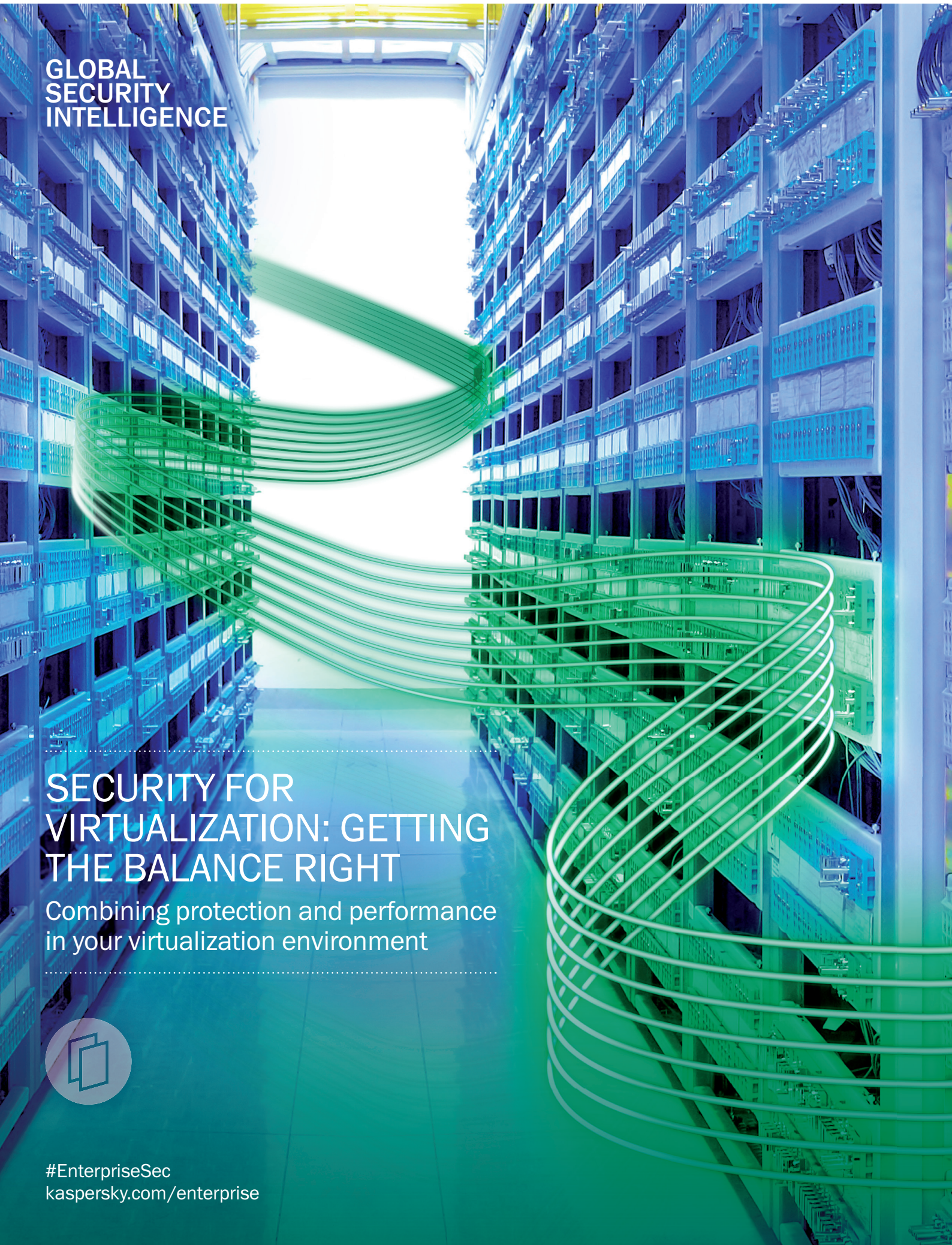
KASPERSKY lab

GLOBAL SECURITY INTELLIGENCE



SECURITY FOR VIRTUALIZATION: GETTING THE BALANCE RIGHT

Combining protection and performance in your virtualization environment

#EnterpriseSec
kaspersky.com/enterprise

CONTENTS

INTRODUCTION

VIRTUALIZATION HAS TRANSFORMED THE CORPORATE IT ENVIRONMENT

Organisations globally are subject to greater levels of cyber-threat than ever before. It is vital that the IT infrastructure, both physical and virtual, is fully and effectively secured.

