machine's anti-malware database can severely impact the performance of other applications.

To alleviate this, you may be tempted to stagger the database updates – so that no more than a specified number of virtual machines will update at the same time. However, this approach will mean that the security on some of the virtual machines will lag behind that of other virtual machines on the same host – so some of your virtual machines will be more vulnerable to new or emerging malware and attacks.

Some security products that have been specifically developed for virtualized environments will randomize updates – to minimise the potential for update storms.

INSTANT ON GAPS

Instant on gaps can be a major security risk for agent-based products.

Consider the case of an office worker logging off their virtual desktop at 5:00 p.m. and then logging back on at 8:00 a.m. the next morning. For those 15 hours, their virtual machine has been totally inactive – and that means its antivirus database and the security application won't have received any updates.

Although 15 hours may not seem like a long time, in today's fast moving world, there are a lot of new malware items that can be launched in this relatively short period – and, when it's first powered up in the morning the user's virtual desktop could have no protection against the latest threats.

If the user starts his day with a quick browse across a few Internet sites – before the security software update has completed– his virtual computer could be extremely vulnerable to attacks.

Similarly, when administrators first set up a new virtual machine, the instant on gap will mean the machine is vulnerable – until after the security application and database have been updated.

A Message From Max

"Our initial project was a bit rushed, to say the least. Security was almost an afterthought – so we just used our normal security package on each virtual machine."

"We really thought that we'd benefit from using a security product that we were already familiar with. Then, towards the end of the project, we wondered why we weren't getting anywhere near our predicted consolidation ratios . . . or the cost savings that my boss was expecting!"

AGENTLESS SECURITY SOFTWARE

For VMware®-based virtual environments, vendors are able to offer agentless security products that make use of a special feature in VMware vSphere – to access the file systems in the virtual machines.

Whereas agent-based security products require the full security agent – and its database – to be replicated on every virtual machine on each host, these agentless security applications only need one instance of the anti-malware database and one virtual machine that's dedicated to security . . . in order to protect every virtual machine that is running on that host.

Agentless security products can protect virtual servers and virtual desktops, while having no significant impact on hypervisor performance.

Compared with traditional agent-based security, agentless solutions place much less demand on the host machine's CPU, memory and storage – so IT departments can achieve:

- Higher guest virtual machine densities.
- Higher performance for critical applications and business processes.
- Easy deployment and automatic protection of the newly created virtual machine.
- Higher return on investment.

Furthermore, with only one dedicated security virtual machine, malware scanning storms and security database/application update storms are eliminated. In addition, instant on gaps do not occur.

SMALL FOOTPRINT AGENTS

For Citrix®-based and Microsoft®-based virtual infrastructure, agentless security is not an option. Instead, vendors have developed security solutions that use a combination of a virtual appliance on the virtual host and a small footprint agent – or light agent – on each virtual machine. These light agent solutions can offer a combination of enhanced security and relatively high consolidation ratios.

Light agent solutions often deliver security and management technologies that are not provided by agentless products, including:

- The ability to scan memory – and find memory resident malware.
- Control tools that can be particularly useful in virtual desktop environments.
- Host-based network security – including a firewall and host intrusion prevention system (HIPS).

Even though there is a light agent on each virtual machine, update storms do not occur – as there is only one instance of the security database, which is held within the virtual appliance – and scanning storms are eliminated, because the security virtual appliance automatically randomizes file system scanning.

WORKING OUT WHICH TECHNOLOGY IS BEST FOR YOU

For virtualization security, there's no one size fits all solution. The optimum approach for your organization – and the unique architecture of your IT infrastructure – will depend on a number of factors, including:

- The level of risk you're likely to encounter
- The value of the data that your systems store and process
- The consolidation ratios that you're aiming to achieve
- Your organization's virtual environment – including servers and desktops
- Your choice of virtualization platform – including VMware, Citrix or Microsoft

However there can be extreme cases whereby a traditional agent-based security product may be necessary. In general, security that's optimized for virtual environments is desirable as it will offer significant performance, consolidation and operating cost benefits.

