KASPERSKY lab

GLOBAL IT SECURITY RISKS SURVEY 2014 – VIRTUALIZATION

Table of contents

GLOBAL IT SECURITY RISKS: 2014 – VIRTUALIZATION 0
THE MAIN FINDINGS 2
METHODOLOGY 4
MANAGING VIRTUALIZATION 5
VIRTUALIZATION SECURITY IN THE PAST AND FUTURE 6
THE GROWING IMPORTANCE OF VIRTUALIZATION 10
VIRTUALIZATION SECURITY AWARENESS AND IMPLEMENTATION 14
CONCLUSIONS AND RECOMMENDATIONS 17

THE MAIN FINDINGS

Managing Virtualization and Virtualization Security in the Past and Future

Of the almost 4,500 survey respondents worldwide, 14% cited **securing virtualized infrastructure** as one of the top three most important information security priorities for the next 12 months. This was cited most often among Enterprise organizations (with 5,000+ employees), 21% of which selected "securing virtualized infrastructure" as one of their most important security priorities for the next 12 months.

Security concerns were cited by 43% of all survey respondents as "an important barrier to the implementation of virtualized infrastructure, and 41% said they "struggle to manage the security solutions in our virtual environments." 64% agreed that "security should be one of the first considerations when rolling out virtual infrastructure."

The issue of "managing change" was a top concern of 22% of survey respondents. Within this group, 29% (or roughly 6% of all survey respondents) cited **deployment and management of virtualization technology** as a "change" they've been forced to manage over the past year.

The Growing Importance of Virtualization

52% of survey respondents agreed that virtual environments are increasingly forming **a core part of their business IT infrastructure.**

Server virtualization is the most common form of virtual infrastructure, already implemented by 55% of global respondents. An additional 6% plan to adopt server virtualization within the next 12 months, giving a projected total of slightly less than two-thirds of all global businesses.

Virtual Desktop Infrastructure (VDI) has been adopted by 25% of global businesses, with another 10% planning to implement VDI within the next 12 months. An additional 28% responded that they were "interested" in VDI (without specific plans to adopt), giving VDI the highest rate of potential for future growth.

The three **most common functions implemented on virtual infrastructure** are "Email & Communications Applications" (implemented by 42% of virtualization users); "Database Applications" (39%); and "Financial Management & Accounting Applications" (32%).

Certain types of virtualized application usage are expected to grow faster than others. 59% of virtualization users expect to increase the degree of virtualization for Collaboration Platforms within the next 12 months. 55% expect to increase their use of virtualization for

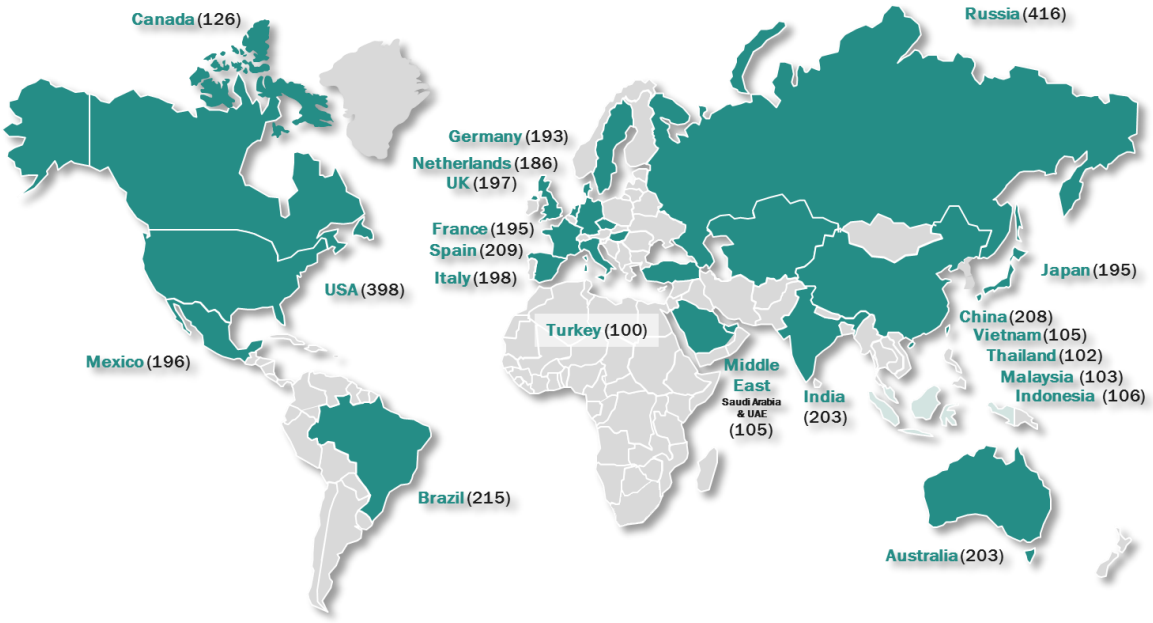
Customer Relationship Management (CRM) applications, and another 55% expect to increase their use of virtualized Test and Development Environments.

Virtualization Security Awareness and Implementation

Despite rising awareness of virtualization security concerns, knowledge of virtualization-specific security technology remains low. Only one out of every three IT security experts expressed a "clear understanding" of light agent and agent-based virtualization security. Only one out of every four expressed a "clear understanding" of agent-less virtualization security.

When measuring attitudes towards virtualization security, 46% of global respondents believe "virtual environments can be adequately protected by conventional security solutions." 36% believe "the security concerns in virtual environments are significantly lower" than in physical environments.

