SECURITY SNAPSHOT

FACT V. FICTION IN THE WORLD OF VIRTUALIZATION SECURITY

KASPERSKY lab

WHAT ARE THE RISKS TO VIRTUAL ENVIRONMENTS?

2x businesses pay more than twice as much to recover from a security breach if a virtual infrastructure is involved.[1]

42% think that virtual environments are safer than physical ones.[2]

HOW DOES SECURITY AFFECT THE VIRTUAL ENVIRONMENT?

89% say that replacing a traditional security software with one built specifically for virtualization created a positive impact on the performance of their virtual machines.[3]

34% aren't aware of the performance benefits such solutions provide.[4]

HOW CONCERNED SHOULD YOU BE ABOUT SECURITY IN YOUR VIRTUAL ENVIRONMENT?

53% are highly concerned about the security of virtualized environments.[5]

27% have deployed a security solution specifically designed for virtual environments.[6]

1. Global IT Security Risks Survey 2015
2. Kaspersky Lab's Security of Virtual Infrastructure: IT Security Risks Special Report Series
3. Global IT Security Risks Survey 2015
4. Kaspersky Lab's Security of Virtual Infrastructure: IT Security Risks Special Report Series
5. IT Security Risks Survey (2015), Global Report, B2B International
6. Kaspersky Lab's Security of Virtual Infrastructure: IT Security Risks Special Report Series

FINDING THE RIGHT BALANCE IN VIRTUALIZATION

Going virtual is not just a trend anymore. It's a business practice. In fact, **77% of organizations with more than 250 employees are now using some form of virtualized infrastructure.**[7]

The benefits of using a virtualized solution are enormous, including cost containment, the speed that comes with delivering capacity on demand, the stability of simpler, standardized systems, and the efficiency of centralized management.

But the risks are enormous, too. **Data breaches that involve virtual environments are over two times more costly** on average than those that do not, with the figures standing at **$34K/$74K** for SMBs and **$454K/$942K** for enterprises.[8] And since virtual machines are often the least protected areas of IT infrastructure, businesses who don't have a security solution in place open themselves up to very costly attacks; this may result in lost business opportunities, temporary loss of access to business critical information, and damage to a company's reputation.

With these considerations in mind, it is essential that organizations maximize protection while minimizing performance impact in order to strike the right balance between security and systems efficiency. Finding that balance will help your business to reap the rewards that a virtualized infrastructure brings with minimal drain on resources.

7. Kaspersky Lab's Security of Virtual Infrastructure: IT Security Risks Special Report Series
8. Global IT Security Risks Survey 2015

CHOOSING THE RIGHT VIRTUAL SOLUTION

When planning the deployment of new workstations—or updates of existing machines—many companies consider purchasing a number of VDI-farm servers instead of the customary desktops and notebooks. Building a new server infrastructure may be expensive, but the high initial expenditure can be recouped within 3-4 years. With lower deployment and maintenance costs, energy savings and a higher degree of manageability, you can achieve the right equilibrium of lower overall expenses and a higher level of security for your organization's sensitive data.

Do your research.
A virtualization security solution must have, at the minimum, a high detection rate and the ability to spot suspicious activity right away. In addition, it should have a low impact on resources and be architecturally built to minimize impact on performance. Only a solution specifically built for the virtualized environment can encompass all of these attributes.

Choose a quality security solution.
A high quality security solution will be able to apply policies when under attack, ensuring that the system recognizes the potential malicious activity and counteracts the issue.

Implement a customized security solution.
Security solutions that are purpose-built for a virtualized environment have numerous advantages, such as centralized management and reporting, easy installation and management and multi-layered protection. This allows you to manage both physical and virtual machines in a similar way from the same console. In addition, there should be no compromise between security and virtual machine performance. The security should be on par with physical systems, but without the performance costs.

Know Your Options

In order to identify the right security for your environment, you need to understand the options that are available to you. There are three major approaches for virtualized environments:

Agent-Based
A security agent is installed on every virtual machine. While many conventional agent-based security solutions are virtual-aware and provide excellent protection, they consume significant resources and very quickly become counter-productive when scaling in virtual environments.

TAKEAWAY:
Has many security features, but is a bit hungry on resources.

Agentless
This is a separate virtual machine (VM) on a physical server that protects all other VMs via a special virtualization platform interface. With agentless virtual security, consolidation ratios are kept high. Also, this solution is extremely simple and fast to deploy and manage. The drawbacks are simple. It is for VMware environments only and, having been authored by a virtual vendor, it lacks some of the advanced security functionality.

TAKEAWAY:
Is light on resources, but offers limited functionality and platform support.

Light Agent
This is the best of both worlds approach that combines security dedicated to a virtual environment together with small software agents. It means that advanced capabilities are available for each virtual machine, while keeping the security profile continually updated.

