▶ VIRTUALIZATION SECURITY IS NOT AN OXYMORON

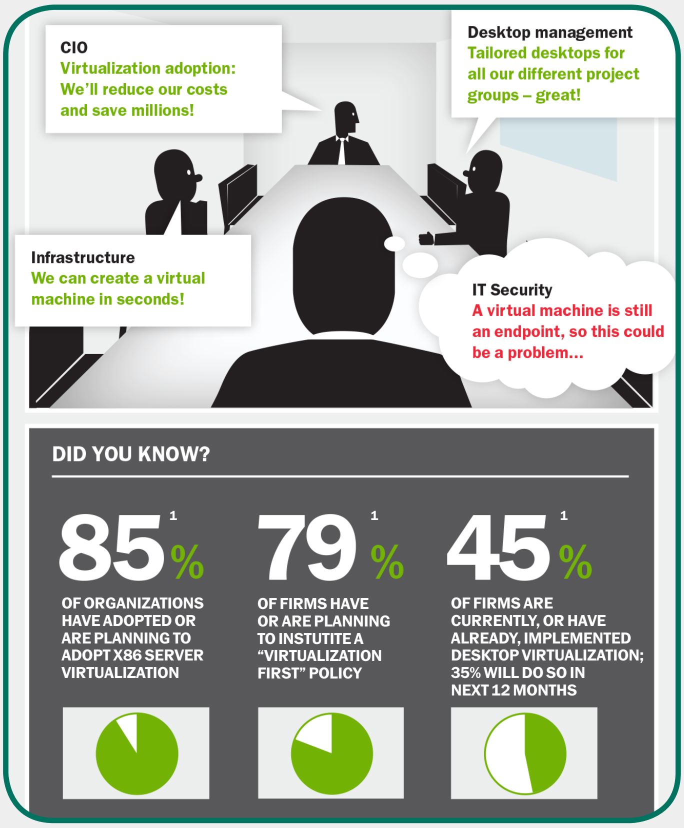
With Kaspersky, now you can.
kaspersky.com/business
Be Ready for What's Next

KASPERSKY lab

PREPARING FOR THE VIRTUALIZATION ADVANTAGE

Widely acknowledged and celebrated, the business benefits of virtualization include energy savings, improved server provisioning, easy application deployment, faster disaster recovery, decreased hardware costs, minimized space requirements, and centralized management oversight.[1]

It's not surprising that the vast majority of corporate technology decision makers surveyed report that they have adopted server virtualization and Virtual Desktop Infrastructure (VDI) or have plans to implement it within the next year.[2] Based on the statistics alone, it's clear that virtualization isn't just for high-tech companies anymore. It's now standard operating procedure for all types of organizations with widespread e-suite support.


CIO
Virtualization adoption: We'll reduce our costs and save millions!
Desktop management
Tailored desktops for all our different project groups – great!
Infrastructure
We can create a virtual machine in seconds!
IT Security
A virtual machine is still an endpoint, so this could be a problem...

DID YOU KNOW?

85%[1] OF ORGANIZATIONS HAVE ADOPTED OR ARE PLANNING TO ADOPT X86 SERVER VIRTUALIZATION

79%[1] OF FIRMS HAVE OR ARE PLANNING TO INSTUTITE A "VIRTUALIZATION FIRST" POLICY

45%[1] OF FIRMS ARE CURRENTLY, OR HAVE ALREADY, IMPLEMENTED DESKTOP VIRTUALIZATION; 35% WILL DO SO IN NEXT 12 MONTHS

[3]

Unfortunately, the convenience of virtualization comes at a security cost that's not so widely acknowledged. Like it or not, joining the wonderful world of virtualization exposes your organization to a wide array of new cybersecurity threats. Of the same businesses surveyed by Forrester, the focus–or lack of focus–on cybersecurity is troubling:

- 53% are not securing their virtual infrastructure
- 27% believe that the security risks in a virtual environment are lower or significantly lower than those for physical infrastructure
- Only 17% of North American companies (18% in Europe) have implemented agentless security for their virtual infrastructure[4]

[1] "Top 10 benefits of server virtualization," InfoWorld, November 11, 2011 (http://www.infoworld.com/d/virtualization/top-10-benefits-server-virtualization-177828?page=0,0)
[3] The CISO's Guide to Virtualization Security, Forrester Research, Inc., January 2012
[2&4] Survey conducted by independent research company O+K for Kaspersky Lab, Q1 2012

VIRTUALIZATION 101

Warning: The following information is unnecessary for anyone with an IT background, but it may be helpful for explaining virtualization to non-techy folks who sign the checks for security expenditures in your organization.

Virtualization is the simulation of software and/or a hardware platform that other software runs on. This simulated environment is a virtual machine (VM). In full virtualization, one or more operating systems (OS) and their applications are run on top of the virtual hardware – each running as a "guest" on the host. These guests are managed by a hypervisor, which controls the flow of instructions between the guests and the physical hardware. The hypervisor isolates the guests so that each guest only has access to its own resources.

WHY VIRTUALIZATION?

In traditional physical environments, servers typically run at around 20% of capacity, often with multiple servers wasting power and capacity, while taking up expensive floor space. Virtualizing servers and desktops can eliminate this waste and result in significant business benefits, including the following:

- Cost containment: reduces the overall hardware footprint as well as hardware costs and floor space, power consumption and management requirements.
- Improved server provisioning: Increases the speed of IT by delivering new capacity on demand to make the whole business more agile and competitive.
- Stability: With a virtual machine completely detached from the hardware, it means greater resiliency, reduced downtime, and better system availability, which in turn enables greater productivity.
- Centralized management: Although virtualization is a complex technology that requires skilled deployment and maintenance, it introduces additional tools that allow you to manage systems centrally, ultimately reducing administrative and support costs.

> Virtualization is all about maximizing your investment through optimizing your IT infrastructure. If your anti-malware solution requires that both software and a signature database be installed on each of your virtual machines, the object of the exercise is partly defeated — your protection is compromising your productivity.

SECURITY CHALLENGES

So while the business benefits are clear, the risks are less well documented and understood, which makes selecting the right virtual-aware anti-malware solution even more important. With so much confidential data floating around, it's critical for businesses to protect all their virtual servers, their machines and the information they process and store.

As John Sawyer from influential technology site Tech Center points out, "In the end, they're all servers — and someone somewhere is going to want to break into them." [5]

Performance, protection and resource issues arise from traditional agent-based anti-malware solutions operating in virtual environments. The options for securing virtual machines from malware have all involved an unhappy a compromise between protection and performance or management, performance or management. Some of the risks are already present in physical environments (and extend into a virtual environment), while some are unique to virtualization.

Virtualization is all about maximizing your investment through optimizing your IT infrastructure. If your anti-malware solution requires that both software and a signature database be installed on each of your virtual machines, the object of the exercise is partly defeated — your protection is compromising your productivity.

There is a pervasive myth that virtual machines are inherently more secure than physical machines. The truth is rather different. According to the National Institute of Standards and Technology, "Virtualization adds layers of technology, which can increase the security management burden… Combining many systems onto a single physical computer can cause a larger impact if a security compromise occurs. Further, virtualization systems…create a dangerous attack vector in which a single compromised virtual machine impacts the entire virtual infrastructure." [6]

A virus in one virtual machine can infect data stores that other virtual machines use, spreading infection and compromising additional systems and data. One virtual machine can be used to "eavesdrop" on another's traffic. Cyber-gangs are targeting businesses. Malware creators are now writing code that targets both physical and virtual machines.

Some malware is designed to survive the "tear-down" of a non-persistent virtual machine, allowing the malware to "return" when the virtual machine is re-commissioned.