METHODOLOGY

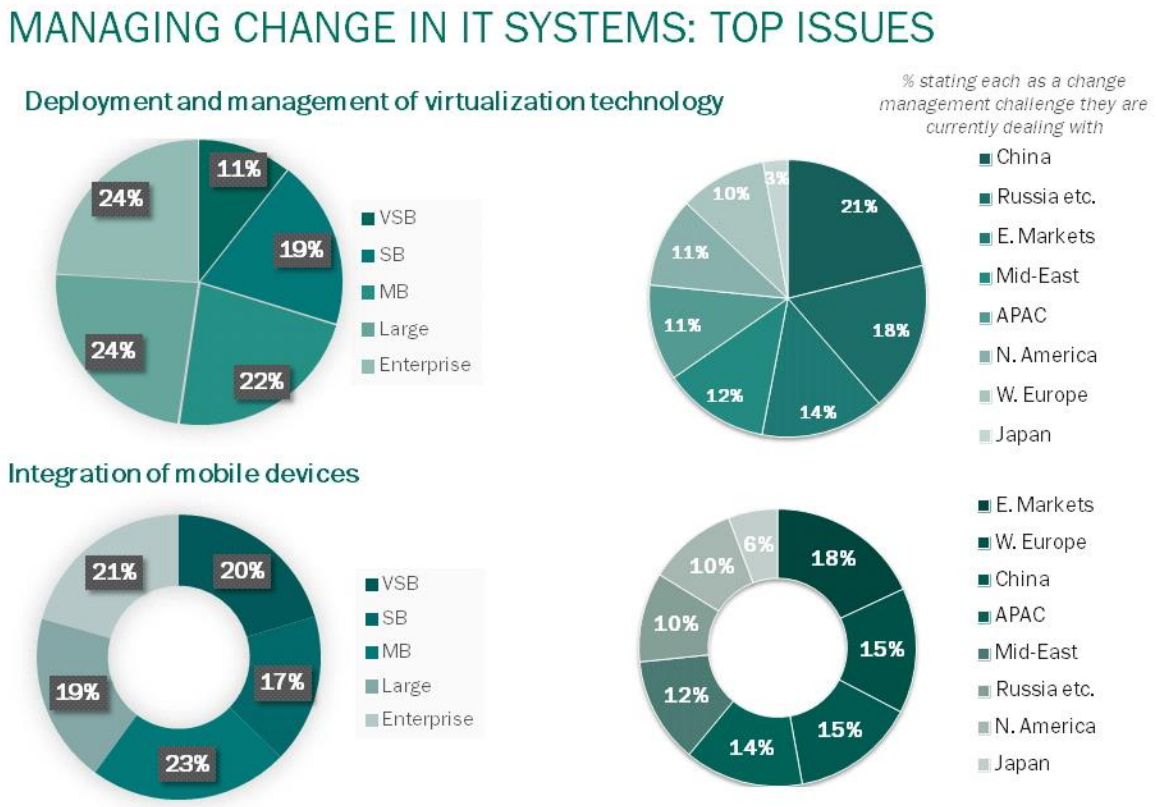


A total of 3,900 respondents from 27 countries – including representatives from companies of all sizes – took part in this year's survey. Compared to the previous year, the survey grew both in total size and global scope (the 2013 survey included 2,900 respondents in 24 countries). More than 54% of the participants were mid-sized, large and very large companies. Approximately 17% of the respondents were corporations in the Large Enterprise segment (with anywhere from 5,000 to 50,000 employees), while 12% of the survey participants fit into the Large-Medium category (1,500 to 5,000 employees). About 25% of the survey participants were companies with anywhere from 250 to 1,500 employees, and the remaining respondents represented small and very small businesses.

All of the companies that took part in the survey answered dozens of questions concerning the main obstacles that both the company's general management and IT management face, specifically when building and maintaining a reliable, smooth-running IT infrastructure. Additionally, respondents answered questions about the resources allocated by their companies for tackling IT problems, including data security problems. The survey questions asked respondents about business conditions within a period of the previous 12 months, from April 2013 through May 2014.

MANAGING VIRTUALIZATION

For IT managers who have dealt with “the pain of change” over the past year, virtualization technology has been a key area of struggle. While the benefits of virtualization are numerous – including reduced hardware costs, improved agility to respond to business demands, and easier management – a smooth transition from physical to virtual requires a detailed understanding of all the unique characteristics of this new environment, and the rules of physical IT infrastructure, including those related to security, often don’t apply.

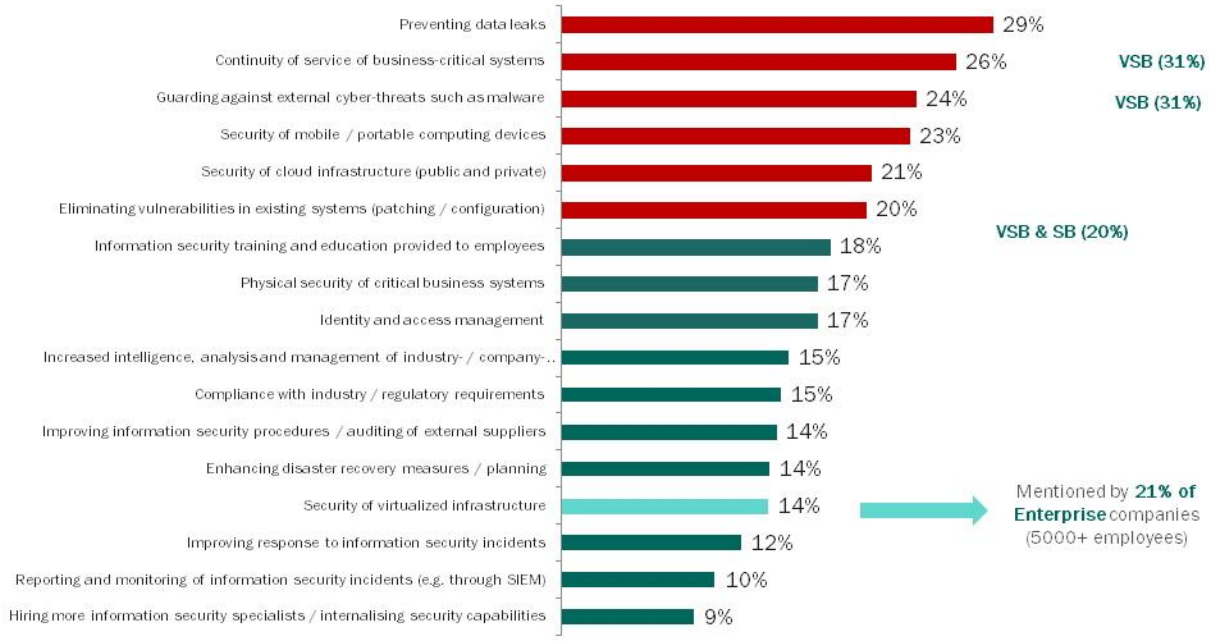


Interestingly, the percentage of respondents dealing with the challenges of virtualization is almost identical at all levels from Medium-sized Business (100-1499 employees) through Enterprises (5000+ employees). Very Small Businesses (25 employees or fewer) showed the most notable difference.