For solutions that are optimized for virtualization, it's a matter of choosing either an agentless solution or a small footprint/light agent security product:

- For VMware-based virtual environments, agentless security can help you to achieve high consolidation ratios and significant ROI increase due to its ease of deployment and simple management.
- Light agent security can deliver an enhanced level of protection. Because agentless solutions are not available for Citrix-based and Microsoft-based virtual infrastructures, light agent products provide the best security solution for these environments.
- A virtualization-aware full agent solution can help in cases where you're using a wider range of guest operating systems including Linux – or you're running a less common hypervisor.

A Message From Max

"Being a one-man IT and security department can have its advantages. A friend – who heads the IT security function in a much larger company – was appalled when his employer's first venture into virtualization was masterminded by the IT operations team, without involving the IT security team."

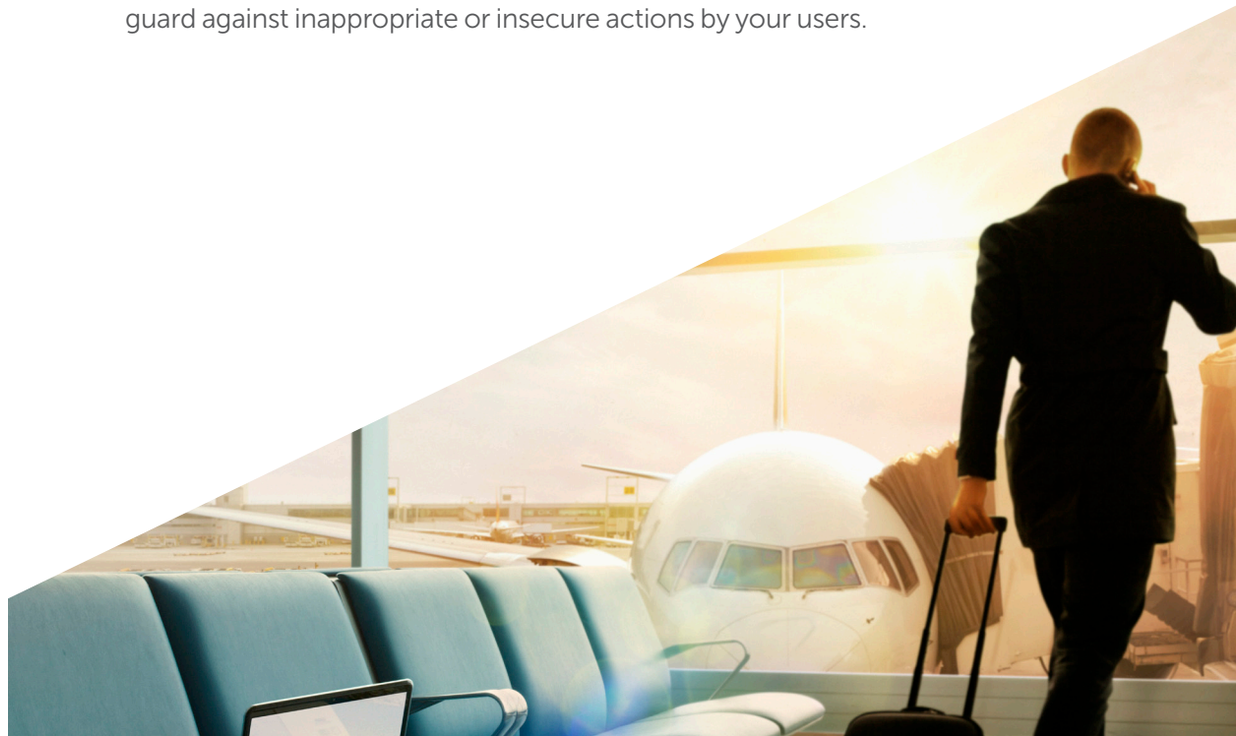
"Having to play catch-up on security – halfway through a project – made for some sleepless nights."

HAVING IT ALL

For some businesses, a mixture of both agentless and light agent security products may be appropriate.

For example, in a tightly controlled data center environment – where servers are performing work that doesn't require them to be constantly connected to the Internet – an agentless security solution may provide more than enough protection.

However, for a virtualized desktop environment – where there's much less control over how the virtual desktops are being used by employees – there may be a valid case for the deeper levels of protection that a light agent security solution can deliver. This is particularly true if your choice of light agent security product includes additional security technologies, such as Application Control, Device Control and Web Control features that can guard against inappropriate or insecure actions by your users.