The addition of security functionality into any IT system, is going to involve some level of resource consumption. The aim is always to maximise protection whilst minimising performance impact – balancing security and systems efficiency.

This issue is particularly critical for virtual infrastructures. The greatest benefits that virtualization can bring to the corporate table are the performance efficiency and optimisation gains, and the associated cost savings. Installing resource-heavy security solutions on virtual systems can erode these benefits, undermining the original business case for investment in virtualization.

Selecting the correct security solution for a specific virtual environment is not straightforward. This paper aims to provide guidance on identifying the right security approach for your virtual environment, achieved through the correct balance between security and performance. Because the 'correct balance' will be slightly different for every organisation, there is no single definitive answer. But key to this balance lies primarily in the presence, and type, of security agent at the virtual endpoint; the balance between the ability to enable security functions at the endpoint and the amount of valuable processing space taken up in doing so.

We'll discuss three security approaches to virtual endpoint security, their effect on achieving the best ROI, and offer some advice on how to achieve the best performance versus security balance for your virtual, as well as physical and mobile environments.

The three approaches are:
- Agent-based
- Agentless
- Light Agent

Understanding these approaches, and their strengths and weaknesses, is essential to finding the right balance for you.

VIRTUALIZATION

IN A RECENT SURVEY BY GARTNER, DESKTOP VIRTUALIZATION IN AT LEAST ONE FORM WAS FOUND TO BE IN USE BY SLIGHTLY MORE THAN 60% OF RESPONDENTS.[1]

GARTNER FORECASTS A 13.14% TOTAL GROWTH IN THE WORLDWIDE ENTERPRISE MARKET FOR HOSTED VIRTUAL DESKTOPS DURING 2014, WITH ONGOING GROWTH STILL AS HIGH AS 7.38% IN 2017.[2]

Virtualizing servers and desktops can bring enormous business benefits.

Some key examples include:

- Cost containment: Virtualization reduces the overall hardware footprint, reducing hardware expenditures, floor space, power consumption, management requirements, etc.
- Speed: Virtualization increases the speed of IT by delivering new capacity on demand. This agility can ultimately result in greater competitiveness of the entire business.
- Stability: Simpler, standardised, redundant systems lead to greater resiliency, ensure better system availability, enabling employees to be more productive whenever and wherever they work.
- Centralised management: Virtual systems can be created instantly, and managed and configured centrally reducing administrative and support costs.

In short, businesses embrace virtualization because it optimises IT efficiency, and that in turn reduces costs.

1 Market Trends: Desktop Virtualization, 2013, 10 October 2013 – Gartner, Inc.
2 Forecast: Enterprise Software Markets, Worldwide, 2010 – 2017, Q413 Update – Gartner, Inc.

VIRTUAL SECURITY: THE RISKS

IN EARLY 2011, KASPERSKY WAS TRACKING 35 MILLION THREATS IN ITS MASTER DATABASE. ONE YEAR LATER THAT DATABASE HAS NEARLY DOUBLED TO OVER 67 MILLION. KASPERSKY NOW SEES AN AVERAGE OF 315,000 NEW THREATS EVERY DAY.

ARE VIRTUAL MACHINES (VMs) INHERENTLY MORE SECURE THAN PHYSICAL MACHINES?

The answer is no. While there may be a handful of attack vectors to which VMs are less prone – ransomeware threats to virtual servers, for example – VMs are just as vulnerable to most forms of malware, including malicious email attachments, drive-by-downloads, botnet Trojans, networks worms and even targeted 'spear-phishing' attacks.

