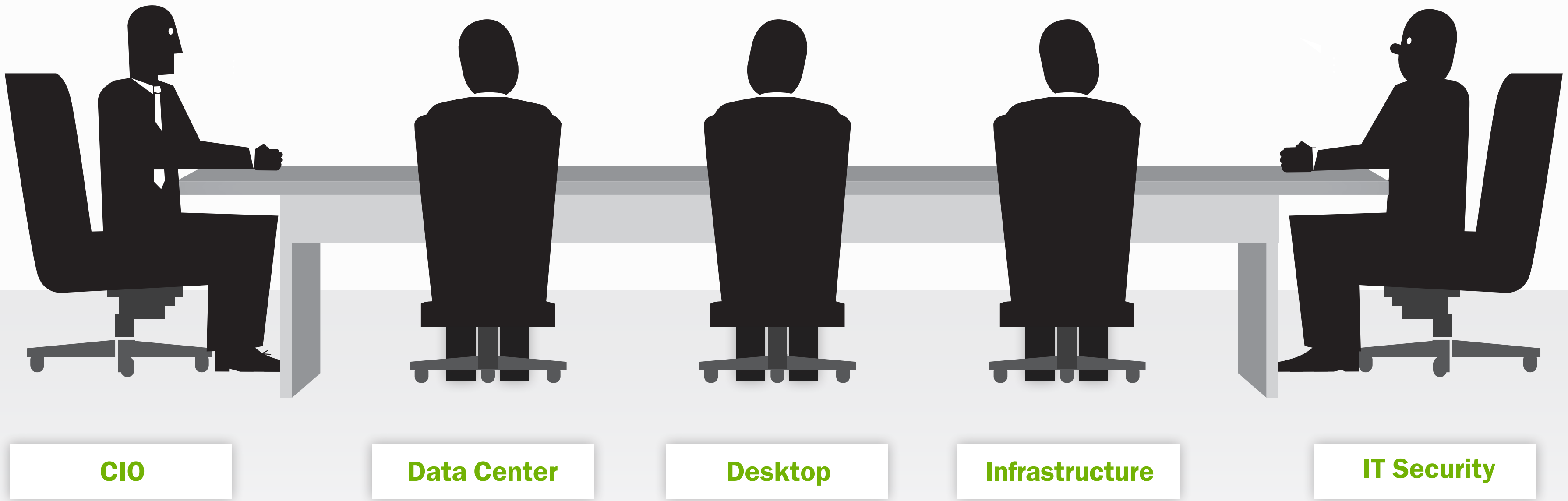
SECURITY FOR VIRTUALIZATION

The challenge, the solution, and how to get the business on board



in partnership with vmware®

kaspersky.com/bereaday

KASPERSKY lab

VIRTUALIZATION
THE STORY SO FAR

1

Few of us would dispute that virtualization makes good business sense.

So how does virtualization work?

It is the simulation of software and/or a hardware platform, which 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.

Similarly, in desktop virtualization a single PC “runs” more than one OS instance, by running multiple virtual machines off a server.

The bottom-line benefits of 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.

Eliminating this by virtualizing servers and desktops can bring enormous business benefits:

Cost containment: reduces the overall hardware footprint, lowers hardware costs, floor space, power consumption and management requirements.

Performance: Increases the speed of IT by delivering new capacity on demand to make the whole business more agile and competitive.

