SECURITY OF VIRTUAL INFRASTRUCTURE

IT SECURITY RISKS SPECIAL REPORT SERIES

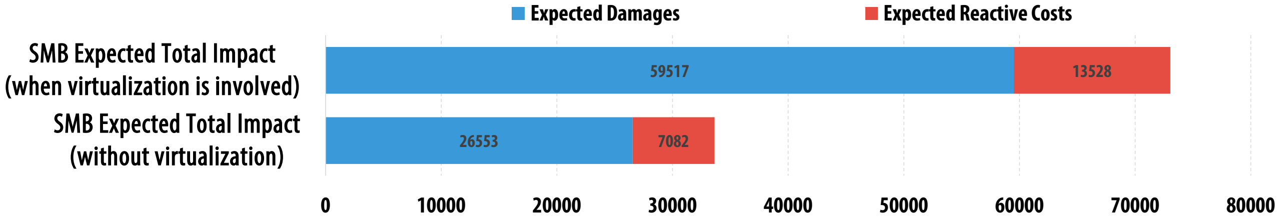
Kaspersky Lab

Corporate IT Security Risks survey details:

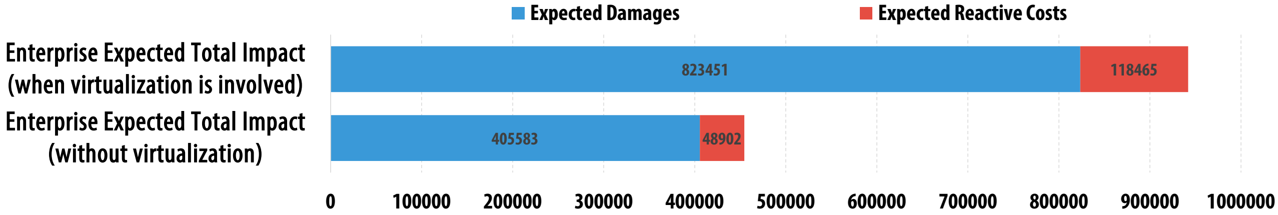
- More than 5500 companies in 25+ countries around the world
- Top managers and IT pros answered questions about security, IT threats and infrastructure

What we have found:

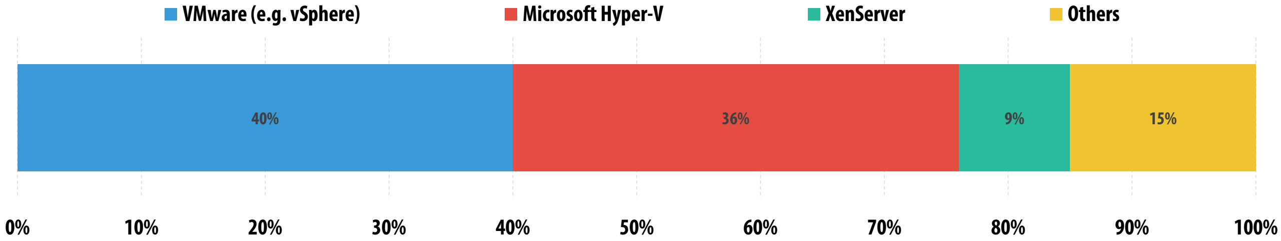
- **x2**: Businesses pay twice as much to recover from a security breach if virtual infrastructure was involved
  - Average direct cost of recovery for SMBs is close to $60,000 per incident



  - Enterprises spend more than $800,000 on recovery.



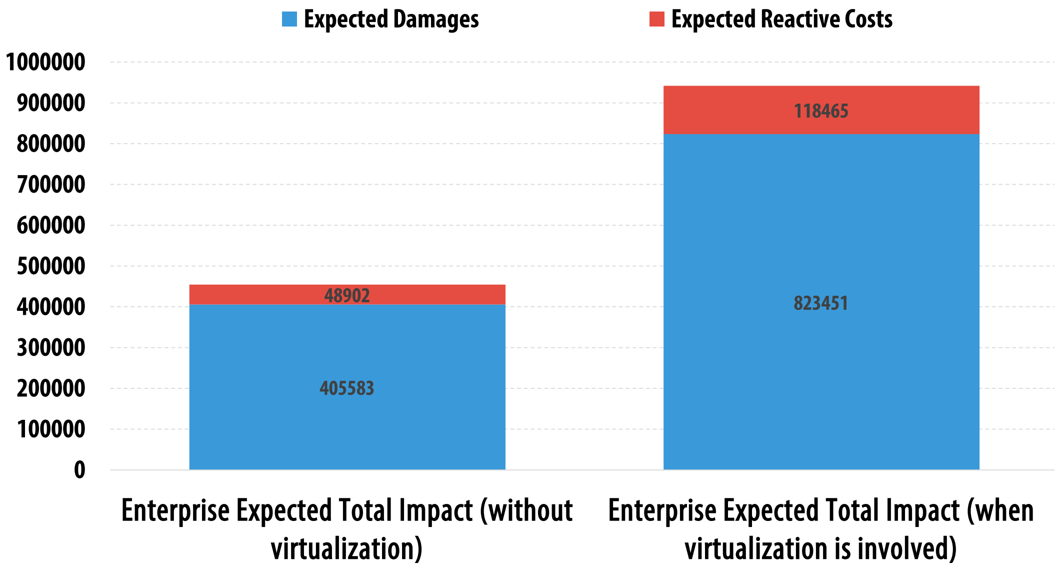
- 3 reasons for a cost increase:
  - Security complexity: only **56%** of companies are fully prepared to deal with security risks in a virtual environment
  - Need to improve understanding of risks specific to virtual environments: just **52%** of company representatives feel they fully understand the risks.
  - Extensive use of virtual infrastructure for mission-critical operations.
- **62%** of businesses use virtualization in some form
- Top 3 virtualization platforms in use: VMWare (**40%**), Microsoft (**36%**) and Citrix (**9%**)



