Virtualization Security

Security – an essential prerequisite for successful virtualization

Survey

This independent survey was supported by CA Technologies

Author: Martin Kuppinger

1 Overview

During September and October 2010 KuppingerCole conducted an independent survey of the status and plans for Virtualization Security amongst organizations. This survey shows that security is a key success factor to virtualization. Organizations transitioning to a virtualized or cloud IT model need to invest in a security strategy, in organization and skills, and in technology. Vendors need to provide better integration between security and service management plus security tools to better support heterogeneous virtualized and physical environment.

Highlights of the results are:

- The major driver of virtualization is the improvement of IT operational efficiency. The least important drivers are preparation for Cloud IT closely followed by meeting Green IT targets.
- The major inhibitor for implementing virtualization security is the lack of expertise and skills to plan and implement it. Around a quarter of organizations believe that virtual environments in general are less secure than physical environments.
- The most important security challenge and concern is around “data sprawl”. This issue is closely followed by concerns relating to the fulfilment of both regulatory compliance and internal audit requirements in a virtualized or cloud environment.
- One key issue highlighted by the survey is that nearly three quarters of respondents are concerned about the far-reaching privileges introduced by hypervisors which might lead to abuse. Technologies available today to mitigate the risks posed by privileged access in virtualized environments yet these are not widely deployed.
- There is a lack of integration between virtualization, security, and service management less than half organizations report integration in this area.
- Too many security activities are still dependent upon manual processes, performed without supporting technology and the scale of virtualization makes this approach untenable.
- By not investing in virtualization security when there are well identified security threats organizations are taking unnecessary risks which could easily be mitigated.

The survey allowed participants to add comments and free text. Some of these comments have been added as quotes to the report.

2 Executive summary

The survey provides a number of important results showing that security is the critical issue to solve when it comes to virtualization and private clouds. Solving this issue is a major concern which is top on the organization's agenda.

The survey of planned deployments for 2012 shows that the primary focus of organizations is server virtualization and storage virtualization. By the end of 2012, over half (50.8%) of the organizations surveyed expect to have deployed server virtualization to more than 50% of their systems. And 33.3% of the organizations expect to have deployed storage virtualization for more than 50% of the systems. From the KuppingerCole perspective, these numbers show the gap between the hype around virtualization and its real, phased implementation.

It is no surprise that the survey shows VMware is the leading provider of virtualization technologies, with deployments in 83.5% of the organizations. However, Citrix with 51.7% for their Xen technologies and Microsoft with 41.1%, mainly around Hyper-V, are closer than most might have expected. However, more importantly, these numbers show that the majority of organizations use at least two different providers for their virtualization technology.

When looking at the drivers for virtualization, as is to be expected, the major driver is the improvement of IT operational efficiency. The survey shows that 90.8% of the organizations rate this as the major driver or at least a driver. Closely following operational efficiency is the control of IT costs with 82.4% of organizations citing this. Least important is preparation for Cloud IT with 53.9% of organizations rating this as not a driver or only a minor one, closely followed by meeting Green IT targets.

The major inhibitor for implementing virtualization security is the lack of expertise and skills to plan and implement it. Other critical points are budgets for the upfront costs of implementing virtualization security and the complexity of managing security across virtual environments and platforms. When looking at the overall numbers, it becomes obvious that the biggest inhibitor for virtualization security is still the relative immaturity of organizations when it comes to virtualization. There is a lack of expertise and skills, there is also a lack of processes, policies and standards, and a need for improved support for virtualization security from vendors.

Around a quarter of organizations claim that virtual environments in general are less secure than physical environments. This result shows that vendors need to provide better support for virtualization security – security is a significant concern when it comes to the adoption of virtualization.

Most of the participants responded that they are looking for integrated solutions to seamlessly secure both virtual and physical environments, with 83.8% of the participants opting for that approach. This result demonstrates the lack of a significant market for "pure play virtualization security".

The survey results show that the most important security challenge and concern related to virtualization security, besides the risks imposted by privileged users which are discussed later on in this report, is around "data sprawl". That is the risk of data moving around the virtualized IT systems without control and ending up in less secure environments, 41.7% of participants considered this very important. This issue is closely followed by concerns relating to the fulfillment of both regulatory and internal compliance requirements. This demonstrates a strong understanding amongst participants of the relationship between business risks (both operational and strategic) and IT risks.

One key issue highlighted by the survey is that 73.2% of respondents are concerned about the far-reaching privileges introduced by hypervisors which might lead to abuse. However, only around half of the organizations have processes and technology deployed to mitigate these risks. For example performing regular access re-certifications of privileged users or adequately monitoring and logging privileged access. This shows that the advanced technologies available today to mitigate the risks posed by privileged access in virtualized environments are not yet widely deployed.

Even worse is the state of integration between virtualization, security, and service management. Half of the organizations have implemented or are implementing integration between change and configuration management and IT security management.

But when it comes to the integration of virtualization security with incident and problem management, applying service levels to virtualization security management, managing performance of security services, or the integration of security services into service catalogs, the implementation rate is always well below 50%. From the KuppingerCole perspective, such integration is one of the key decision criteria when choosing vendors in both IT management and security management market segments.