SECURITY THAT GIVES YOU MORE OPTIONS

Kaspersky Lab has virtual security solutions for a wide range of Windows®-based virtual environments, including:

- VMware.
- Citrix.
- Microsoft.

Kaspersky Lab also has security solutions for environments that use two or more virtual vendors' products.

Kaspersky Lab also gives businesses the ability to choose the security approach that best suits their specific virtual environment:

- Kaspersky Security for Virtualization | Agentless.
- Kaspersky Security for Virtualization | Light Agent.
- Kaspersky Lab's agent-based security solutions.

ONE LICENSE – TWO WORLD-CLASS SECURITY TECHNOLOGIES

When you buy Kaspersky Security for Virtualization, you get access to both:

- Kaspersky Security for Virtualization | Agentless.
- Kaspersky Security for Virtualization | Light Agent.

. . . so you can deploy different security applications to different areas of your IT infrastructure.

You can also choose between per virtual machine or per core licensing – to select the option that is most cost-effective for your business.

KASPERSKY SECURITY FOR VIRTUALIZATION | AGENTLESS

Where as traditional security products require a full security agent to be installed on each of your virtual machines, Kaspersky Security for Virtualization | Agentless allows you to protect every virtual machine on a virtual host – just by installing a single security virtual appliance.

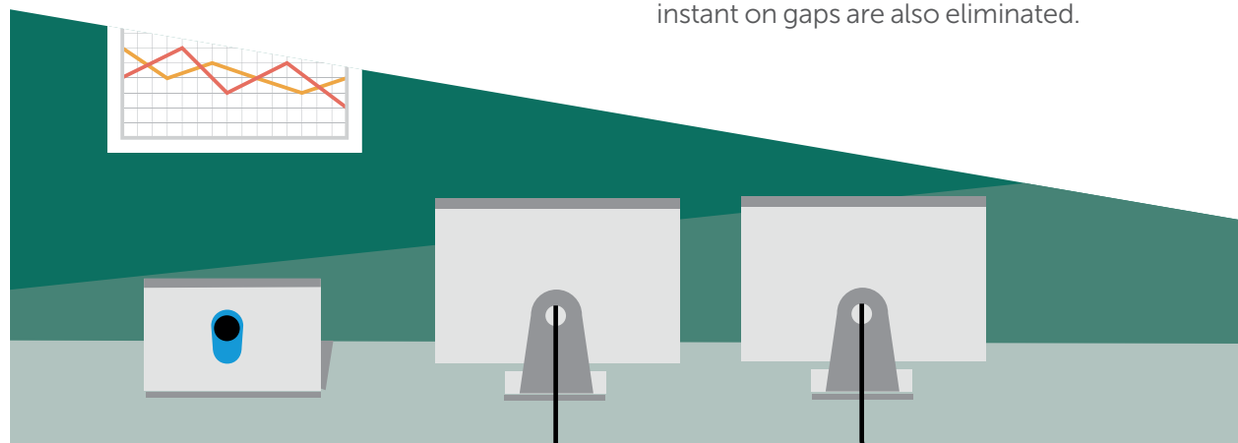
Kaspersky Security for Virtualization | Agentless is the ideal choice for VMware-based projects where you're aiming to achieve good ROI through seamless and non-affecting deployment and steady consolidation ratios – including some data center environments or on servers that aren't constantly accessing the Internet.

Kaspersky Security for Virtualization | Agentless delivers:

- File-level anti-malware protection.
- Network-level protection – using Kaspersky's Network Attack Blocker technology.
- Cloud-assisted, real-time threat data – from the Kaspersky Security Network.

Because Kaspersky Security for Virtualization | Agentless can be deployed without your having to reboot any machines – or put the host server into maintenance mode– it's ideally suited to data centers and businesses that are looking to achieve "five nines" (99.999%) uptime.

Scanning storms, update storms, and instant on gaps are also eliminated.



KASPERSKY SECURITY FOR VIRTUALIZATION | LIGHT AGENT

With Kaspersky Security for Virtualization | Light Agent, one dedicated virtual appliance is installed on the host and a small software agent – called a light agent – is installed on each virtual machine. This offers a greater level of security than is typically achieved by an agentless solution, but still uses far less processing power and storage capacity than a traditional agent-based solution.