- **9%** of businesses use open-source virtualization platforms: Xen (**6%**) and KVM (**3%**)
- **42%** of businesses still think that virtual environments are safer than physical ones.
- Few companies are using specialized security solutions for virtual environments:
  - **73%** of businesses are not using specialized IT security solutions
  - **34%** aren't even aware of the performance benefits such solutions provide
  - Of those using specialized IT Security methods, **48%** use agent-based solutions. The adoption of agentless (**35%**) and light-agent approaches (**13%**) is significantly lower.

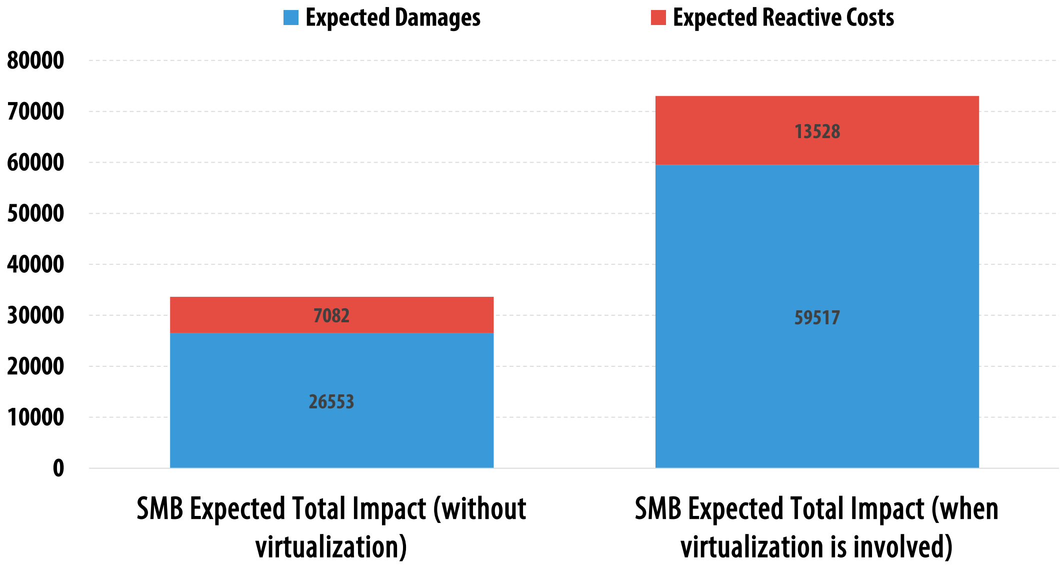
KEY FINDING: VIRTUAL INFRASTRUCTURE DOUBLES THE COST OF A SECURITY BREACH

The most interesting result that was discovered during this survey is the comparison of financial losses reported by companies. If virtual infrastructure is affected, businesses have to pay a significant premium to recover from a security breach. For large companies (1500+ seats) the average cost of a security incident is more than $800K. If we include indirect expenses, such as staff training to mitigate future risks after the attack, the total cost comes close to one million USD.