VIRTUALIZATION SECURITY IN THE PAST AND FUTURE

COMPANY IT SECURITY PRIORITIES FOR THE NEXT 12 MONTHS

PREVENTING DATA LEAKS IS THE TOP IT SECURITY PRIORITY, WITH CONTINUITY OF SERVICE A CLOSE SECOND



When it comes to establishing security priorities, business clearly have many factors to contend with. At first glance securing virtual infrastructure seems to rate comparatively low. It is noteworthy that Enterprises regard virtualization security as a higher priority than the global average, especially since we saw from the previous page that Large Businesses and Medium Businesses face similar levels of virtualization management challenges within their organization. It is also noteworthy that “continuity of service of business-critical systems” is the second most common priority. Later in this report we’ll show that virtualization is indeed becoming a “business-critical” system.

COMPANY IT SECURITY PRIORITIES FOR THE NEXT 12 MONTHS

BY VERTICAL

A NUMBER OF INTERESTING IT SECURITY PRIORITIES EMERGE AT THE INDUSTRY VERTICAL LEVEL

	Manufacturing	IT/ Software Etc.	Financial Services	Business Services	Construction/ Engineering	Government /Defence	Education	Healthcare /Services	Consumer Services	Other	Transportation /Logistics	Telecoms	Real-Estate	Utilities & Energy	Media /Design	Non-Profit /Charitable	E-commerce /Online Retail
Base	724	613	328	305	294	292	279	199	535	187	140	116	99	95	93	71	68
Preventing **data leaks**	33%	26%	31%	28%	33%	29%	29%	25%	29%	25%	34%	16%	35%	28%	28%	21%	28%
Continuity of service of business-critical systems	24%	25%	23%	27%	24%	21%	28%	29%	30%	29%	26%	40%	28%	27%	29%	37%	26%
Guarding against **external cyber-threats** e.g. malware	22%	21%	19%	27%	23%	29%	23%	21%	28%	28%	29%	16%	26%	19%	33%	18%	25%
Security of mobile / portable computing devices	21%	21%	17%	32%	24%	24%	23%	26%	25%	27%	21%	25%	27%	23%	20%	30%	26%
Security of cloud infrastructure (public and private)	19%	24%	17%	27%	14%	18%	22%	21%	19%	22%	23%	23%	21%	16%	37%	24%	18%
Eliminating vulnerabilities in existing systems	19%	20%	20%	19%	22%	22%	16%	25%	20%	24%	24%	24%	20%	24%	24%	23%	19%
Information security training provided to employees	16%	17%	14%	17%	23%	21%	28%	18%	17%	19%	11%	14%	17%	16%	19%	21%	19%
Physical security of critical business systems	20%	18%	16%	19%	20%	13%	14%	9%	19%	19%	16%	16%	12%	17%	14%	8%	19%
Identity and **access management**	18%	14%	17%	17%	16%	23%	19%	20%	18%	14%	11%	18%	16%	17%	10%	31%	22%
Focussed approaches to industry-specific threats	15%	15%	18%	14%	19%	15%	13%	14%	17%	11%	15%	19%	10%	13%	14%	10%	16%
Compliance with industry / regulatory requirements	14%	11%	23%	10%	12%	17%	16%	28%	13%	17%	13%	13%	13%	18%	4%	18%	10%
Security of **virtualized infrastructure**	13%	21%	16%	10%	11%	17%	10%	12%	11%	11%	16%	14%	10%	19%	12%	10%	15%

Base: 4,438 All Respondents

The prioritization of virtualized security remained relatively consistent across all regions and also remained consistent when compared across various vertical markets, with one exception. Perhaps predictably, the IT/Software industry reported the highest level of prioritization for virtual security, at 21%. Less predictably, the next highest rate of prioritization was in the Utilities & Energy sector, at 19%. This may be an indicator of an overall trend of Utilities & Energy placing a higher priority on security in general.

At 14%, virtualization security may not rank as a high priority when compared to all other security concerns, but the understanding that virtual environments require securing remains quite high. It seems that securing virtual environments is on everyone's "to-do" list, just not at the top. For example:

ATTITUDES TOWARDS TECHNOLOGICAL TRENDS

BY REGION: US BUSINESSES FEEL BETTER EQUIPPED TO DEAL WITH THE SECURITY ISSUES ARISING FROM MOBILE DEVICE USAGE & ARE LESS CONCERNED ABOUT CRYPTOLOCKER

	Globally	Russia etc.	China	N. America	W. Europe	E. Markets	APAC	Mid-East	Japan
Base	4,438	518	208	400	1,576	611	822	105	198
We make every effort to ensure our anti-fraud measures are up-to-date	62%	73%	72%	66%	58%	62%	63%	50%	57%
Virtualized environments increasingly form a core part of our critical IT infrastructure	52%	59%	66%	49%	47%	57%	56%	42%	46%