While virtualization is ultimately beneficial for companies — and is often seen as the best way to expand networks, improve efficiency and optimize data security — IT managers are now facing a whole new set of challenges. Due to the speed and ease of creating virtual machines, users on a network have the capability and the technology to create their own machines without the IT administrator's knowledge.

Ironically, businesses that have implemented virtualization to eliminate server sprawl are now at risk from VM sprawl, which makes IT staff work hard to control and audit your virtualized activities.

[5] Tech Insight: Keeping Server Vtirtualization Secure, John Sawyer on Darkreading.com, May 2009

[6] NIST: Guide to security for full virtualization technologies 2. Kaspersky Lab research, Q1 2012

DID YOU KNOW?

70,000 NEW THREATS A DAY!

Proliferation of threats is increasing (e.g., Zeus malware, which can be purchased online)

INSTANT ON GAPS!

Dormant virtual machines brought back online may have security gaps, such as outdated signature databases.

1 IN 14 WEB DOWNLOADS CONTAINS MALWARE!

VM SPRAWL

Virtual machines can be created in minutes, often without the IT department's consent. If you can't see the machines, you can't protect them.

SCANNING STORMS

Simultaneous scans on multiple machines can drain the host's processing power, drastically slowing or even crashing the host machine.

[7]

CAUTIONARY TALES

In February 2011, a terminated IT administrator at a Japanese pharmaceutical company used a service account to access the company's network. Once connected, he deleted 88 virtual servers that contained most of the company's IT infrastructure, tracking system and financial management software.[8]

In August 2012, a malicious Trojan known as "Crisis" or "Morcut" targeted virtual machines and intercepted financial data in widespread attack that affected journalists, activists and financial institutions.[9]

As the prevalence of virtualization grows, so does the frequency of cyberattacks on virtual machines. Quite simply, the bad guys go where they can steal the most money and data without being discovered. "Viruses targeting virtual machines (VM) are growing in numbers and will soon be the dominant force in the world of [cybercrime]."[10]

[7] NIST: Guide to security for full virtualization technologies 2. Kaspersky Lab research, Q1 2012

[8] "The CISO's Guide to Virtualization Security," Forrester Research, January 2012.

[9] "Crisis Trojan Makes Its Way onto Virtual Machines," ThreatPost, August 2012 http://threatpost.com/crisis-trojan-makes-its-way-virtual-machines-082112/76936

[10] "'VM-aware' viruses on the rise," ComputerWeekly.com, October 2012, http://www.computerweekly.com/news/2240169662/VM-aware-viruses-on-the-rise

A SMART SECURITY SOLUTION

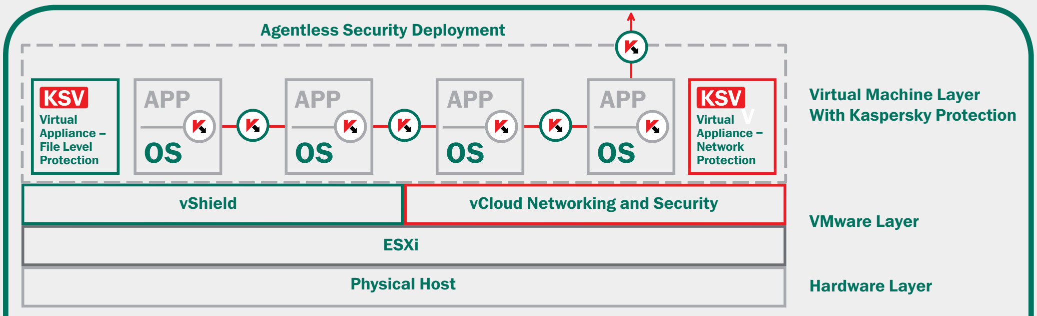
Many of the traditional, agent-based anti-malware products are not well suited to virtualized environments. Virtualization is all about maximizing your investment through optimizing your IT infrastructure. If your anti-malware solution requires that both software and a signature database be installed on each of your virtual machines, the object of the exercise is partly defeated — your protection is compromising your productivity.