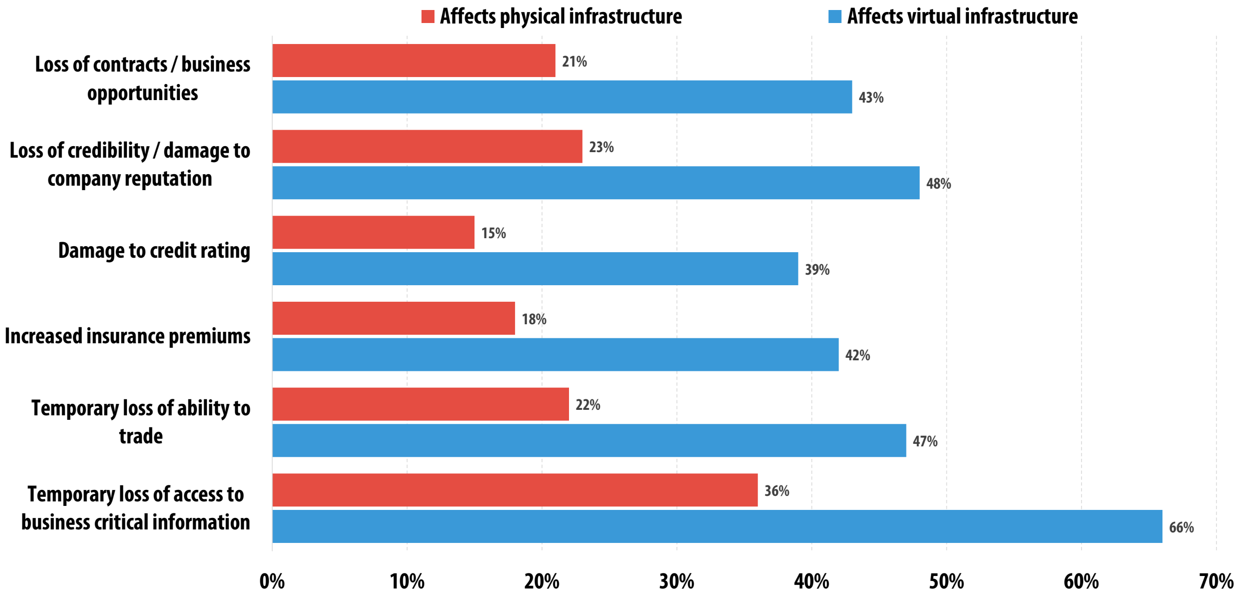
Overall financial losses due to data breaches for enterprises in US dollars

SMBs reported an average damage of more than $26,000 for an attack on their physical infrastructure. The involvement of virtual infrastructure in a security breach however, brings the cost closer to $60,000 (not including reactive spend).



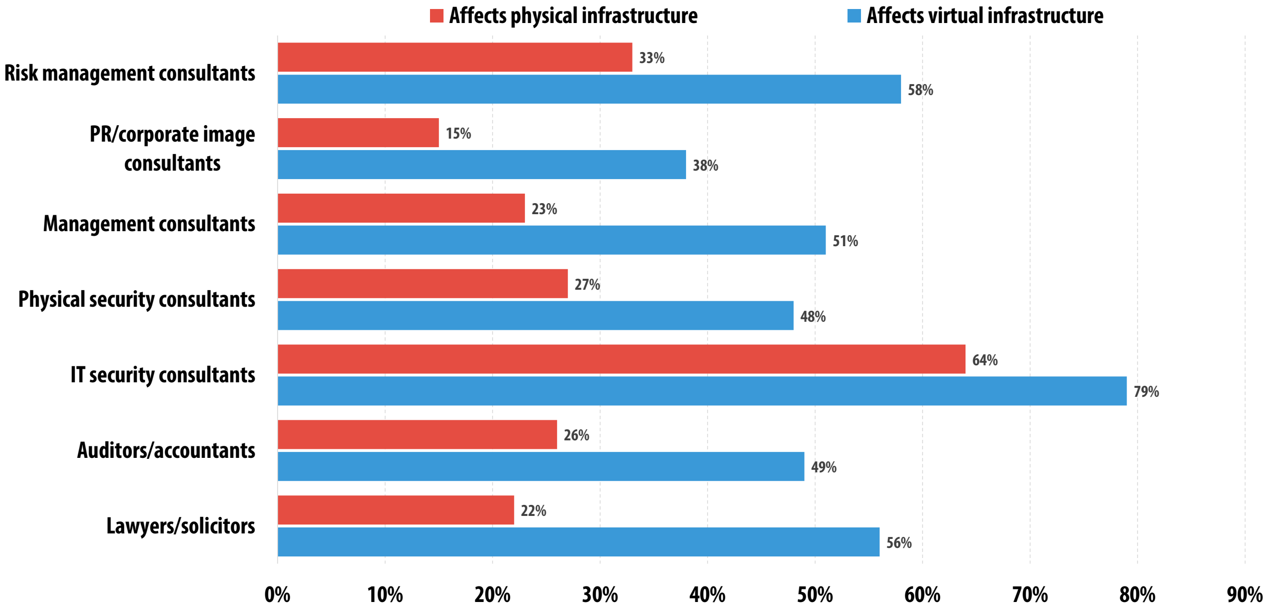
Overall financial losses due to data breaches for small and medium businesses in US dollars

What could be the reason for this extra spend on recovery? Although we see clearly that IT security in the virtual environment is complicated topic for many businesses (more on that below), the main reason is that virtual infrastructure is more frequently used for mission-critical operations and/or to store highly sensitive data. The following breakdown of the consequences of a security breach involving/not involving virtual infrastructure provides proof:



Breakdown of the consequences of a security breach that affects virtual infrastructure (blue) and only physical infrastructure (red). Indicates the percentage of businesses reporting a certain type of a consequence of an attack.