These threats persist while the virtual system is active and in use.

According to the National Institute of Standards and Technology:

"Virtualization adds layers of technology, which can increase the security management burden by necessitating additional security controls. Combining many systems onto a single physical computer can cause a larger impact if a security compromise occurs. Further, virtualization systems, which rely on a shared resource infrastructure, create a dangerous attack vector in which a single compromised VM (virtual machine) impacts the entire virtual infrastructure."[3]

Additional risks to the virtual environment include:

- Network infection: Malware, killed on a non-persistent VM when it is taken down, will probably have already infected other machines via the virtual network. Given the speeds possible in these networks, the infection can spread like wildfire, infecting new machines as they are spun up.
- Storage infection: Malware can also spread through infecting the data stores that VMs access.
- One VM can be used to 'eavesdrop' on another VM's traffic.
- Malware creators are also broadening their attack strategy by writing code that targets both physical and virtual machines.

MALWARE THREATS CONTINUE TO RISE AT AN ALARMING RATE

In early 2011, Kaspersky was tracking 35 million threats in its master database. One year later that database has nearly doubled to over 67 million. Kaspersky Lab now sees an average of 315,000 new threats every day.

The weapons of cyber-warfare directed at organisations, from hit-and-run strikes on the supply-chain to 'watering-hole attacks', combining spear phishing and drive-by downloads, are growing ever elaborate. No one is immune.

"Any organisation can become a victim. Every organisation holds data that could be of value to cybercriminals, or they can be used as a 'stepping-stones' to reach other companies"
David Emm of the Kaspersky GReAT (Global Research and Analysis) Team[4]

In short, business has never before been in such need of IT systems protection, both in the physical and the virtual world.

Because virtualization technology has been embraced by business, and particularly enterprise organisations, who offer rich pickings, cybercriminals have every reason to raise their game and focus even more of their efforts on infiltrating, infecting and manipulating virtual systems.

3 Guide to Security for Full Virtualization Technologies, National Institute of Standards & Technology, 2011
4 Kaspersky Security Bulletin 2013

VIRTUAL SECURITY: THE BALANCE

Organisations invest in virtualization to increase efficiency and save costs. The optimised performance that delivers these cost savings must be preserved. And one element which takes up some level of systems capacity is security software.

It's a fact that some anti-virus implementations can bog down virtual infrastructure, reducing consolidation ratios and compromising the ROI. One security benchmark whitepaper suggests that certain antivirus configurations can create an up to 40% reduction in capacity on the virtual desktop host.[5]

But it is also a fact that virtual systems are vulnerable to cyber-threats and must be protected. Whatever the costs of implementing security, they are likely to be vastly out-weighed by the costs of a major security breach – which could be enough, in terms of reputation damage alone, to threaten the entire organisation.

The myth that virtual environments are innately secure and don't require protection has now largely been exploded. This is partly thanks to the dedicated work of cybercriminals worldwide, who have long recognised and are now exploiting the fresh arena of opportunity provided by virtualized systems (Morcut, aka Crisis, the first Trojan targeting VMs, was identified way back in 2012).

But there remains a reluctance to commit to, and invest in, security for virtualized systems at the same level as for physical systems.

What reasons lie behind the apparent paradox of 'fast to virtualize, slow to secure'? Gartner puts the crux of the matter in a nutshell:

"Securing the [virtual] platform doesn't come without a cost, not just for security software licencing, but also in the form of a potential performance impact. Anti-malware scanning products can significantly reduce platform capacity, especially if the products are not optimally configured for the environment." [6]

The primary justification for investment in virtualization is the increased performance efficiencies and cost savings achievable. If platform capacity is compromised through inappropriately designed and configured security software, that justification is undermined.

To date, the options available for securing VMs from malware have all involved an unhappy compromise between protection, performance, and management.