Finally, the participants were asked about the deployment of specific tools for IT security management in their production virtualization environments. Again, the results show that there is a long way to go – many security activities obviously still depend upon manual processes, performed without supporting technology, e.g. as mentioned above for access certification of privileged accounts. Even user provisioning is only deployed in 59.0% of the organizations. Given that this is a relatively mature area, there are still a significant number of companies which have not yet implemented this.

The key finding for the current state of virtualization security is that most organizations still have a lot of work to do in this area – at both the organizational and conceptual level as well as in implementing tools to achieve the required level of security in virtualized environments. By not investing in virtualization security when there are well identified security threats organizations are taking unnecessary risks which could easily be mitigated.

When asked for the major inhibitors to moving quickly towards private cloud models, the survey results show cloud security issues (84.4%) and cloud privacy and compliance issues (84.9%) as being most important. While 38.5% of the respondents expect the security issues to be resolved by the end of 2011, only 29.8% of them expect this to be true for the privacy and compliance issues. In other words, users expect privacy and regulatory compliance to slow down the evolution of their IT towards a Cloud model.

Overall, the responses show that the Cloud computing model and the dependencies between Cloud computing and other IT disciplines like service management are not fully understood. Especially the fact that Cloud computing is mainly about the optimized delivery and consumption of services is not yet widely accepted. On the other hand, there is a clear perception that security and especially IAM and GRC are core technologies to successful Cloud computing.

In short, the most important takeaway is: invest in a strategy, in organization and skills, and in technology to support security for virtualized and private cloud environments. Security is a key success factor for successful deployments in the cloud.

3 About the survey

KuppingerCole conducted an independent survey on the status and plans for Virtualization Security. This survey, which has been commissioned by CA Technologies, focused on the specific requirements that organizations have for securing their virtualized IT environments. The survey also analyzed the evolution of internal environments towards a private cloud model, again with a specific focus on the security issues around this.

The survey was conducted online during September/October 2010, with some additional phone interviews. 335 respondents participated in the survey from Germany, the United Kingdom, France, Italy, the Nordics (Denmark, Finland, Norway, and Sweden), Benelux (Belgium, Netherlands, and Luxemburg), Iberia (Portugal, Spain), Switzerland, and the USA. Thus the survey provides a representative view on the status and plans around Virtualization Security for Europe as well as for the US.

The majority of participants in the survey held senior positions in the organization. Of the participants, 6.3% are VP or Director of Security. 12.3% are Security Managers, 5.9 % are VP or Director of overall IT and 21.9% have other managerial tasks in IT. Furthermore, around 15% of the participants have other titles including CEO, CISO, and Interim General Manager which also indicate senior positions in the organizations.

Thus, just over 60% of the participants have leading positions in their organizations; whilst close to 40% have other job titles. 53.9% of the respondents are involved or highly involved in the day to day security management of virtualized environments, with 32% being partially involved.

The participants are well distributed across different industries, with Financial Services & Insurance being most represented (15.6%), closely followed by Telecoms & Media (13.8%), Public Sector (12.3%), and Manufacturing (11.9%). Other industries include Pharmaceuticals, Utilities, and others. In addition there is a significant number from MSPs (Managed Service Providers) which build and run the virtualized environments for their customers.

> The most remarkable use case and benefit of security in our virtual environment is the ability to implement the same security constraints for every VM and all users, with the same standard rules.
>
> Virtualization Security Project Lead, Forbes Global 2000 Company

38.7% of the organizations surveyed have more than 10,000 employees. 25.7% have between 1,000 and 10,000 employees, the rest having less than 1,000. However, lest this be misleading, the smaller organizations include the outsourced IT organizations of large corporations, as well as managed service providers (MSPs). Hence the number of very large IT environments is well beyond 40%. That correlates to the IT spending, with close to 50% of the organizations having IT spending above 5 million US$.

The significant number of participants and their good distribution across regions, responsibilities, and size ensure a representative and up to date view on Virtualization Security. Interestingly, there are no statistically relevant differences in the results between different regions. The US, UK, and Benelux show a slightly higher adoption rate of virtualization, but the overall perception of Virtualization Security and the way to make progress is consistent across the regions.

4 Current state of virtualization

The first part of the survey focused on the current state of virtualization in general and of virtualization security in particular.

Current state of implementation of virtualization

Interestingly, virtualization isn't the standard foundation for IT production environments in most organizations (figure 1). Only 34.2% of the organizations have deployed server virtualization for more than 50% of their systems. Those amongst the 11.4% with a deployment ratio of 70% and more were mainly small organizations and MSPs. Other types of virtualization have significantly fewer deployments:

- Storage virtualization is used for more than 50% of the systems in 16.3% of the organizations.
- Desktop virtualization is used for more than 50% of the systems in 8.2% of the organizations.
- Application virtualization is used for more than 50% of the systems in 10.0% of the organizations.