An attack on a company's virtual infrastructure is much more likely to result in the temporary loss of important data, an inability to operate core services and damage to reputation. We have also observed that businesses recovering from an attack on virtual infrastructure spend more on both IT consultants, and lawyers:

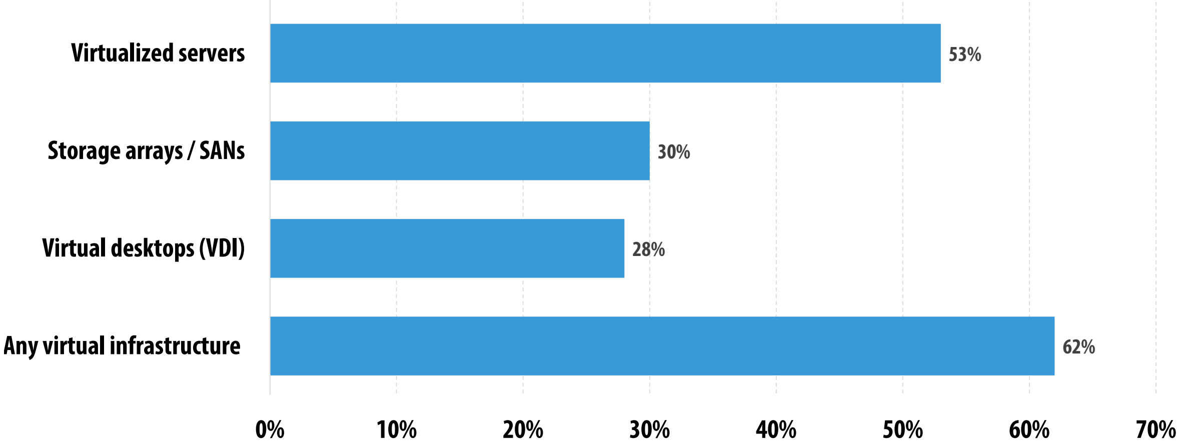


Breakdown of recovery measures from a security breach that affects virtual infrastructure (blue) and only physical infrastructure (red). Indicates the percentage of businesses reporting a certain type of an expenses required to recover from an attack.

A significant increase of expenses on lawyers and IT security consultants at the same time indicates that accidents involving virtual infrastructure are more likely to be revealed to the public, clients and partners.