So, what can the prudent IT manager do to maintain an efficient yet well-protected virtual environment – while still realizing the full business benefits of virtualization? Where does the balance lie and how can it be delivered?

The answer lies in how the security system is designed, whether its architecture is designed in response to the specific constraints of virtual environments, and particularly the existence and functionality of a security agent at the virtual endpoint.

Let's now examine the three approaches – agent-based, agentless and light agent security.

5 Phase 5 – Antivirus and best practices on VDI V1, January 2013, Project Virtual Reality Check (VRC)
6 Know the Security Implications of Adopting Hosted Virtual Desktops, 8 April 2013 – Gartner, Inc.

THE AGENT-BASED OPTION

One possible approach is to use a traditional, agent-based, security solution. This involves loading a full copy of the antivirus software onto each VM, exactly as happens with most physical endpoint security solutions.

While this approach can provide a reasonably high level of security, there are typically steep costs in terms of resources and performance levels in deploying software designed for physical environments across a shared resource.

THE ADVANTAGES

- Where a legacy physical security system is extended to the virtual environment, there are the benefits of operational familiarity, and those of not having to initiate a new procurement process.
- Economies of scale and efficiency savings may be achieved by running a single security system across both physical and virtual environments.
- Organisations with very few VMs, and no plans to employ more, may not view the financial investment in virtualization-specific security software as justified.

THE LIMITATIONS

Compromised performance

As the antivirus software and signature database is loaded onto each VM, virtual systems performance can become severely compromised. Duplication of signature databases and redundant file scanning unnecessarily consumes valuable system resources, and these and other underlying redundancies negatively impact memory, storage, and CPU availability, increasing resource utilisation so that consolidation ratios are reduced.

Resource Contention and AV-storms

With each virtual endpoint agent undertaking all security tasks independently, resource contention becomes an issue.

Symptoms include:

- **Scanning storms** – when multiple VMs begin scheduled scans simultaneously, the processing power of the host machine can be drained, resulting in host utilisation and performance issues (and even potentially bringing the host to a grinding halt).
- **Update storms** – as with scanning storms, these may occur when all VMs with local signature database attempt to download and install updates simultaneously.

Security gaps

VMs can be easily taken off line and go dormant for long intervals. When they are brought back online (awakened), the VM may have security gaps, such as unpatched software vulnerabilities and outdated virus signature databases, creating a 'window of vulnerability' ripe for exploitation by cybercriminals.

Incompatibility

Virtual and physical machines differ in critical ways – the use of non-persistent disks, for example and the live VM migration process. Standard anti-malware, designed for physical endpoints, tends not to make allowance for virtual as well as machine characteristics, and so can cause unexpected lags and glitches, or even fail to run at all.

Incompatibility is not inevitable. Kaspersky's Endpoint Security for Business solution was designed with an understanding that there are organisations that will choose to run the same agent-based solution over both physical and virtual infrastructures. As a result, Kaspersky Endpoint Security for Business is entirely capable of operating smoothly and effectively in virtualized environments, and specific adjustments designed to optimize virtual systems performance make Kaspersky Endpoint Security for Business a serious contender where an agent-based solution is preferred.

THE BALANCE

An agent-based option tips the balance firmly against performance efficiency, reducing VM density and impacting on the ROI. While comparatively effective security may be achieved through an agent-based approach, this is at a resource cost which most organisations employing virtualization technology would consider prohibitive.

THE AGENTLESS OPTION

Traditional security software agents are just too resource-heavy and inflexible for VM environments. What if virtual systems security could be implemented without needing an endpoint agent at all?

This is an option, if the security system is integrated tightly with the virtualization platform, and can use functionality built into the platform to communicate with individual VMs.

A single separate virtual appliance can then be used to provide anti-malware protection for all VMs

THE ADVANTAGES

- By removing all scanning processing from the individual VM, the overall memory footprint becomes very light, extending the physical hardware capabilities and increasing consolidation density.
- There is no longer a window of vulnerability when a new machine is created, as the virtual security appliance is continuously updating itself.
- As only the virtual security appliance undertakes virus checks and receives updates from the security vendor, AV storms are easily avoided and I/O consumption limited.