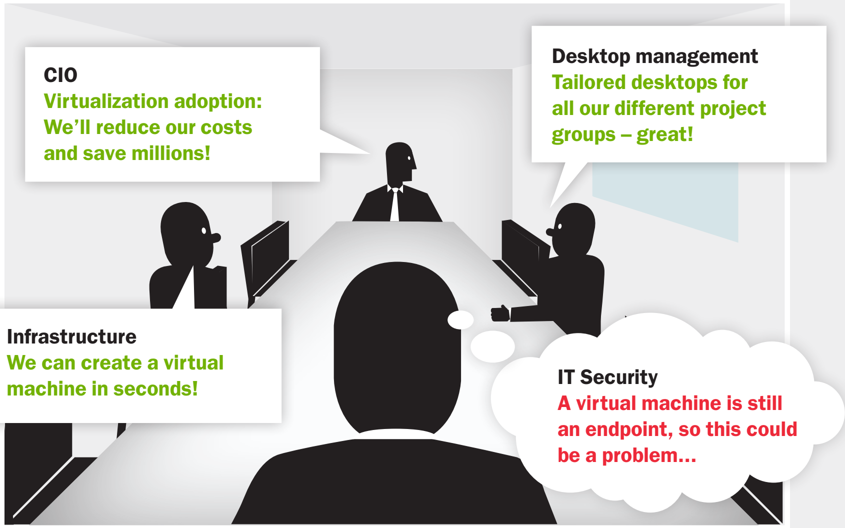
Stability: Simpler, standardized systems mean greater resiliency and better system availability, which in turn enables greater productivity.

Centralized management: Virtual systems can be created instantly, and managed and configured centrally, reducing administrative and support costs.

A note of caution

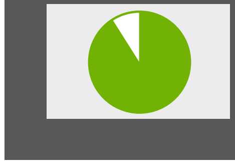
However, our view – and that of leading analysts – is that in the rush to implement virtualization, security has come a poor second.

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.

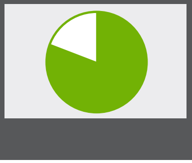

CIO
Virtualization adoption: We’ll reduce our costs and save millions!
Desktop management
Tailored desktops for all our different project groups – great!
Infrastructure
We can create a virtual machine in seconds!
IT Security
A virtual machine is still an endpoint, so this could be a problem…

DID YOU KNOW?

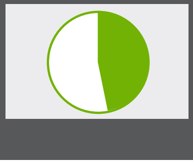
[1]85% OF ORGANIZATIONS HAVE ADOPTED OR ARE PLANNING TO ADOPT X86 SERVER VIRTUALIZATION



[1]79% OF FIRMS HAVE OR ARE PLANNING TO INSTITUTE A “VIRTUALIZATION FIRST” POLICY



[2]45% OF FIRMS ARE CURRENTLY, OR HAVE ALREADY, IMPLEMENTED DESKTOP VIRTUALIZATION; 35% WILL IN THE NEXT 12 MONTHS



The real problem is virtualization may NOT be your project, but if you’re tasked with IT security, it’s still your risk… ▶

[1] The CISO’s Guide to Virtualization Security, Forrester Research, Inc., January 2012 [2] Survey conducted by independent research company O+K for Kaspersky Lab, Q1 2012

VIRTUALIZATION
THE RISKS

2

So, what are the real risks? Some are already present in physical environments (and extend into a virtual environment), while some are unique to virtualization…

Virtualization – more secure than physical?

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."[1]

That's not all

- Infection 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 it 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 knowing about it.

Ironically, businesses that implemented virtualization to eliminate server sprawl are now at risk from VM sprawl, which makes it harder to control and audit the machines connecting to the network.

This is more complex than I thought. What we've got in place today won't serve us well tomorrow…
And, I need to make sure the data center team appreciate the full extent of the risks…
What are my options in terms of solving this?
I need to help them see the bigger picture, so they'll understand my recommendations…

DID YOU KNOW?

70,000 NEW THREATS A DAY!
Proliferation of threats is increasing e.g. Zeus malware, which can be purchased online.[2]

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

1 IN 14 WEB DOWNLOADS CONTAIN MALWARE! [2]

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

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

…it's time for a quick analysis of what makes for a viable approach ▶

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

SECURITY FOR VIRTUALIZATION
WHAT ARE THE OPTIONS?

3

While you may be clear about the right security approach for virtualization, many IT professionals don't realise the complexities involved and potential risks, which can jeopardize a virtualization project. For clarity, here are the available options – and our recommended approach.