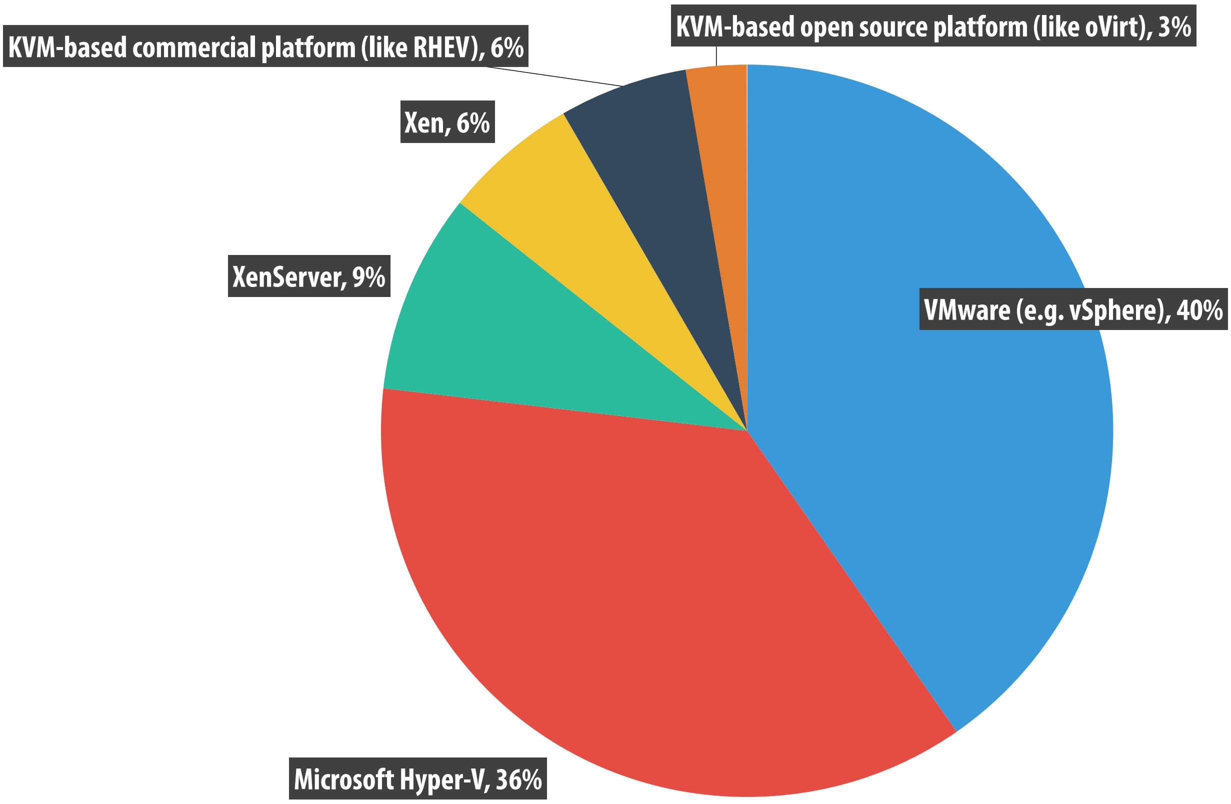
SPECIFICS OF VIRTUAL INFRASTRUCTURE

Going virtual is not a trend anymore, but a business practice. 62% of respondents claimed that their company is using virtualization in some form.

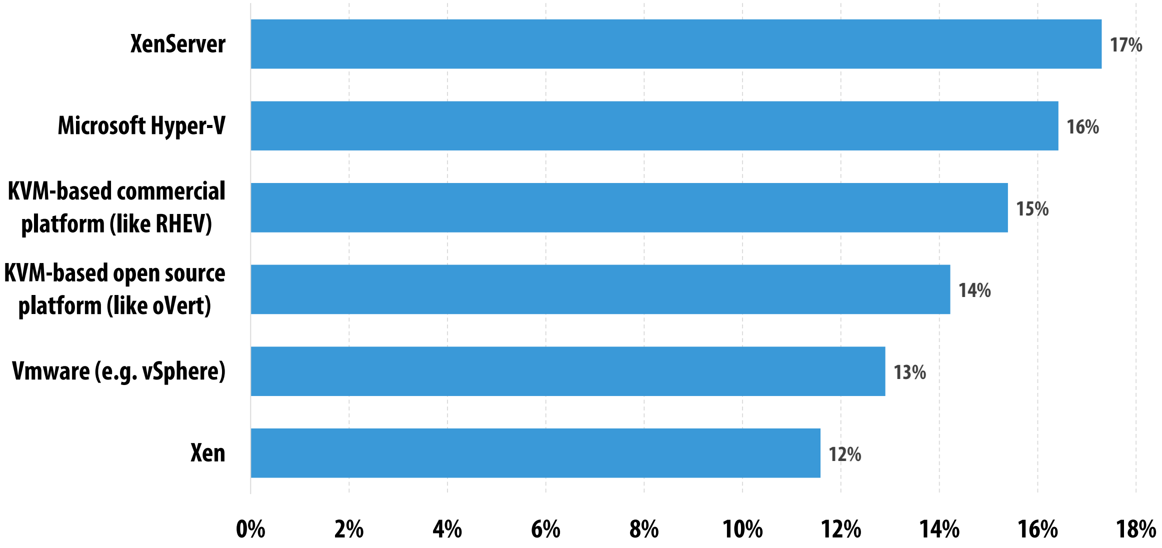


Adoption of different types of virtualized infrastructure and the overall share of businesses using any type of virtual infrastructure.

As a company grows, the need for virtual infrastructure increases. Among companies with over 1500 employees 77% of organizations have virtual infrastructure implemented in some form.



According to virtualization specialists (experts in the virtualization solutions used in business), the most popular hypervisor platforms are VMware and Microsoft, however KVM is gaining traction. In the corporate wish list for virtual infrastructure, KVM (commercial implementation or open-source) is one of the most desired platforms.



Virtualization platforms companies are likely to adopt in the next two years

Virtualization platforms provided by Microsoft and VMware are being used by more than two thirds of respondents. Microsoft's Hyper-V is also number two in the list of platforms companies are likely to choose in the near future. And judging by this data, KVM looks to be the most promising competitor for current market leaders, especially if both commercial and freely available open-source versions of the platform are taken into account.