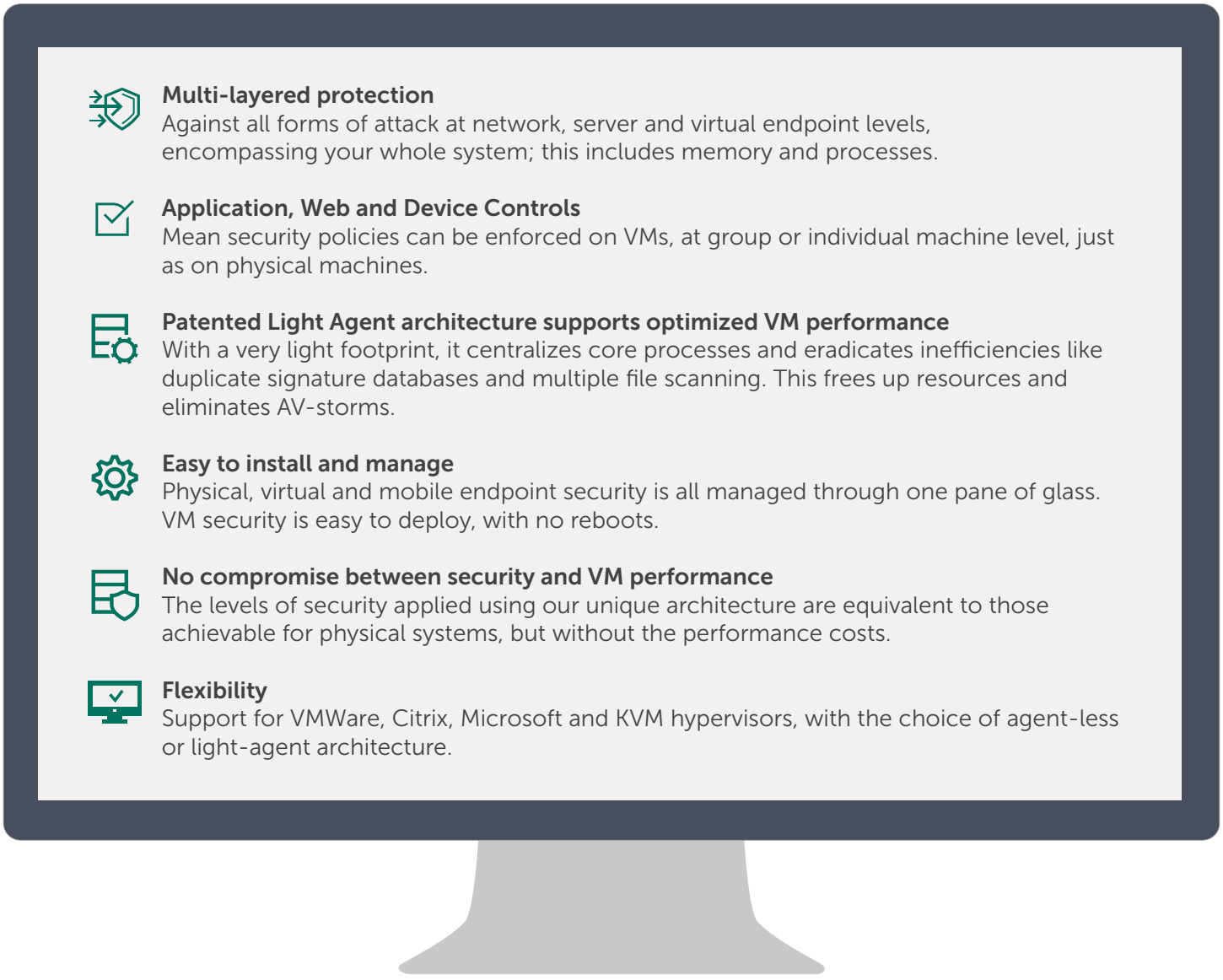
TAKEAWAY:
Has a better feature set than agentless, while still having a low impact on performance.

KASPERSKY SECURITY FOR VIRTUALIZATION

Kaspersky Security for Virtualization (KSV) offers the flexibility to implement any combination of light agent and agentless applications. Kaspersky Endpoint Security for Business (KESB) can be implemented for agent-based needs.

Because KSV has been developed specifically for virtual machines, it helps businesses to maintain high virtualization density and high performance, resulting in an improved return on investment. Instead of having to install a full security agent on every virtual machine, KSV offers a more efficient way to protect your virtualized environment, placing less load on your processors, memory, storage and I/O.

Advantages of the KSV Solution:



Multi-layered protection
Against all forms of attack at network, server and virtual endpoint levels, encompassing your whole system; this includes memory and processes.

Application, Web and Device Controls
Mean security policies can be enforced on VMs, at group or individual machine level, just as on physical machines.

Patented Light Agent architecture supports optimized VM performance
With a very light footprint, it centralizes core processes and eradicates inefficiencies like duplicate signature databases and multiple file scanning. This frees up resources and eliminates AV-storms.

Easy to install and manage
Physical, virtual and mobile endpoint security is all managed through one pane of glass. VM security is easy to deploy, with no reboots.

No compromise between security and VM performance
The levels of security applied using our unique architecture are equivalent to those achievable for physical systems, but without the performance costs.

Flexibility
Support for VMWare, Citrix, Microsoft and KVM hypervisors, with the choice of agent-less or light-agent architecture.

TRY KASPERSKY LAB

Discover how Kaspersky Lab's premium security can protect your business from malware and cybercrime with a no-obligation trial. Register today to download full product versions and evaluate how successfully they protect your IT infrastructure, endpoints and confidential business data.

Get Your Free Trial Today >

JOIN THE CONVERSATION


Like us on Facebook


Follow us on Twitter


Join us on LinkedIn


Watch us on YouTube

Review Our Blog

ABOUT KASPERSKY LAB

Kaspersky Lab is one of the world's fastest-growing cybersecurity companies and the largest that is privately-owned. The company is ranked among the world's top four vendors of security solutions for endpoint users (IDC, 2014). Since 1997, Kaspersky Lab has been an innovator in cybersecurity and provides effective digital security solutions and threat intelligence for large enterprises, SMBs and consumers. Kaspersky Lab is an international company, operating in almost 200 countries and territories across the globe, providing protection for over 400 million users worldwide. Learn more at usa.kaspersky.com.

Contact Kaspersky Lab today to learn more about Kaspersky Endpoint Security for Business and our other IT security solutions and services:

usa.kaspersky.com/business-security

(866) 563-3099

corporatesales@kaspersky.com

KASPERSKY lab

THE POWER OF PROTECTION