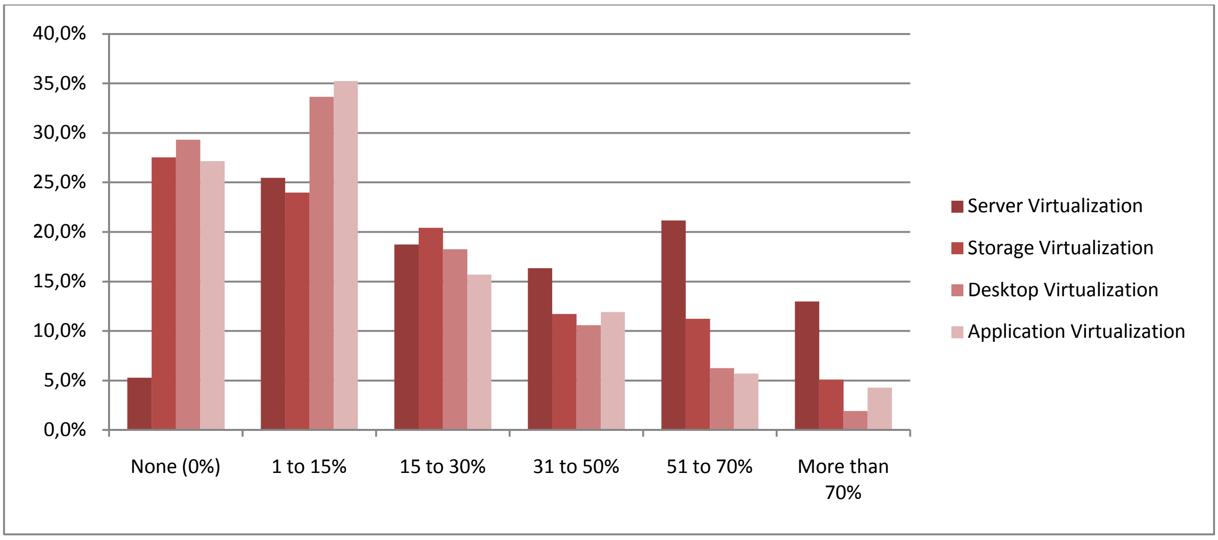

Fig. 1: Current state of implementation of virtualization approaches (% of virtualized systems from total number of systems)

Planned state of implementation of virtualization approaches by end of 2012

When looking at the planned deployments for 2012, it is clear that the primary focus of organizations is on server virtualization and storage virtualization (figure 2). By the end of 2012, deployment of server virtualization to more than 50% of the systems is expected at 50.8% of the organizations. Storage virtualization is expected to be deployed for more than 50% of the systems at 33.3% of the organizations.

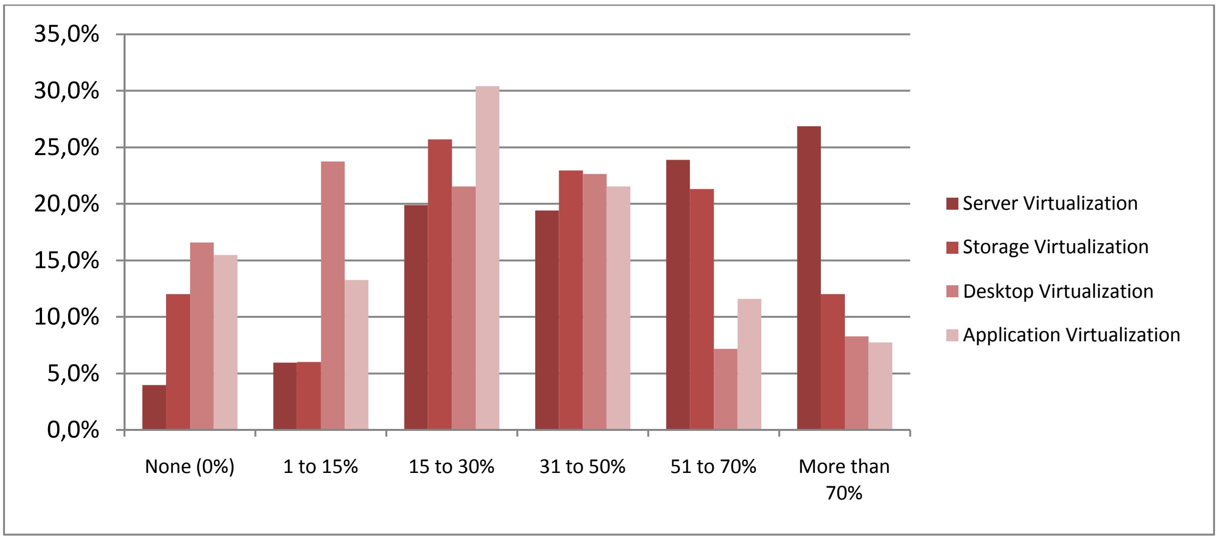

Fig. 2: Planned state of implementation of virtualization approaches by end of 2012 (% of virtualized systems from total number of systems)

From the KuppingerCole perspective, these numbers show the gap between the hype around virtualization and the reality of its phased implementation. Only 3.4% of the organizations expect not to be using server virtualization in their environment by the end of 2012. Hence virtualization is becoming a standard model. However, it takes significant time to change the existing environments from physical servers to a virtualized infrastructure. This is clearly reflected by these numbers. However there are several inhibitors to deploying virtualized IT infrastructures which will be discussed later on in this document.