Option 1 – No security

This is not an option! Virtual machines are still endpoints, and need to be protected.

Option 2 – Agent-based

While a full copy of anti-malware software on each virtual machine can provide robust protection, there's a steep cost in deploying duplicate software across a shared resource. The underlying resource requirement negatively impacts memory, storage and CPU availability, reducing hardware utilization and reducing performance.

Agent-based anti-malware, particularly in virtual desktops, can hamper ROI as it impedes the performance of the guest, limits the density of the virtual cluster and introduces unnecessary risk.

Option 3 – Agentless

An agentless security solution provides anti-malware protection to many virtual machines. This improves performance by offloading the anti-malware processing from all the virtual machines, reducing memory footprint, extending physical hardware capabilities and increasing consolidation ratios (density).

This approach drives better ROI, but can create its own problems:

Reduced protection

Solutions designed for virtual environments may not include layered protection modules such as application control, web filtering, host intrusion protection and personal firewall.

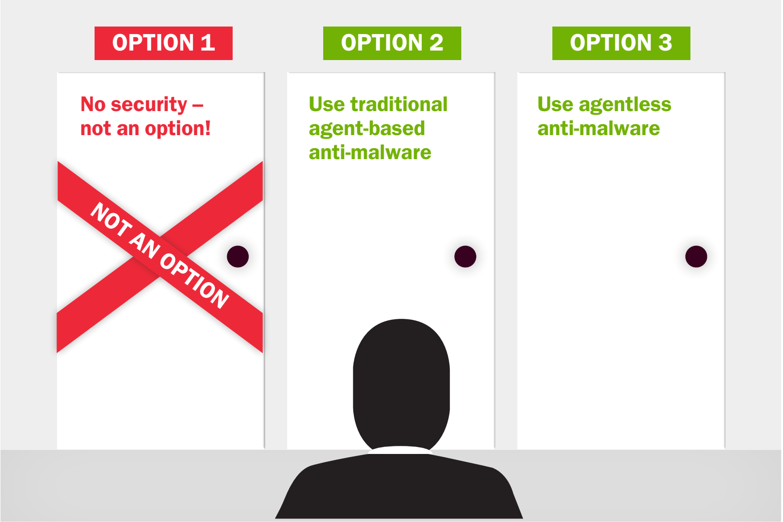
If these tools are absent, the incumbent anti-malware detection engine should be the best available to compensate for the lack of additional protection layers.

Sometimes critical systems also require agent-based anti-malware applications. This creates a mixture of both protection methods that must be maintained, increasing administrative costs.

Physical and virtual system management

Most companies that have deployed virtualization also maintain physical environments.

Today this requires multiple management consoles as both types of systems must be managed and maintained separately, doubling overheads and increasing cost.


OPTION 1
No security – not an option!
NOT AN OPTION
OPTION 2
Use traditional agent-based anti-malware
OPTION 3
Use agentless anti-malware

THE PROS AND CONS

Agent-based

Pros:
Robust security.

Cons:
Can soak up system resources and therefore reduce performance and consolidation ratios.

Agentless

Pros:
Light on system resources.

Cons:
Some options in the market have reduced security capability and lower detection rates, as well as time-consuming multiple management consoles.

But, at Kaspersky, we are giving you another option….

SECURITY FOR VIRTUALIZATION
THE KASPERSKY OPTION

vmware READY

4

No compromise on security, no compromise on performance. Kaspersky Security for Virtualization gives you the right balance.

When you can see it, you can manage it

Imagine having one clear view of your whole environment, from data center to desktop.

It would give you the visibility you need to manage threats; the agility and flexibility to respond faster to malware, and to the changing needs of the business.