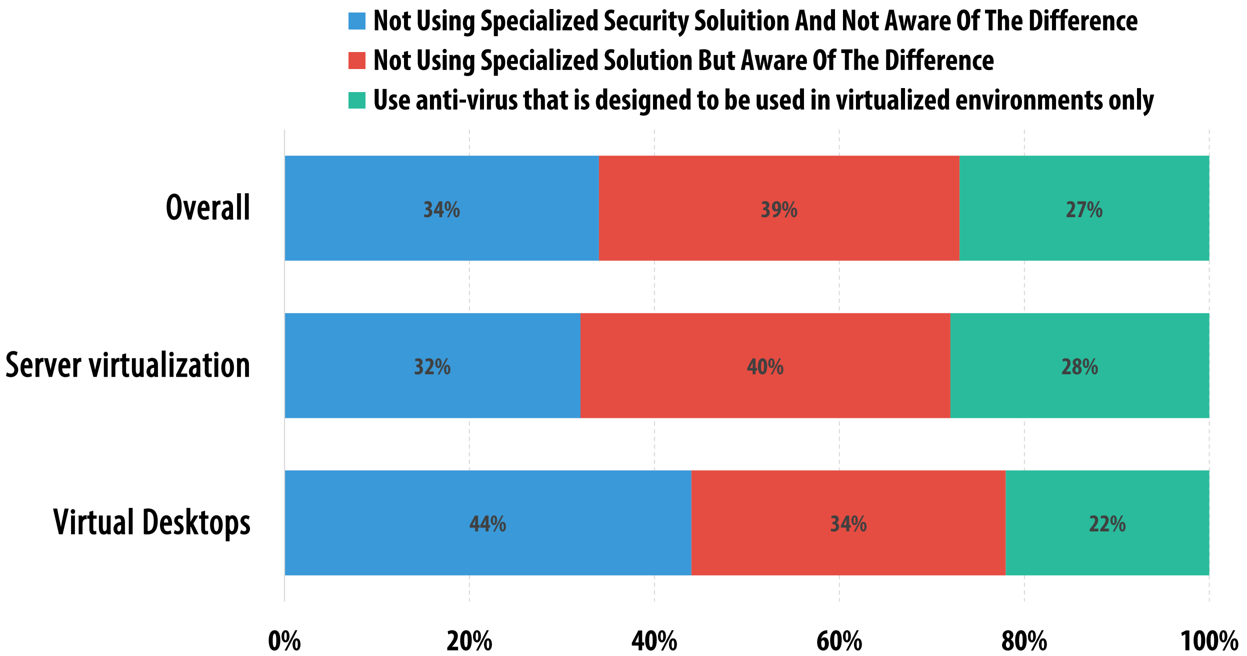
SECURITY OF VIRTUAL INFRASTRUCTURE

The protection of physical endpoints and servers provides companies with a choice of a security software vendor, but before protecting virtual desktop or server a company has to choose an approach first. There are three major security approaches for virtualized environments:

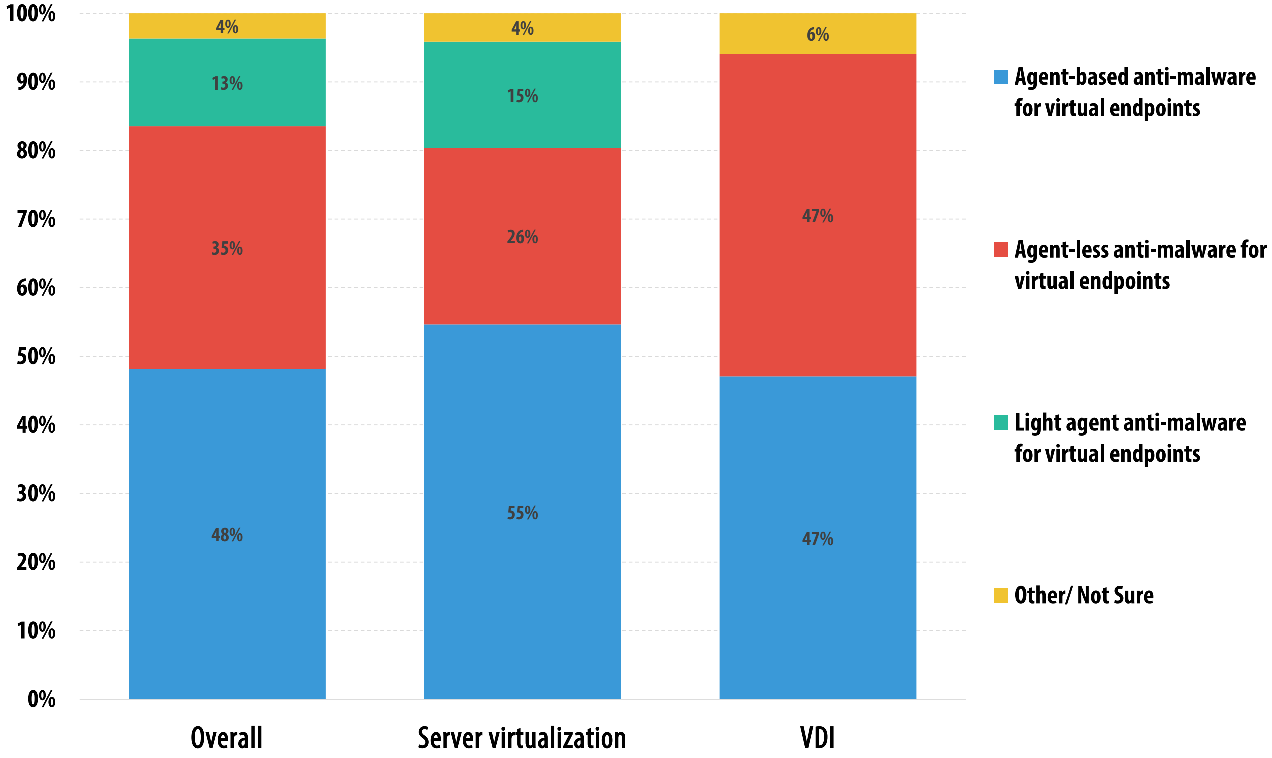
- Agent-based: a security 'agent' is installed on every virtual machine (this involves many security features and is a bit hungry on resources)
- Agentless: a separate virtual machine on a physical server protects all other virtual machines via a special virtualization platform interface (this is light on resources, but offers limited functionality and platform support)
- Light agent: a 'best of both worlds' approach (a better feature-set than agent-less, whilst still having a low impact on performance)