Current providers of virtual server platforms

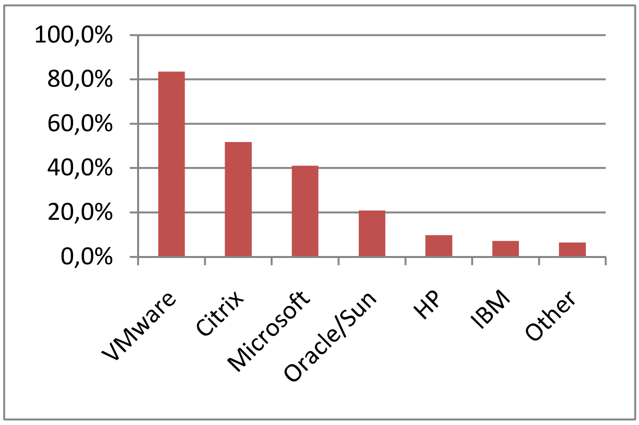

Fig. 3: Current providers of virtual server platforms (more than one answer allowed)

When looking at the providers of virtualization technologies, it is no surprise that VMware is the leader, with deployments in 83.5% of the organizations surveyed (figure 3). However, Citrix with 51.7% for their Xen technologies and Microsoft with 41.1%, mainly around Hyper-V, are following more closely than some might have expected. However, the most important finding from these results is that most organizations use at least two different providers for their virtualization technology.

These results support the KuppingerCole opinion that successful management of virtualized environments requires management tools which can flexibly and seamlessly support different hypervisors. We expect that Citrix as well as Microsoft will increase their shares of deployed virtualization technologies – and in the future others like Red Hat with KVM will also play a larger role than today.

Drivers for virtualization

When looking at the drivers for virtualization (figure 4), that the results of the survey confirm that improvement of IT operational efficiency is the most significant force. 90.8% of organizations surveyed rate this as major driver or at least a driver. This is closely followed by the control of IT costs with 82.4% of respondents citing this. Another close follower is agility with more than 75%. Agility is one of the benefits which becomes obvious once virtualized environments have reached a certain level of maturity.

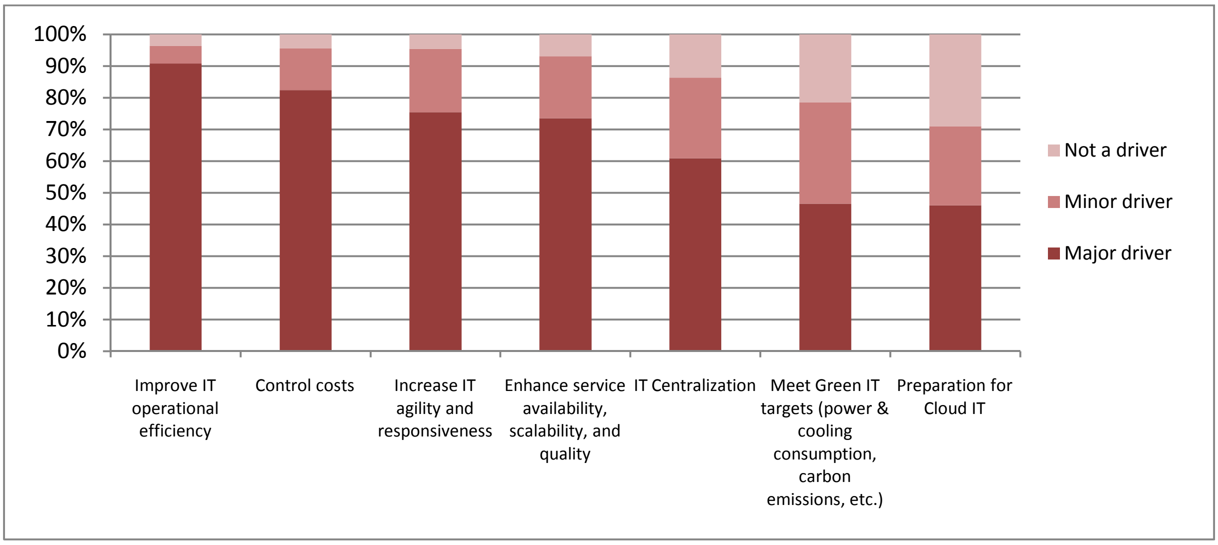

Fig. 4: Drivers for virtualization.

> Since the international company is changing quickly, the demand for services is changing. Virtualization adds the benefit to easily expand services.
>
> Security Engineer, Fortune Global 500 Company

Much more interesting is to look at which factors a significant number of organizations do not consider to be drivers. The least important is preparation for Cloud IT with 53.9% of organizations rating this as not a driver or only a minor one, this closely followed by meeting Green IT targets. Many vendors use Green IT as the justification for virtualization; however this does not seem to match the actual perception of their potential customers. The relatively low perception of virtualization as foundation for Cloud IT, on the other hand, could be a reflection of the relative immaturity of a strategic shift towards Cloud IT.