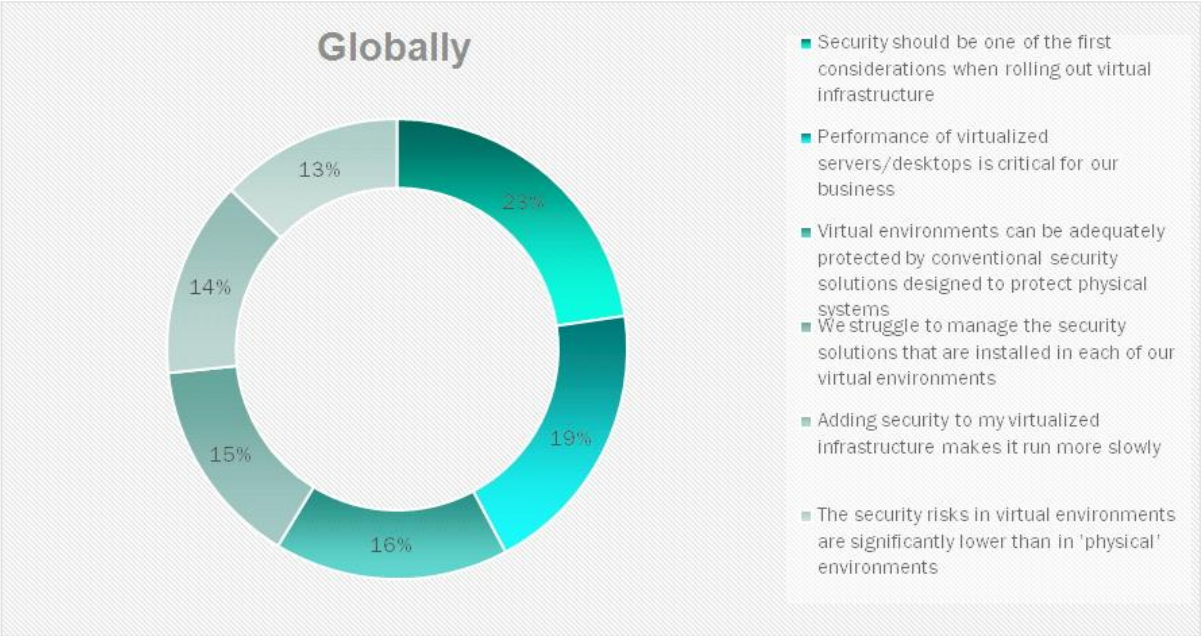
Significantly higher Significantly lower Base: 4,438 All Respondents

A global average of 43% agreed that security concerns are a barrier to the implementation of virtualized security. This attitude was less prevalent in the Middle East and Russia, but was substantially more common than average in China and the APAC region.

ATTITUDES TOWARDS THE VIRTUAL ENVIRONMENT

AGAIN, THE SECURITY IS THE TOP CONCERN

Chart Shows % Of Respondents Agreeing With Each Statement (% Agreeing or Strongly Agreeing)



W4N17. For each of the following statements relating to virtualization, to what extent do you agree or disagree with each (On a scale of 1-5)

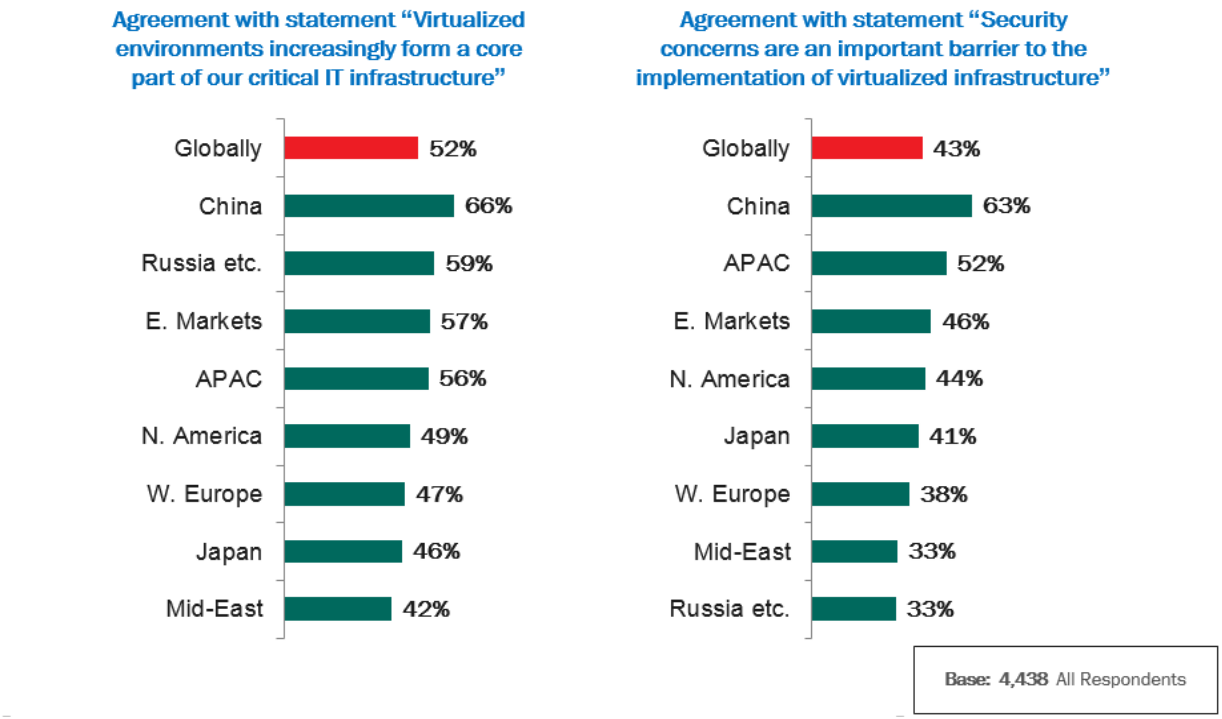
Base: 2,544 All Respondents With Any Virtualization Implemented

Here, we see again that virtualization security is a top consideration, with 64% agreeing that security should be a key consideration when rolling out virtual infrastructure. This was taken from the portion of the respondent pool that already has some form of virtualization implemented (slightly more than half of the total respondent pool), so it stands to reason that they are more knowledgeable about virtualization security concerns than their non-virtual counterparts. That number drops to 43% when asked of the total respondent pool (next page).