Read more on the different virtual security approaches here.

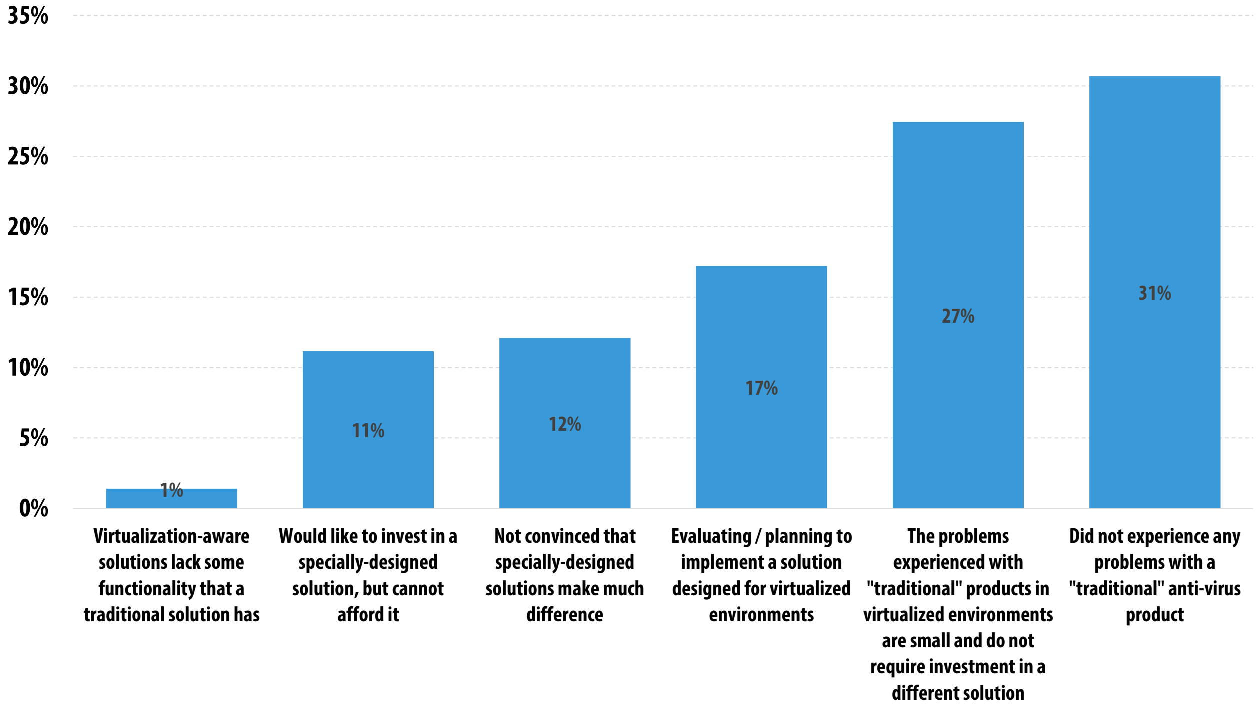
The research shows that not many companies are actually aware of the difference between these approaches. In fact, only 27% of businesses admitted the deployment of a security solution, specifically designed for virtual environments.