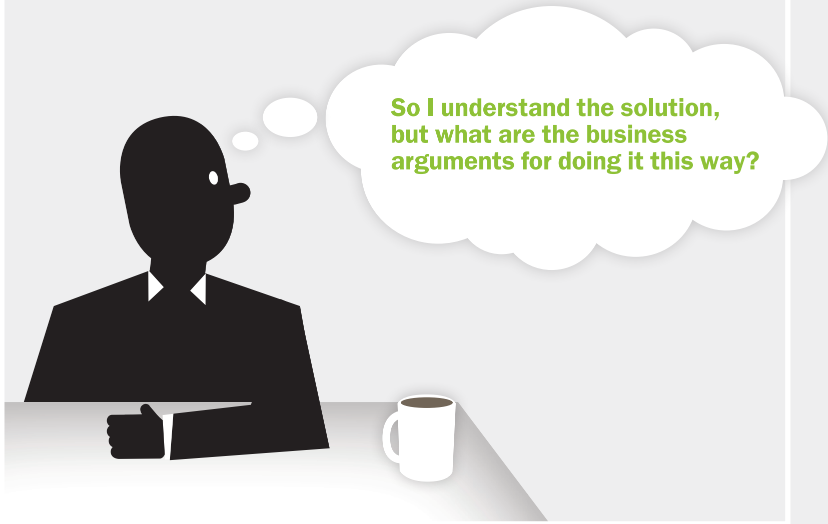
And it would give you a solid platform to build out your virtualization program, without the need for – or the cost of – separate management consoles.

That's exactly what Kaspersky Security for Virtualization (an agentless system that supports VMware vSphere) gives you. Managed by Kaspersky Security Center 9.0, it provides IT administrators with a single-pane view of all protected machines (whether virtual or physical).

IT professionals benefit from easy management. Protection status, security events and reports are presented clearly and intuitively.

Kaspersky Security Center 9.0 (with Kaspersky Security for Virtualization vCenter integration) also gives administrators visibility into the logical and physical structure that resembles familiar VMware management tools.

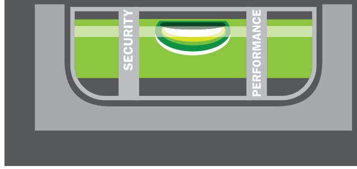
This allows them to effectively manage security operations and take quick actions (such as remediation, diagnostics or forensics).


So I understand the solution, but what are the business arguments for doing it this way?

THE BENEFITS

GET THE RIGHT BALANCE!

An agentless approach to maintain great performance, but with the robust security protection you need.



GREAT VISIBILITY = GREAT SECURITY!

Integrated with Kaspersky Security Center 9.0. See, protect and manage virtual, physical and mobile endpoints, all in one place!

So, what are the business benefits and why should I buy from Kaspersky?

THE KASPERSKY OPTION
THE BUSINESS ARGUMENTS

5

If virtualization security itself is complex, the approach needed is quite clear. As are the business benefits to take to the rest of the organization.

Better visibility = better management
A single management console that gives your business visibility across virtual, physical and mobile endpoints. So when new endpoints (either physical or virtual) are created, you're instantly aware, and instantly covered.

High detection rate = reduced business risk
Kaspersky's exceptionally high detection rates mean that your organization runs less business risk.

Single AV engine = higher density = better virtualization ROI
Kaspersky's agentless approach means a light footprint across your entire IT infrastructure. This means you can keep the performance benefits you hoped for from virtualization.

And why Kaspersky Lab?

One of the fastest growing independent specialist IT security companies in the world
Kaspersky's product strength and innovation has driven continuous rapid growth – as more and more organizations discover the increased protection and ease of management that Kaspersky products bring.

#1 anti-malware OEM provider in the world
Companies such as Microsoft, IBM, Checkpoint, Juniper and others have placed their trust in Kaspersky and have chosen to embed our anti-malware technology inside their own solutions.

Technical superiority

- The greatest number of gold and platinum awards across all testing categories since 2004 from Anti-Malware Test Lab.
- More than 50 passing scores on the rigorous VB100 testing regimen since 2000.
- The Checkmark Platinum Product Award from West Coast Labs.
- Winner of the 2011 Product of the Year award from AV Comparatives for being the only vendor to achieve an Advanced+ rating on every test.