THE GROWING IMPORTANCE OF VIRTUALIZATION

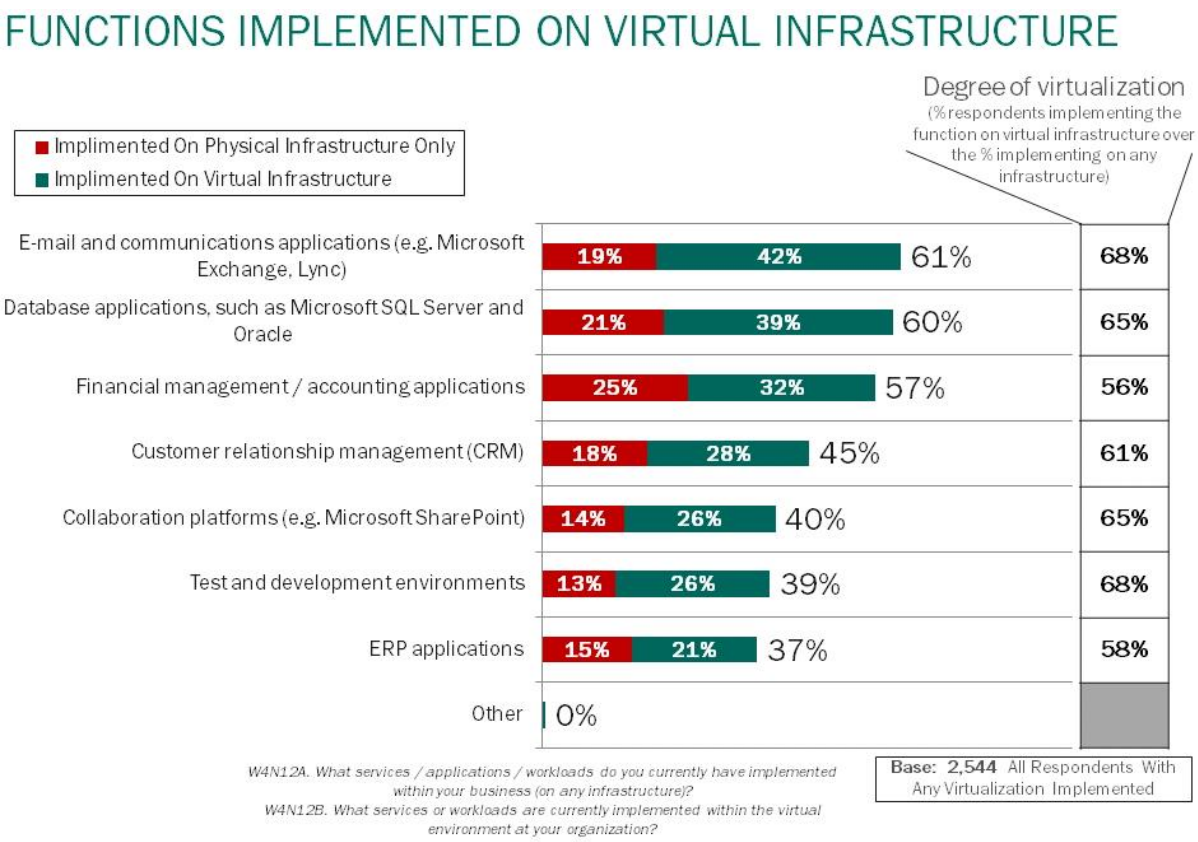
THE INCREASED IMPORTANCE OF VIRTUAL INFRASTRUCTURE

BUT RELUCTANCE TO FURTHER ADOPT DUE TO SECURITY CONCERNS



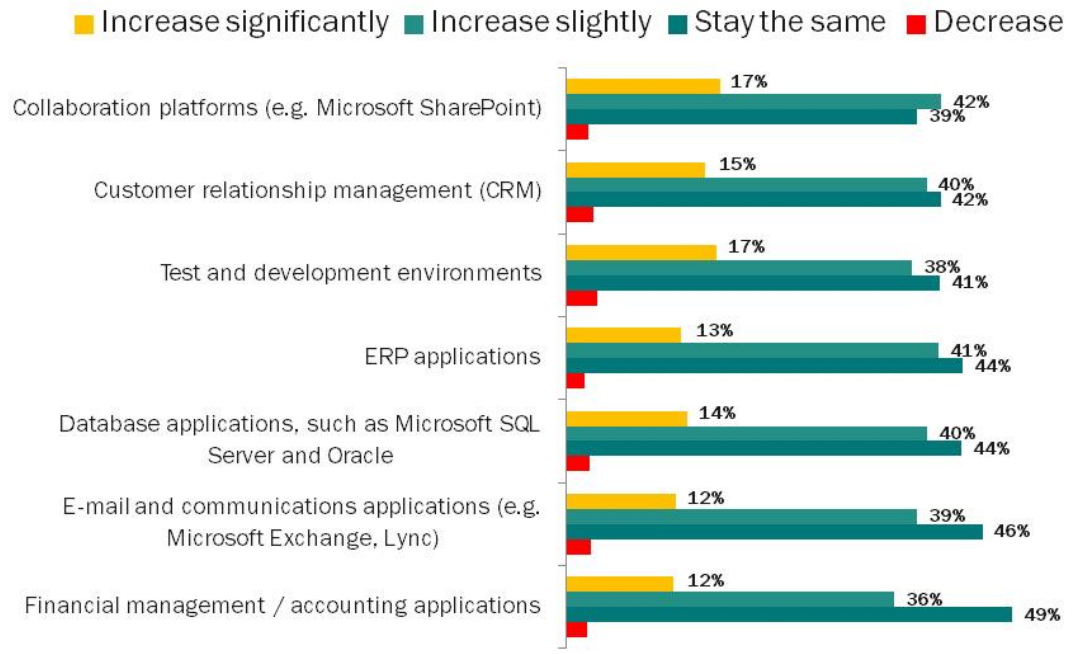
Alongside the attitude of security being a barrier for virtualization implementation (which 43% of the total survey respondent pool agreed), we see another key trend: virtualized environments are becoming a core part of mission-critical IT infrastructure. 52% of all respondents agreed that virtual servers and desktops are housing the core applications and business data that organizations need to function. This can included financial data, customer records and the intellectual property that forms the basis of a successful business.