Interestingly, one of the participants that mentioned cost control as one of the major drivers found that in practice this result was not achieved. The organization actually experienced an increase in IT costs, which they claim to be a result of poor preparation. From the KuppingerCole perspective this highlights that there is a price to pay for virtualization – while infrastructures become more dynamic, the virtualization layer adds an extra level of complexity. Hence the move towards virtualization needs to be well-planned and needs to be supported by tools which help manage the extra complexity of these environments to control costs.

5 Current state of virtualization security

The second group of questions in the survey focused on the current state of virtualization security.

Inhibitors to deploying virtualization security in organizations

The results show that the major inhibitor most commonly mentioned was the lack of expertise and skills to plan and implement virtualization security. 19.3% of organizations named this as a major inhibitor (figure 5).

When looking at the sum total of responses for major inhibitor and inhibitor (i.e. excluding minor or not an inhibitor), the most significant factors were budgets and upfront cost of implementing virtualization security, as well as complexity of managing security across virtual environments and platforms. It is no surprise that budgets and upfront costs appear to be an inhibitor – security comes at a price, and unfortunately this is widely ignored when starting projects.

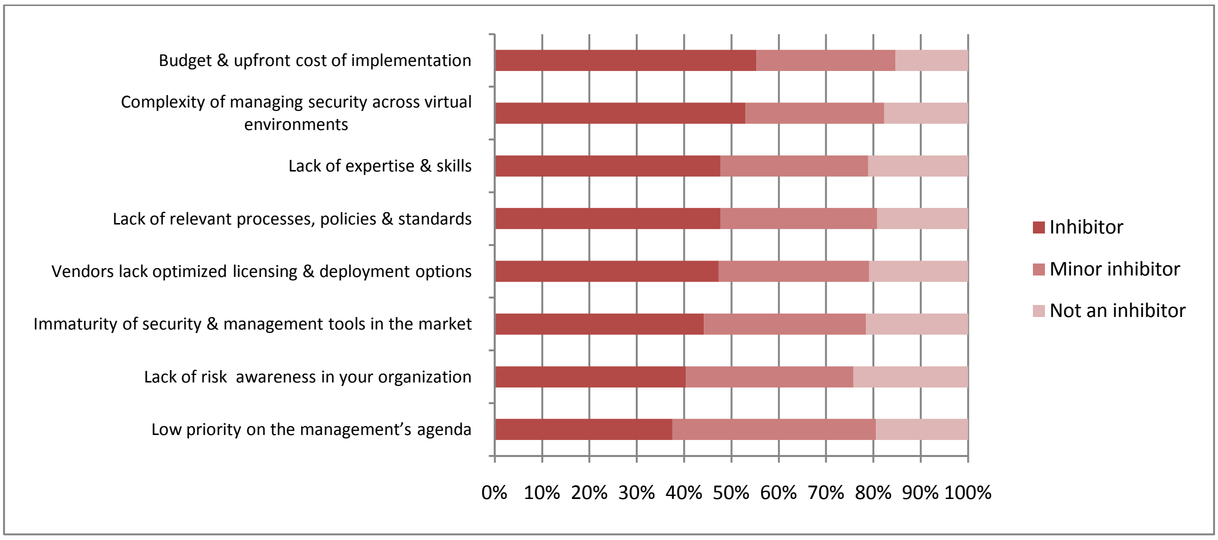

Fig. 5: Inhibitors to deploying virtualization security in organizations

From our perspective complexity has two facets. One facet is complexity in general – it is more complex to manage security for virtualized environments than for physical environments. This is because virtualization leads to an increased number of instances, the location of applications and data moving between different host systems, and other aspects of "sprawl". The other facet is the complexity of managing security across different virtual environments and platforms provided by different vendors.

Supporting security management in heterogeneous virtualized environments (which are a reality according to the results of virtualization status questions) is a key requirement for successful deployments.

> Security is the foundation for the entire virtualized environment.
>
> IT-Manager, Forbes Global 2000 Company

When looking at the factors which are considered as minor or not an inhibitor, it becomes obvious that the awareness of the need for virtualization security is not an inhibitor. Virtualization security is on the agenda of the management, and the inherent risks of virtualization are well understood by most organizations.

From the overall results, it is clear that the biggest inhibitor to virtualization security is the relative immaturity of organizations when it comes to virtualization. There is a lack of expertise and skills, and there is a lack of processes, policies and standards. There is also a lack of optimized support for security for heterogeneous virtualization environments from vendors. Also lacking are: support across the entire Host-Hypervisor-Guests stack, as well as support for optimized deployment and appropriate licensing models for virtualized environments.

> Our biggest obstacle with virtualization security is simply having staff with the skills necessary to wade through all the security challenges and offerings.
>
> Consultant, Cloud Provider

Comparing security in physical and virtual environments

Another question was about comparing the security of physical to virtualized environments. An interesting finding here is that more than 50% of the organizations rate the security issues at the same level for both types of IT infrastructures – for each of the points surveyed.