Kaspersky Security for Virtualization | Light Agent delivers:

- Advanced anti-malware protection.
- Advanced network-level protection – using, HIPS, firewall and Kaspersky's Network Attack Blocker technology.
- Application Control – to help you manage which applications are allowed to launch.
- Device Control – so you can manage how removable devices are permitted access to your systems.
- Web Control – to help you manage Internet usage and block access to specific types of website.
- Automatic Exploit Prevention (AEP) – to defend against malware that exploits vulnerabilities in your operating system and applications.
- Cloud-assisted, real-time threat data – from the Kaspersky Security Network.

When you deploy Kaspersky Security for Virtualization | Light Agent, there's no need to reboot any machines – or put the host server into maintenance mode – so Kaspersky Lab's light agent solution can help you to make "five nines" (99.999%) uptime a reality.

Again, scanning storms, update storms and instant on gaps are also eliminated.

ONE MANAGEMENT CONSOLE – MULTIPLE BENEFITS

Kaspersky Security for Virtualization includes Kaspersky Security Center – an easy-to-use management interface that lets you configure and control a wide range of Kaspersky Lab's security and systems management technologies, via a single console.

Whether you're using Kaspersky Security for Virtualization | Agentless, Kaspersky Security for Virtualization | Light Agent – or a combination of both applications – you'll be able to control them both from one unified management console, which means:

- If you migrate from VMware to Citrix, Microsoft to VMware or Citrix to Microsoft, you'll still be able to use the same management console.

- Because the same management console also controls Kaspersky Lab's agent-based security solutions – including Kaspersky Endpoint Security for Business and Kaspersky Total Security for Business – Kaspersky Lab makes it easier for you to migrate from physical to virtual environments at the pace that best suits your business.

Kaspersky Security Center helps you to manage Kaspersky Lab's security and systems management technologies across physical, virtual and mobile devices.

KASPERSKY ENDPOINT SECURITY FOR BUSINESS

For those rare instances when you need to run a full security agent on your virtual machines, you can choose from one of the tiers of Kaspersky Endpoint Security for Business – or our ultimate business security solution, Kaspersky Total Security for Business.

MAX'S STRATEGY TIPS – FOR SECURE VIRTUALIZATION

"The cost savings and operational benefits offered by virtualization can be very compelling – but there are a few things to bear in mind when you're putting together your project strategy . . . if you're going to maintain the security of your company's systems and information."

- Make sure security is considered at the very outset of any potential virtualization project. If your company's virtualization roll-out plans don't include security – that's an incomplete and insecure strategy.
- When you're assessing which virtualization platform is right for your project, make sure you also consider how that platform will affect your security options.
- Consider starting by replicating all of the security policies you currently apply to your physical IT infrastructure – to your new virtual environment.
- Assess each project – and its security requirements – before setting targets for performance and consolidation ratios.

- Carefully review the available security technologies, including:
  - Agent-based.
  - Agentless.
  - Light Agent.
- Choose a security solution that will accommodate changes in the virtualization software that you're running. If you're using VMware now, but you later move to Citrix, you'll want to avoid the expense of having to buy new security software licenses and also having to retrain on the use of a new security package.
- Assess how well your chosen virtualization security software is integrated with other security technologies. Higher levels of integration will mean a much lower load on your IT administration resources.
- To ease the burden on your IT security and IT administration teams, choose a security solution that enables you to control multiple security technologies and functions from a single management console.

LEARN MORE ABOUT VIRTUALIZATION SECURITY

Kaspersky Lab is the world's largest privately held vendor of endpoint protection solutions. The company is ranked among the world's top four vendors of security solutions for endpoint users.* Throughout its more than 17-year history Kaspersky Lab has remained an innovator in IT security and provides effective digital security solutions for large enterprises, SMBs and consumers. Kaspersky Lab, with its holding company registered in the United Kingdom, currently operates in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide.

Call Kaspersky Lab today at 866-563-3099 or email us at corporatesales@kaspersky.com.

Visit kaspersky.com/business to find out more or have a look at our additional content around Virtualization Security.

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2013. The rating was published in the IDC report "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (IDC #250210, August 2014). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2013.

KASPERSKY lab THE POWER OF PROTECTION