Built from the ground up

- While many security vendors acquire technologies, all of our software code is written by our own developers. This single architecture means Kaspersky customers benefit from exceptional protection and consolidated management.
- Frequent updates, faster response. Kaspersky pioneered the practice of hourly updates and our response times are significantly below industry averages.

Single place to manage virtual, physical and mobile – efficient and consolidated view of your organization.
High detection rate = reduced threat = reduced risk
Kaspersky Security for Virtualization is VMware ready and works perfectly with VMware vShield, providing you with an optimized solution for your virtual environment.
IT Security
Excellent, I have a clear idea of what Kaspersky is saying and what the benefits are for my organization.
KASPERSKY
Single AV engine – low resource requirement, which means you achieve high consolidation ratios (maximum ROI).

KASPERSKY AT A GLANCE

- More than 800 Kaspersky anti-malware experts work around the globe and around the clock to combat cybercrime, analysing over 70,000 threats daily.
- Trusted by businesses and consumers around the world to protect more than 400 million endpoints.
- 100% focused on security solutions.
- A leader in producing award-winning anti-malware technology products.
- Recognized as "A Leader" in the Gartner Magic Quadrant for Endpoint Protection Platforms.[1]

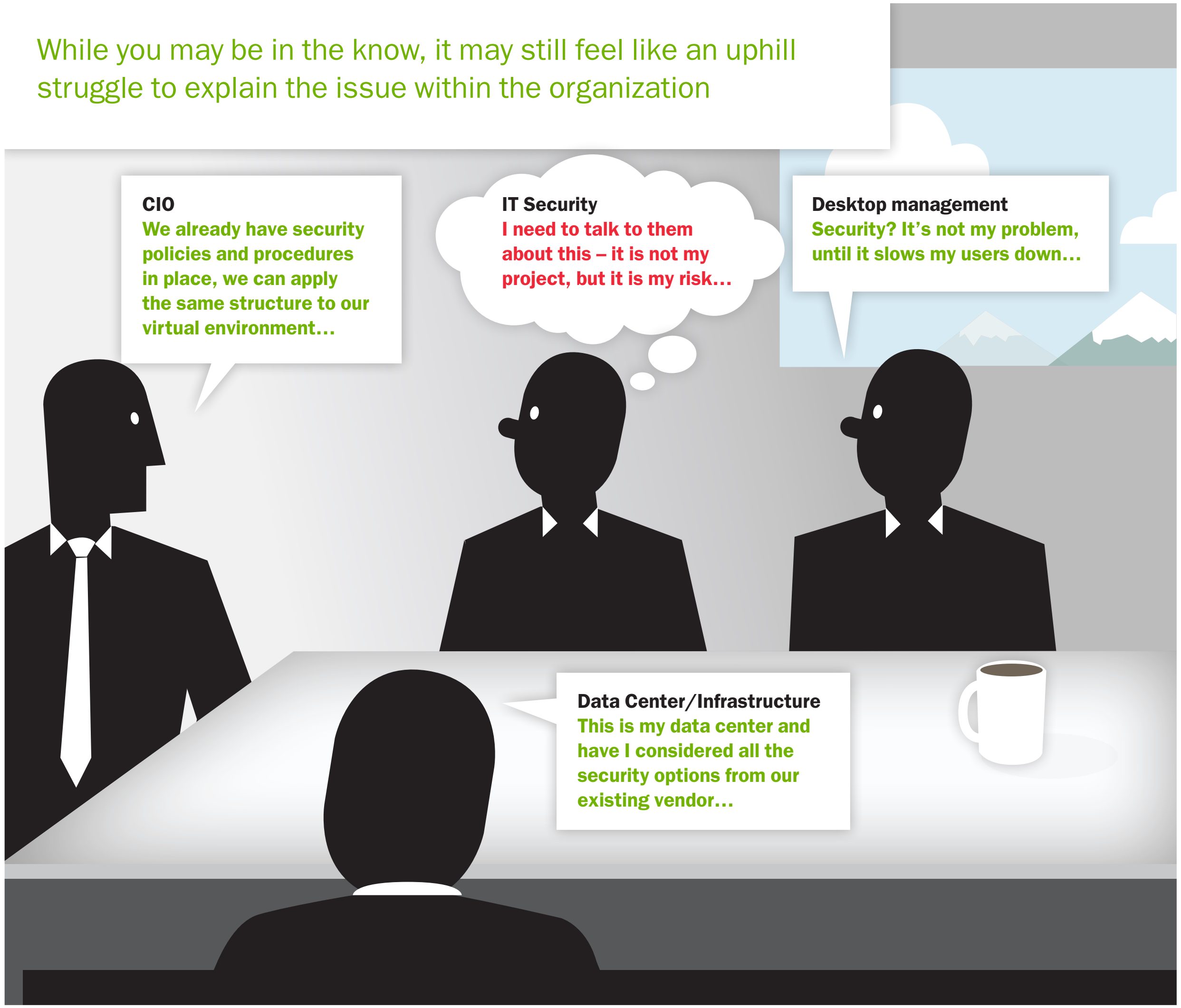
So the approach you should take is clear, but what is the rest of your organization thinking?