Of the companies that use specialized solutions, the majority are still employing agent-based software that affects consolidation ratio and reduces benefits of virtualization employment.

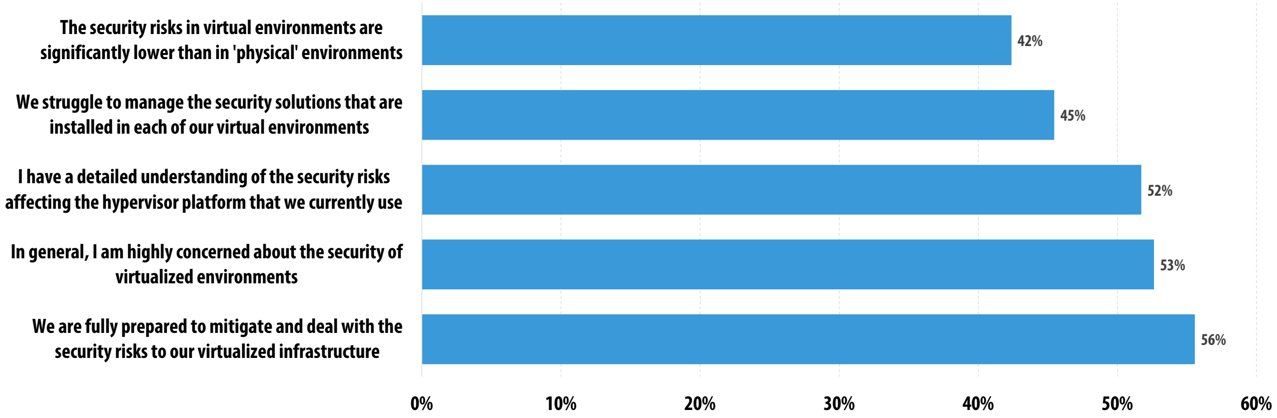


Even more companies are not using virtualization-aware solutions at all. Of those, 31% 'did not experience any problems' with a traditional security solution.



Indeed, in most cases traditional security suites do work in virtual environments. However, what is regarded as a small performance penalty on a physical endpoint, may significantly reduce cost benefits when deployed on multiple virtual machines. This adds to the fact that an attack on virtual infrastructure costs twice as much as those involving only physical endpoints and servers. The conclusion is: IT threats are a significant factor that influences the total cost of ownership (TCO) of a virtual infrastructure. A security breach or even making the wrong choice in security approach may nullify the expected cost benefits of 'going virtual'.

Only 53% of businesses said that they are concerned about securing their virtualized environments, and only a half say that they have a detailed understanding of the security risks affecting the hypervisor platform that they use. At the same time, 56% of respondents think that they are fully prepared to mitigate and deal with the associated threats – but that may be a misguided impression.



The root of many problems with virtual environment protection comes from the old misconception that risks in these environments are significantly lower than in physical environments. 42% of respondents still believe in that.

CONCLUSION

As we have observed during our survey, businesses are excited to adopt virtual infrastructure. But the industry's understanding of this technology, especially virtual-specific security issues, is far from perfect. Virtual environments are trusted more than physical servers, and nothing can be trusted in a grim security environment. This leads to higher recovery costs and inefficient security approaches being deployed. In turn, poor decisions affect ROI and may lead to disappointment in virtualization in the future, an attitude virtual infrastructure does not deserve.

Corporate IT Security Risks survey details

In 2015 Kaspersky Lab together with B2B International questioned 5,564 IT specialists representing companies of all sizes from 35 countries: small and very small businesses (up to 250 employees) - 3465, medium businesses (251-1499 employees) - 1074 and enterprises (over 1500 employees) – 1025. However, most of the questions presented in this report were relevant only to virtualization technology users (62%).

The survey was conducted in 35 countries: Brazil, China, France, Germany, India, Italy, Japan, Russia, Spain, United Kingdom, United States, Mexico, Saudi Arabia, South Africa, Turkey, United Arab Emirates (UAE), Australia, Canada, Indonesia, Malaysia, Singapore, Chile, Colombia, Czech Republic, Greece, Hungary, Kazakhstan, Peru, Denmark, Sweden, Thailand, Vietnam, Netherlands, Belgium and Israel.

Securelist the resource for Kaspersky Lab experts' technical research, analysis, and thoughts.

Follow us

Kaspersky Lab global Website

Eugene Kaspersky Blog

Kaspersky Lab B2C Blog

Kaspersky Lab B2B Blog

Kaspersky Lab security news service

Kaspersky Lab Academy

Kaspersky Lab HQ

39A/3 Leningradskoe Shosse
Moscow, 125212
Russian Federation

Tel:	+7-495-797-8700 +7-495-737-3412
Fax:	+7-495-797-8709