Here are some more details about what types of data are being maintained in virtual environments:



This slide asked businesses that have some virtual systems in their IT infrastructure to indicate what types of business applications they ran in virtual environments versus physical ones. You can see that virtualized email and communications applications were the most common, followed closely by database applications and finance/accounting software. Think of the business information that would flow through these virtual systems – nearly all internal communication, vast repositories of business data and the company's banking information (which could include customer banking information as well). These are indeed mission-critical systems containing information that could be incredibly valuable to cybercriminals.

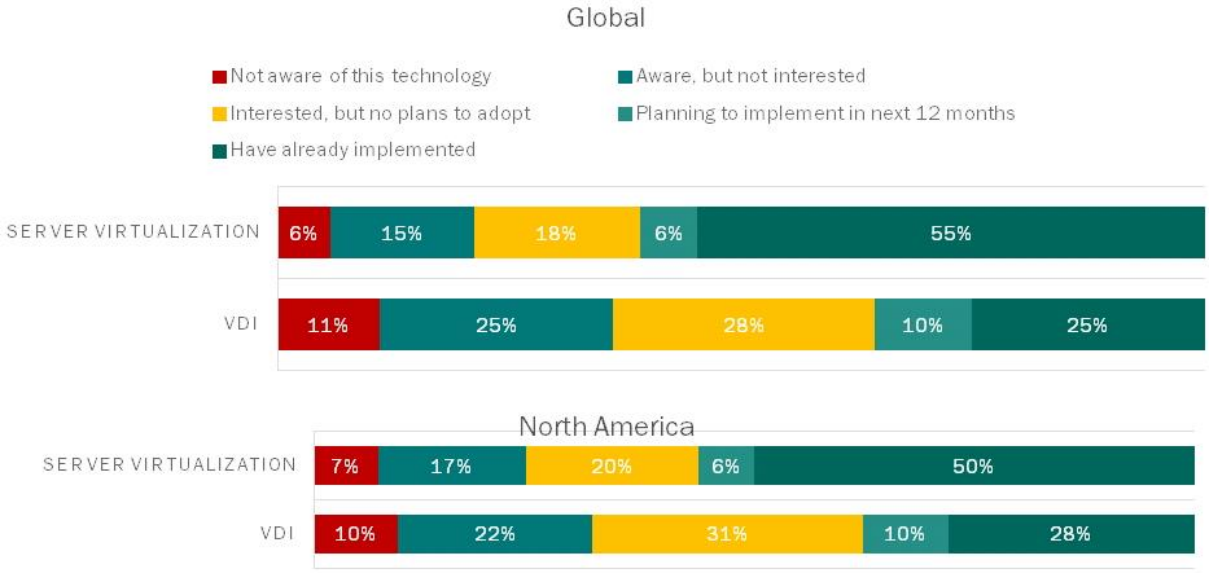
EXPECTED CHANGE IN THE DEGREE OF VIRTUALIZATION OF IT FUNCTIONS



Base: Varies, All Respondents with any form of virtualization implemented who have implemented each function on physical or virtual infrastructure

The use of virtual environments to support core business applications doesn't show any signs of slowing down. Even the *lowest* rate of planned virtualization growth – for financial and account applications – is still projected to increase by 48% in the next 12 months. This shows that businesses that have placed their trust in virtual environments are seeing the benefits and continuing their investment in the platform. But how will security factor into that investment?

VIRTUAL ENVIRONMENT ADOPTION



Another interesting point is the type of virtualization being implemented by businesses. Here, we see that server virtualization is by far the most popular. The concept of virtual desktops appears to be interesting, but businesses seem hesitant to adopt it. So far, the data has established:

1) Businesses are implementing, and often struggling to manage, virtualization.

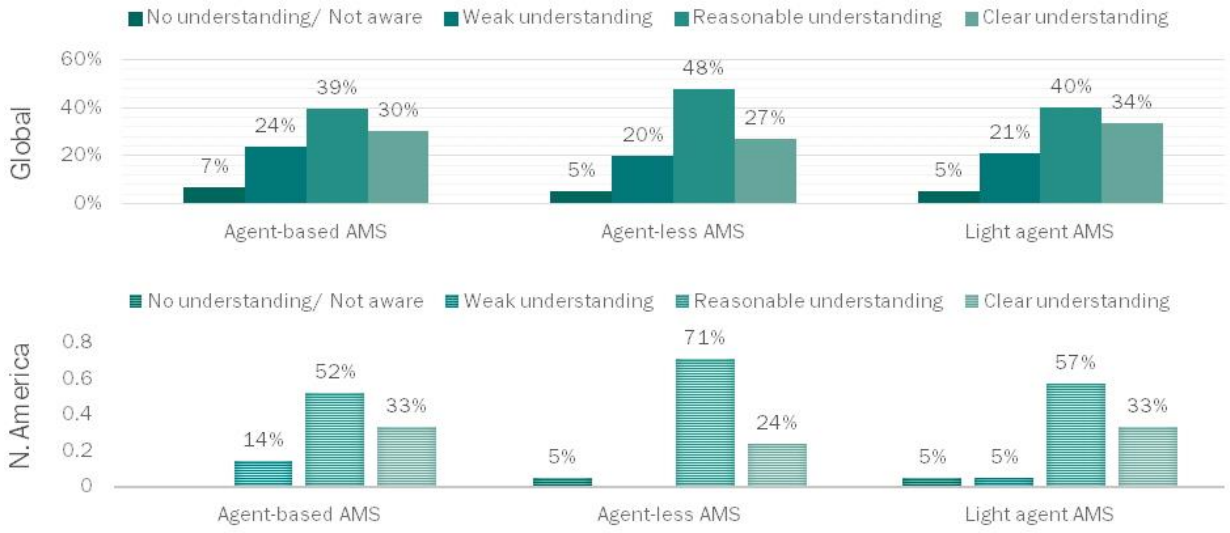
2) Businesses are putting more and more mission-critical data and business applications in virtual environments.

3) Businesses seem to place importance on the “concept” of virtualization security.

Now, let’s examine how virtualization security is actually understood and being implemented.