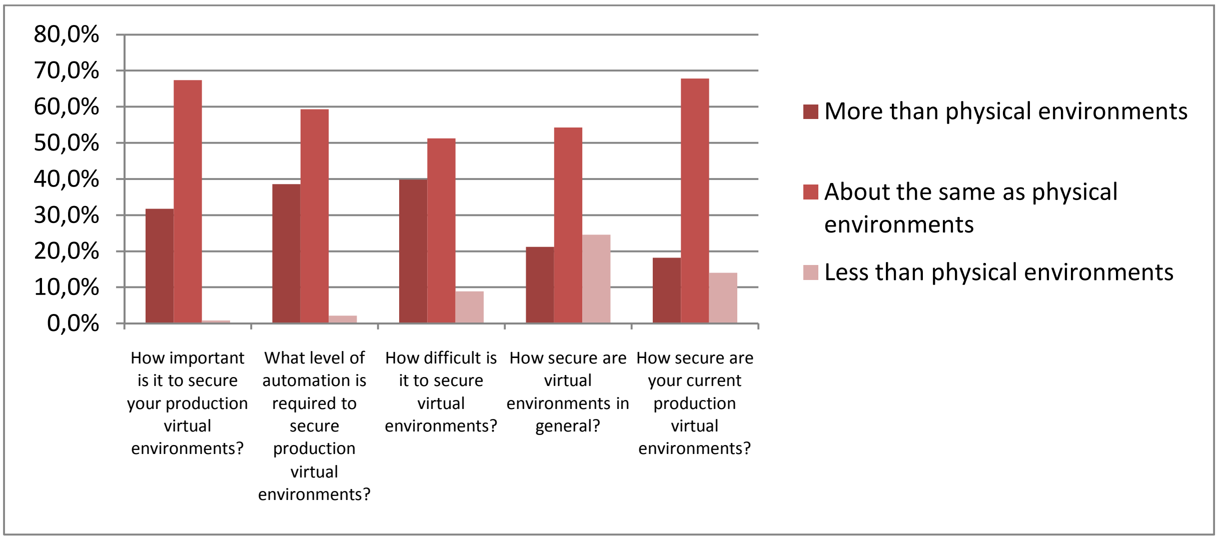

Fig. 6: Comparison of security aspects in physical and virtual environments

However, there are some interesting differences. 31.8% responded that it is more important to secure virtual environments than physical environments. The reason for that is most likely that virtual environments are more dynamic and thus the risks are higher. Only 0.8% rated the physical environments as more critical from a security point-of-view. In other words, security is more of a concern in virtualized environments.

Close to 40% of participants responded that a higher level of automation is required to secure virtual environments – and approximately the same number also responded that it is more difficult to secure virtual environments. When looking at the results in detail, respondents who think that it is more important to secure virtual environments typically expect that a higher level of automation is required and that it is more difficult to secure virtual environments. Thus, the answers to these questions appear to mainly be based on the respondent's overall perception of virtualization security as a significant threat.

Around a quarter of organizations responded that virtual environments in general are less secure than physical environments. This shows that vendors need to provide better support for virtualization security – security is a significant concern when it comes to the adoption of virtualization. It shows as well that enterprises have to work harder on getting their environments secure enough – by an integrated approach for security for both physical and virtualized environments. On the other hand, security is also an opportunity. As shown in figure 8 below, 44.7% of the respondents indicated that server virtualization might be used to improve the level of security. Virtualization can be a risk when not approached with security in mind. But virtualization is also an opportunity mitigate risks, the separation of workloads across different servers, together with a consistent approach to security, helps to achieve this.

6 Management of security in virtualized environments

The next set of questions covered the specific requirements for virtualization security.

> We handle our virtual environment almost exactly the same as our physical environment.
>
> Consultant, Managed Service Provider

Preferences for securing and managing virtual and physical environments.

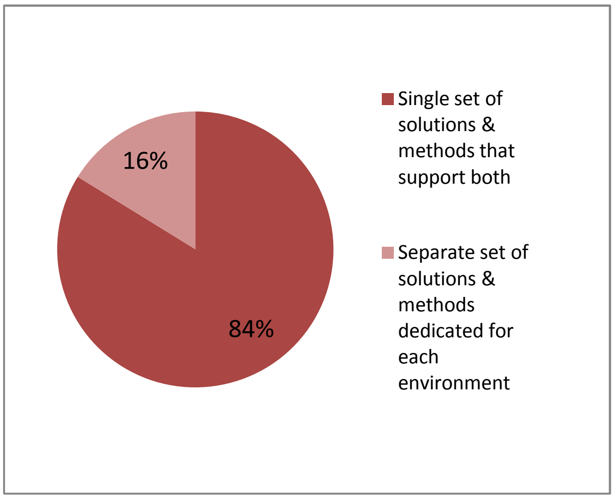

Fig. 7: Preferences for securing and managing virtual and physical environments

Unsurprisingly, most of the participants are looking for integrated solutions to seamlessly secure both virtual and physical environments; 83.8% of the participants selected that choice. This indicates that there is no significant market for "pure play virtualization security", i.e. solutions which focus only on security for virtualization technologies. However, there may be technologies which could add value to existing IT security management solutions. KuppingerCole expects to see more of these add on solutions in the short-term. Mid-term these add on solutions will converge with the existing base to provide heterogeneous support for many types of IT environments.