THE LIMITATIONS

This agentless approach, while driving better ROI, has a number of limitations.

Platforms supported

The agentless approach is currently only possible in VMware environments, where the vShield endpoint facility has been developed with this in mind. However, vShield has its own limitations, which in turn limit the levels of security which can be implemented. Critically, vShield provides the security solution with VM access at file systems level only.

Narrower protection

Without full access to individual VM activity and data, through some form of agent, endpoint protection and controls cannot be deployed.

Modern agent-based anti-malware software should include layered security modules such as application control, web filtering, host based intrusion prevention (HIPS), personal firewall and more, all of which require some form of endpoint agent.

Of course, any security system is only as good as the threat intelligence that informs it and the anti-malware engine that protects it, so the best possible anti-malware security foundation is critical to any security system – agent based or not.

But, if the ability to provide a multi-layered approach through deployment these robust tools is absent, the remaining anti-malware detection engine needs to be as powerful and intelligence-driven as possible.

No anti-malware engine can, however, compete with the security levels possible when VM memory and processes can be accessed. Agentless solutions designed for virtual environments have a narrower scope in able to provide traditional anti-malware protection only.

Separate security systems management

At this point in time, most organisations deploying virtualization maintain both physical and virtual environments.

The deployment of two separate security systems, one for virtual and one for physical machines, implies two separate management consoles. Policies must then be deployed separately across the two environments, and reporting has to be merged manually to obtain an overall security picture.

By employing two parallel but separately administered systems, you are potentially increasing costs by doubling administrative overheads, as well as introducing new opportunities for error.

However, this this isn't always the case. The single integrated platform approach to security adopted by Kaspersky means that virtual and physical security solutions are seamlessly integrated and managed together through a single console.

THE BALANCE

There are situations where an agentless solution is the most efficient option. One example would be might be where virtual servers are used for storage and database management activity. For these heavy-duty internal environments, where machine density is paramount and there is very limited threat exposure, the balance moves in favour of optimising performance by adopting an agentless solution.

But the risks must be weighed carefully. And where the anti-malware engine alone is relied upon, the breadth and depth of protection provided by that engine, and the quality of the threat intelligence that informs it, is of course critical.

THE LIGHT AGENT OPTION

Lightweight agent-based security for virtual environments combines the performance benefits of the agentless solution with the multi-layered security approach of the best agent-based security systems.

When is an agent a 'light agent'? When the agent's capabilities are limited to only those functions which must be only at the endpoint. Just as with the agentless approach, a separate virtual security appliance is also installed, and it is this that handles all the heavy work. The 'light agent' installed on the VM takes on the lightest workload possible, so that the impact of its presence on machine performance is kept to an absolute minimum.

THE ADVANTAGES

Multi-layered security

The presence of light agent means that it is now possible to add advanced endpoint security and control features to the solution, including:

Controls

A toolbox of endpoint controls can be brought into play.

- Individual access to specific applications can be blocked, regulated or permitted, massively restricting opportunities for malware infection through unknown or unpatched vulnerabilities, particularly if a 'Default Deny' scenario is in place.
- Malicious or non work related websites can be blocked or regulated – increasing user productivity as well as safety by controlling inappropriate or time-wasting online activity
- The connection of peripherals can be limited or blocked, preventing the upload of malware or the download of corporate data.

Additional security technologies

HIPS (Host Based Intrusion Prevention) – monitoring system as well as network behaviour, and actively protecting against attacks to the VM memory.

A host-based firewall, helping prevent the spread of malware infection by restricting network access at machine level.

A light agent solution is capable of full interaction with cloud assisted protection technologies enabling advanced technologies like AEP (Advanced Exploit Prevention) and BSS (Behavior Stream Signatures). The quality of the anti-malware engine remains paramount, but now virtual security can employ the full armoury of security technologies available to physical IT environments.