[1] Gartner Magic Quadrant for Endpoint Protection Platforms, Jan 2012.

WHAT EVERYONE ELSE IS THINKING

6

While you may be in the know, it may still feel like an uphill struggle to explain the issue within the organization


CIO
We already have security policies and procedures in place, we can apply the same structure to our virtual environment…
IT Security
I need to talk to them about this – it is not my project, but it is my risk…
Desktop management
Security? It's not my problem, until it slows my users down…
Data Center/Infrastructure
This is my data center and have I considered all the security options from our existing vendor…

What the analysts say:

Forrester Research, Inc.
Given the converged nature of virtual environments, security incidents can result in significant damage; therefore, it is critical that security professionals redouble their efforts and make securing their virtual infrastructure a priority.[1]

IDC
There are still a lot of questions about how to approach security on virtualized servers. With most tools, it's hard for IT to even know how many of the VMs on a particular server even have all their patches up to date.[2]

Gartner, Inc.
Migrating server and desktop workloads from physical to virtual does NOT eliminate the need for endpoint protection.[3]

AND SOME USEFUL STATS TOO:

In a recent Kaspersky survey[4], IT professionals revealed…

15% WERE NOT EVEN AWARE OF ANY VIRTUALIZATION SPECIFIC SECURITY SOLUTIONS

44% PERCEIVE THE RISKS IN A VIRTUAL ENVIRONMENT BEING LOWER OR SIGNIFICANTLY LOWER THAN A PHYSICAL ONE

56% BELIEVE IT'S CRUCIAL TO USE VIRTUALIZATION SPECIFIC SECURITY

62% AGREE THAT THE BALANCE OF PERFORMANCE AND SECURITY IS A CRITICAL ISSUE

Ok, I understand the arguments – but how can I help the team to reconsider the options? ▶

[1] The CISO's Guide to Virtualization Security, Forrester Research, Inc., January 2012 [2] Phil Hochmuth, Program Manager for Security Products, IDC [3] Make optimizing security protection in virtualized environments a priority, Gartner, Inc., February 2012
[4] Survey conducted by independent research company O+K for Kaspersky Lab, Q1 2012

TAKING THE CONVERSATION WIDER
WINNING FRIENDS AND INFLUENCING PEOPLE

7

Building your case is key, but how else can you improve security for virtualization? Here's a checklist:

Increase your colleagues' virtualization knowledge

- Spend time with your Enterprise Architecture and Infrastructure & Operations team to grow skills organically.
- Encourage interaction between your team and the virtualization team.
- Staff from managed service or cloud service provider environments often have deep knowledge of securing multi-tenant workloads.