The potential of server virtualization to improve security posture.

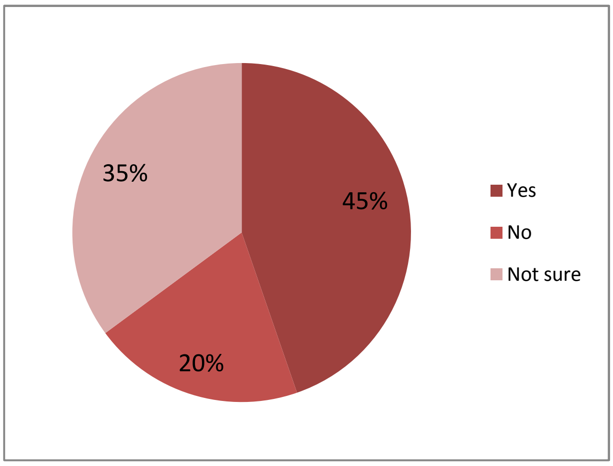

Fig. 8: Rating of the potential of server virtualization to improve security posture

The follow-up questions probed whether the participants believe that server virtualization can be used to improve the security posture and to address security issues. Interestingly, more than a third chose “Don’t know” for the answer. This shows that organizations are well aware of the security risks that virtualization creates, but they are somewhat unsure whether server virtualization, even if done correctly, could also reduce the overall security risks. However, there were more than twice as many respondents who saw a potential for server virtualization to improve security posture.

Importance of security challenges and concerns related to virtualization security

The next question turned to the importance of security challenges and concerns related to virtualization security. Notably, security aspects related to privileged users were covered in separate questions, which are discussed later on in this report. Three areas were considered as very important by at least a third of the respondents. The most important concern is around “data sprawl”, e.g. the risk of data moving around without control and ending up in less secure environments, with 41.7% considering this to be very important. Data sprawl was closely followed by maintaining compliance with regulatory and audit requirements.

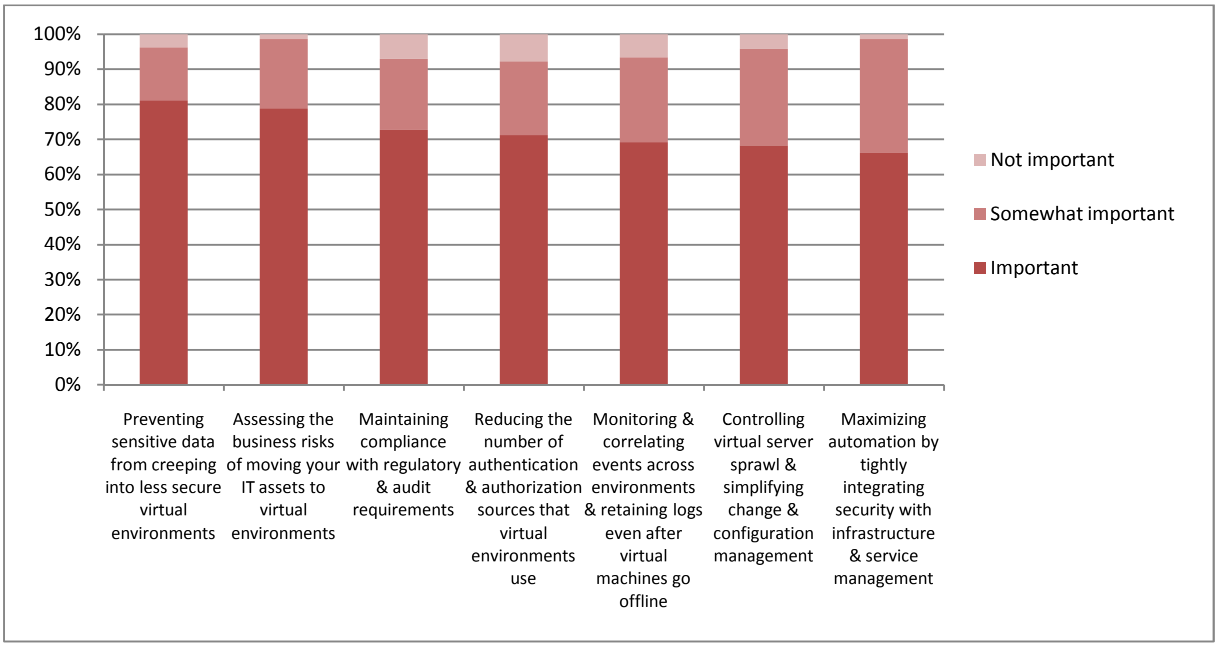

Fig. 9: Importance of security challenges and concerns related to virtualization security

However, the third concern is probably the most interesting one: 34.0% of the participants rated the assessment of business risk for moving IT assets to virtual environments as very important. Aggregating the responses for “very important” and “important”, comes to 78.8%. This shows that there is a strong appreciation of the relationship between business risks (operational and strategic) and IT risks.

Survey: Virtualization Security

Fundamental changes in the IT infrastructure, like the move to virtualized infrastructure, may affect the ability to support the business requirements in a positive or negative way. Thus it is essential to understand the business impact and especially the potential risks – like "data sprawl" mentioned above.