Performance efficiency

By employing a separate virtual security appliance, most of the performance efficiencies gained through an agentless solution can be replicated.

- Hypervisor I/O, CPU, and memory usage are all minimised. As a single virtual appliance, rather than every VM, handles updates, and AV storms are avoided. If the single appliance is continuously updating, 'vulnerability windows' at machine level are also minimised – and up-to-date protection is instantly applied.

  In the case of Kaspersky Security for Virtualization, this continuous update process, providing instant threat protection with the help of the cloud-enabled Kaspersky Security Network, is particularly intensive. So the centralisation of this process is critical.

- Cache technologies can be implemented – the verdict of a file scanned once can be made available to all VMs across the host, avoiding superfluous re-scanning. The result is a significant reduction in both scanning time and resource consumption.

THE LIMITATIONS

There is still an agent

A light agent will always, by definition, have a greater footprint than no agent at all.

Separate security systems management

Most virtual security solutions require a separate console from the rest of the security solution. However, this does not have to be the case. And here we would draw your attention to Kaspersky's unique single platform architecture.

Kaspersky's Security for Virtualization is built on the endpoint security for Business single platform, together with our physical security solutions.

This means that physical and virtual security, though they may be separate solutions designed for optimised performance in different environments, are managed together through a single console. Joint policies can be created and deployed, and joint reporting generated. There is little or no additional administrative burden, and all the benefits of being able to view the security posture of the entire IT environment though a 'single pane of glass'.

THE BALANCE

Light agent solutions are able to fine-tune the balance between performance and protection to achieve the 'best of both worlds'. The presence of an agent allows advanced security and control features to be deployed at the virtual endpoint, while a separate security appliance takes on all the tasks which can be centralised, avoiding duplication and minimising performance impact.

An efficiently designed light agent solution will generally be the most attractive option where advanced security and performance need to be finely balanced.

CONCLUSION

Business recognises the attractive value proposition that virtualization presents, and the dangers presented by an ever-evolving threat environment. However, implementing the wrong security system can significantly impact on your virtual systems performance, and on the extent to which you are truly protected.

The ideal security solution overcomes the failings of legacy protection solutions with an approach that mirrors that of virtualization itself – flexible, adaptable, and capable of delivering a significant ongoing ROI by providing outstanding protection without sacrificing performance.

Through implementing Kaspersky Security for Virtualization, you can achieve that balance. By providing the flexibility to implement any combination of light agent, agentless and indeed agent-based applications, Kaspersky Security for Virtualization offers the protection of our 'best of breed' anti-malware engine, the optimised performance benefits of efficient, fine-tuned virtualization-specific design, and a single integrated management approach to all your security needs.

As acknowledged global experts in IT security, Kaspersky's R&D teams have created a flexible solution delivering the performance benefits you need, while keeping your virtual environment fully secure, supported by the best threat intelligence ecosystem in the world.

The Kaspersky Security Network, together with our world-renowned Threat Research and Global Research and Analysis Teams (GReAT), gives us the broadest view of millions of threats from every corner of the world. This intelligence allows us to see and often predict security incidents, helping enterprises achieve better protection and a more pro-active stance on IT security. We focus our efforts on solving global IT security challenges – from critical infrastructure protection, enterprise mobility and secure virtualization to fraud prevention and security intelligence services.

Kaspersky never stops anticipating and preventing IT security threats – reducing enterprise risk today and in the increasingly complex future.

About Kaspersky Lab

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 16-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 300 million users worldwide.

Learn more at kaspersky.com/enterprise

* The company was rated fourth in the IDC rating Worldwide Endpoint Security Revenue by Vendor, 2012. The rating was published in the IDC report "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares (IDC #242618, August 2013). The report ranked software vendors according to earnings from sales of endpoint security solutions in 2012.