And security needs to cover your entire virtual configuration too — not just endpoints, but servers and particularly virtual networks.

Kaspersky Security for Virtualization (KSV) provides agentless, award-winning protection and network security for VMware®-based virtual environments. KSV goes far beyond simple anti-malware with Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) modules to stop network attacks. Created in close partnership with VMware, KSV is designed to support all VMware technologies. As an agentless solution, Kaspersky Security for Virtualization protects your virtual infrastructure— machines, servers and data centers — more efficiently. KSV is straightforward, straightforward and flexible and includes advanced management features that simplify security across all your endpoints.

With Kaspersky Security for Virtualization, you can benefit from superior protection — for all of your virtual machines — while also improving your system utilization rates, reducing the burden on your IT administration and security personnel and increasing your overall return on investment (ROI).

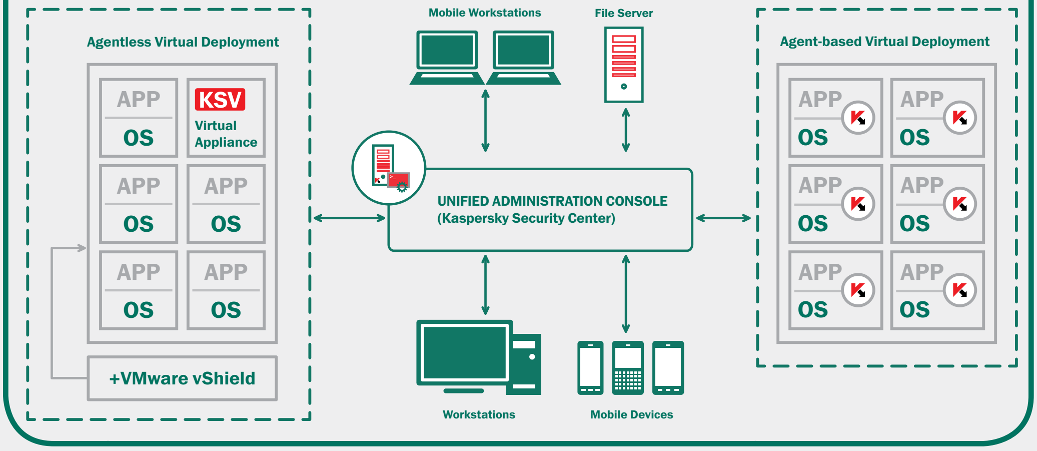
> “With Kaspersky Security for Virtualization, you can benefit from superior protection — for all of your virtual machines — while also improving your system utilization rates, reducing the burden on your IT administration and security personnel and increasing your overall return on investment (ROI).”


Agentless Security Deployment
KSV
Virtual Appliance – File Level Protection
APP
OS
APP
OS
APP
OS
APP
OS
KSV
Virtual Appliance – Network Protection
Virtual Machine Layer With Kaspersky Protection
vShield
vCloud Networking and Security
VMware Layer
ESXi
Physical Host
Hardware Layer

Kaspersky machine and network protection interfaces directly with your VMware environment.

SINGLE PLATFORM ARCHITECTURE

Kaspersky solutions, including Kaspersky Security for Virtualization, are all designed specifically to work seamlessly together and built in-house from the same codebase, using a single platform architecture. This means no gaps, conflicts or inefficient overlaps in your IT security. Instead, an efficient, fully integrated security platform delivers outstanding protection that is easy to manage and highly cost–effective.



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 www.kaspersky.com.

* 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.

Call Kaspersky today at 866-563-3099 or email us at **corporatesales@kaspersky.com**, to learn more about Kaspersky Endpoint Security for Business.

www.kaspersky.com/business

SEE IT. CONTROL IT. PROTECT IT.
With Kaspersky, now you can.

© 2014 Kaspersky Lab ZAO. All rights reserved. Registered trademarks and service marks are the property of their respective owners.