VIRTUALIZATION SECURITY AWARENESS AND IMPLEMENTATION

UNDERSTANDING OF VIRTUAL ENVIRONMENT SECURITY SOLUTIONS AMONGST IT SECURITY EXPERTS



Even amongst IT security experts only around a third felt they had a clear understanding of how these different approaches to virtual environment security functioned although in N. America, most IT security experts had a reasonable understanding

This particular question was asked to participants who regard themselves as IT security experts. Even among these experts, only one-third (on average) felt they had a clear understanding of how these different approaches to virtual environment security functioned. This number dropped to nearly one-quarter when they were asked specifically about agent-less security.

When asking respondents who had some kind of virtualized infrastructure how they secured these systems:

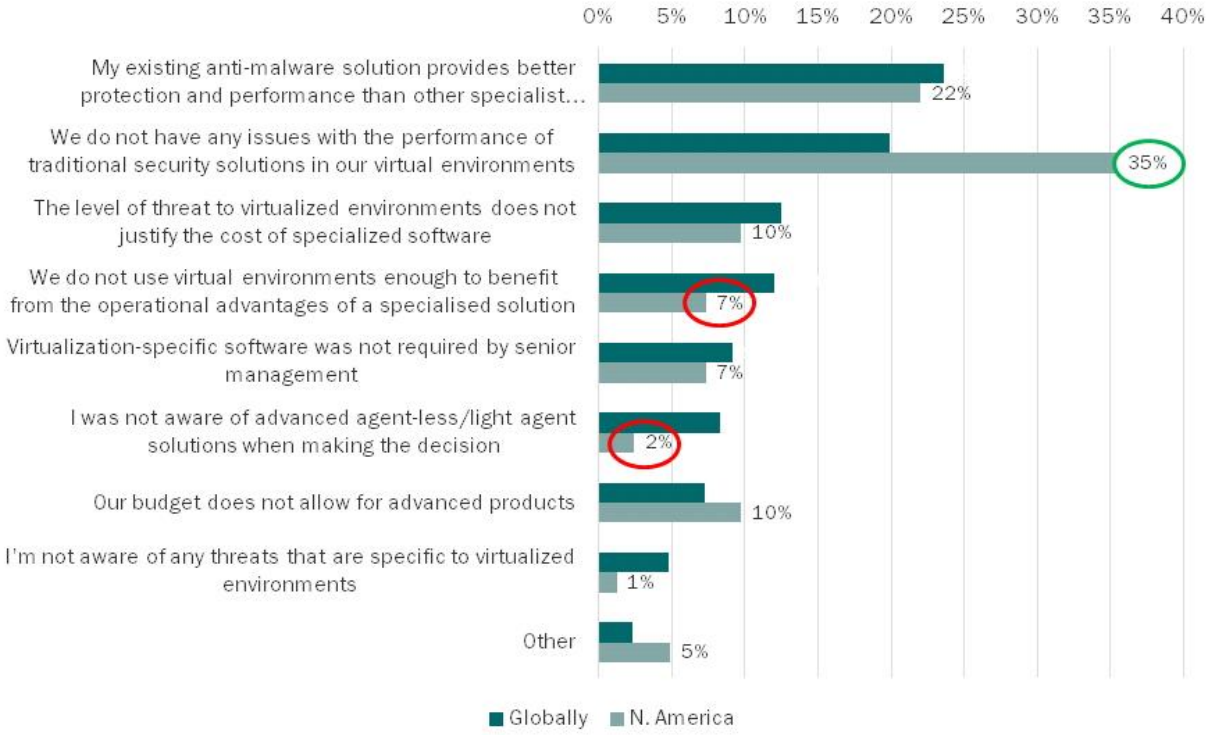
Only **32% reported having a "fully implemented" security solution for the virtual network.** Within this group, 58% reported having "virtually-aware" agent-based anti-malware for their virtual machines. This means they are most likely using the same endpoint security solution deployed on their physical machines. For the rest of the "fully implemented" group, 20% reported using agent-less anti-malware, and 17% said they used light-agent anti-malware to protect their virtual systems.

A staggering **53% of businesses using virtualized infrastructure reported only "partially implementing" a security solution** to protect their virtual machines. This group reported a more even mix of solutions, with 29% using agent-based, 35% using agent-less, and 27% using light agent. The fact that those who are "in the process" of implementing their solution are

more likely to choose a specialized security solution (agent-less or light-agent) suggests businesses are beginning to understand the value that virtualization-specific security can offer. To learn more about the differences between agents-less and light-agent virtualization solutions, read this comparison chart.

With such a clear disconnect in the perceived value of virtualization security and the actual implementation of it, here are some reasons why business have not adopted a specialized solution for their virtual infrastructure.

REASONS FOR NOT ADOPTING A SPECIALISED VIRTUAL ENVIRONMENT SECURITY SOLUTION



W4N16. What is your primary reason for using a traditional endpoint-based solution to protect your virtual environment?

These questions were asked to respondents that use conventional (agent-based) security solutions in their virtual environments. The two most common reasons for this is the belief that an existing anti-malware solution provides better protection than specialized solutions and not encountering any performance issues that would motivate a business to switch solutions.* This attitude towards performance was especially notable among North American survey respondents, who far exceeded the global average for this response.