Apply a "zero trust" model to your network architecture

- There is no longer a trusted internal network and an untrusted external network – all network traffic is untrusted.

Provide better visibility and security

- Virtualization-aware technologies give visibility into intra-VM communication.
- Operational data can be leveraged by security and IT operations staff.

Take a "zero trust" approach to privileged identity management

- Managing privileged users is one of the most important duties in a virtual environment.

Ensure users access resources securely regardless of location

- Privileged users should be using two-factor authentication to access and administer the virtual environment.
- Ensure that service accounts aren't permitted to access the environment externally.

Log all traffic so that you can quickly respond and recover

- Put the right tools in place to quickly detect a policy violation or suspicious activity.
- The hypervisor or virtualization management layer has some logging capabilities but it is limited.

Extend your vulnerability management program into your virtual environment

- Server hardening, including patch management and configuration management, is a core element of vulnerability management.

A parting thought:

Many CISOs are not aware of the virtualization security risks, while others are very concerned about their virtual environments but don't have the authority or the influence to enforce policy or implement new security controls.[1]

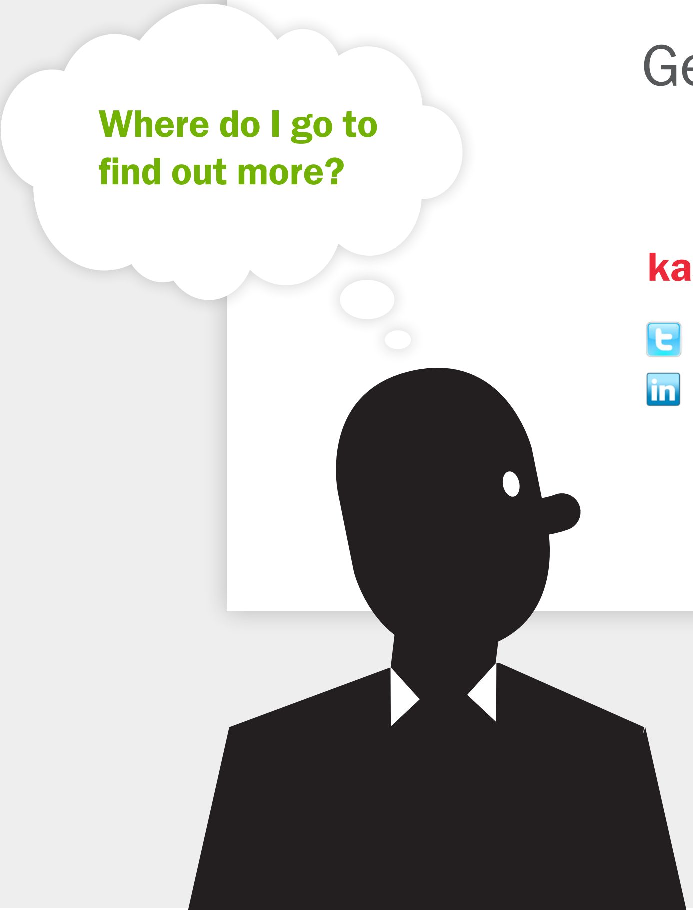
CIO
We need the security guys in at the scoping stage for all virtualization projects…
IT Security
I'm now going to help my organization understand why virtual-aware security is so important…

FOUR SIMPLE STEPS TO GET SECURITY FOR VIRTUALIZATION TAKEN SERIOUSLY THROUGHOUT THE BUSINESS:

1. Put policies and procedures in place
2. Educate the rest of the business
3. Always talk business first, technology second
4. Get out there and network!

Excellent. So where do you go to find out more?

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



SECURITY FOR VIRTUALIZATION

Get the right balance with Kaspersky

kaspersky.com/beready

Twitter.com/kaspersky

LinkedIn Group – IT Security Knowledge Exchange

in partnership with
vmware®

Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings. Gartner research publications consist of the opinions of Gartner's research organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.

KASPERSKY lab