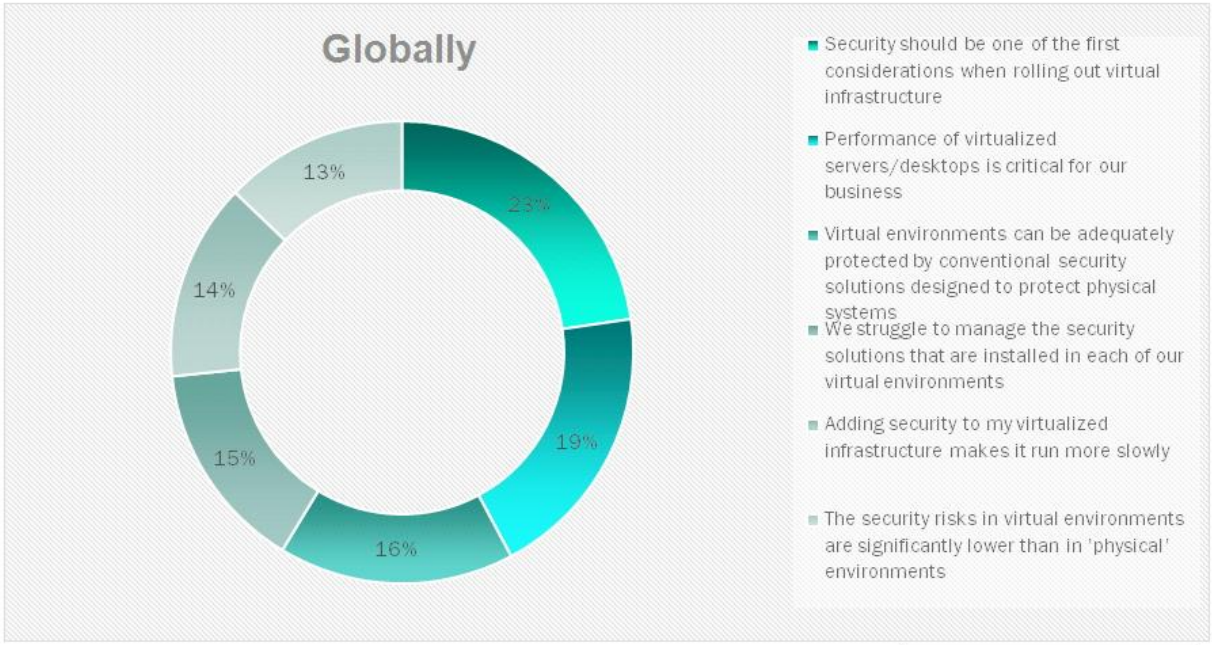
It seems that businesses are taking a “if it’s not broken, don’t fix it” approach to their virtualization security, and the benefits of a specialized solution are not apparent enough to motivate a change.

**In a May 2014 study conducted by the independent security test firm AV-TEST on behalf of Kaspersky Lab, the testers found the protection of conventional and virtualization-specific solutions to be nearly equal, but there was a large difference in performance impact. You can learn more about the test in Kaspersky Lab's press release.*

ATTITUDES TOWARDS THE VIRTUAL ENVIRONMENT

AGAIN, THE SECURITY IS THE TOP CONCERN

Chart Shows % Of Respondents Agreeing With Each Statement (% Agreeing or Strongly Agreeing)



W4N17. For each of the following statements relating to virtualization, to what extent do you agree or disagree with each (On a scale of 1-5)

Base: 2,544 All Respondents With Any Virtualization Implemented

Here we see some more attitudes towards virtualization security that indicate awareness of the importance of secure virtualization, but still show a significant portion of respondents are clinging to outdated beliefs about the technology. 55% agree that performance of virtualized infrastructure is critical for business, while 46% believe conventional physical security can provide adequate protection for virtual networks. These two statistics are noteworthy because they directly conflict with each other. Conventional security systems may be capable of providing adequate protection for virtual networks – but not without a high cost in system performance, server consolidation and overall ROI. This is particularly true at Enterprise and Large Business levels, where duplicating security agents and scanning resources quickly multiply to create a huge drain on the network when performing even basic security tasks.

Also noteworthy are the 36% of respondents who answered that security risks in virtual environments are significantly lower than in physical environments. While this perception was

probably much higher a few years ago, the fact that it is still believed to be true by one-third of IT-savvy respondents means more education in the marketplace is necessary.

Lastly, 41% noted that they struggled to maintain the security solutions installed in their virtual environments. We can only speculate as to the source of these struggles, but these respondents could be referring to maintaining the performance of their virtual machines when bogged down with conventional security solutions. This might also refer to having a separate management interface (or the lack of a centralized management interface), causing respondents to manage two consoles, create two different sets of security polices, etc.

CONCLUSIONS AND RECOMMENDATIONS

Virtualization has been a common IT optimization tool for years, and the rate of virtual platform adoption is increasing in businesses of all sizes and sectors. As with any technology platform, the more broadly adopted it becomes, the more likely it will be targeted by cybercriminals. In addition, businesses are no longer limiting their use of virtualization to just IT test environments or other narrow use cases; instead, businesses are more likely than ever to use virtual environments to store important data and run business-critical applications, which makes virtualized networks an even more attractive target for cybercriminals.

According to our survey results, businesses are becoming more aware of security concerns and requirements for virtual networks, but some lingering misconceptions still persist. Virtual environments are seen to be inherently "more secure" than physical environments. While there is some truth to that belief – IT administrators have historically simply "switched off" and re-started virtual machines to wipe out malware – this cannot be seen as justification for unprotected virtual environments, especially given the nature of data now being stored on virtual machines.

Finally, there is still work to be done around educating businesses, and even self-proclaimed IT security experts, about the differences in virtualization security solutions that exist today. Based on the results of this survey, Kaspersky Lab has the following recommendations for IT managers and C-level executives:

Measure the performance cost of security. The goal of virtualization is to do more with less by optimizing your resources. Using the same security solution that protects your physical endpoints may seem like a logical choice for protecting all your virtual machines – but this can seriously hinder your primary goal of performance optimization. Pay special attention to network traffic and performance losses in larger virtual deployments (50+ machines) – your "physical" security may be negating your virtual ROI.

Assign the right solution to the right use case. There are different types of virtual security offerings, and you will likely need a combination of them within your network. Understanding the strengths of agent-based and agent-less virtualization configurations will help you make sure the right protection is given to each virtual machine. In some cases, you may even find that virtually-aware "physical security" is an appropriate option for specific virtual machines, but in most cases, a security solution built specifically for virtual environments will offer better performance and protection.

Limit "Virtual Sprawl." As virtual endpoints become more widespread and easier to create, make sure the IT department judiciously monitors the virtual machines created and shuts them down when not in use. If a virtual machine created as a "one-off" is used and forgotten about, it can create a serious security gap in your network.

Additional Information:

- Best Practices Guide: Security for Virtualization – Getting the Balance Right
- Kaspersky Security for Virtualization Data Sheet
- Press Release: Kaspersky Lab Tops Competitors in Testing of Security Software in Virtual Environments