All choices were rated by at least 66.0% of participants as important or very important. This includes: consistent authentication and authorization in virtualized environments, monitoring and auditing of events, controlling server sprawl, and optimizing automation by tight security integration. The results clearly indicate that the respondents are well aware of two important points:

- The need for virtualization security in general.
- The need for virtualization security to go beyond single technical tools towards an integrated approach covering many different disciplines.

That fits very well with results for other questions. Virtualization security is not an isolated technical initiative but needs to be as mapped to the business requirements and risks and has to be integrated with existing IT security initiatives. Thus it is about expanding what you have, not about reinventing security specifically for virtualized environments. However, specific capabilities are required to better manage the more distributed environments and to mitigate the risks of data sprawl and server sprawl.

> The most significant obstacles and headaches for security in our virtual environment are the rights given to users to manage virtual machines, due to the lack of knowledge of the entire virtualized environment together with the lack in security management.
>
> Virtualization Security Project Lead, Forbes Global 2000 Company

Risks from privileged users in virtualized environments and status of PxM

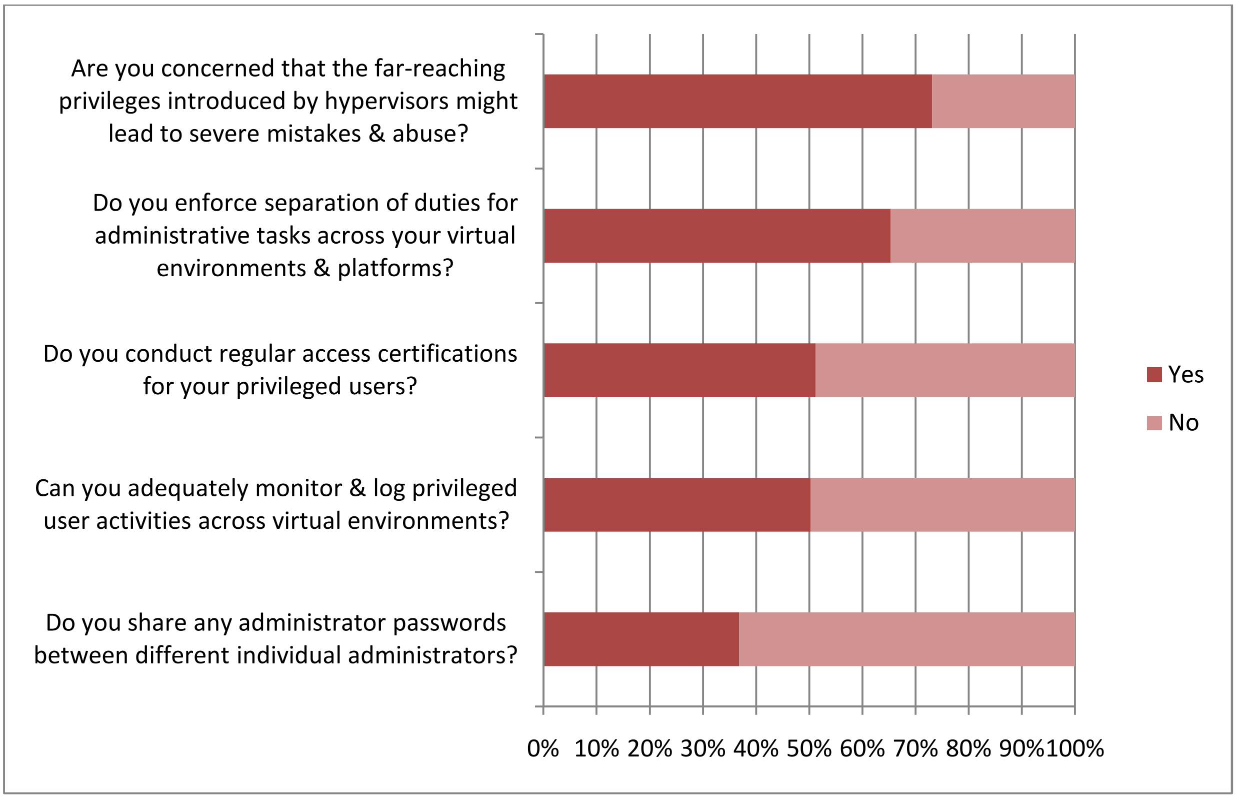

Fig. 10: Risks from privileged users in virtualized environments and status of PxM (Privileged Account/Identity/User Management) in these environments

Figure 10 shows the responses to the first set of questions which focused on specific types of risks in virtualized environments - specifically the risks imposed by privileged users, e.g. users with elevated privileges like administrators, operators, as well as technical users and other types of accounts. The responses show a significant difference between the perceptions of the risks and the actions taken to mitigate these. Nearly three quarters (73.2%) of the respondents are concerned about the far-reaching privileges introduced by hypervisors and their potential for abuse by administrators.

The Hypervisor administration account has extensive privileges with very few limitations or security controls. The Hypervisor also introduces an extra layer into virtualized environments creating new attack surfaces and opening the door to abuse by privileged.

That is tightly related to the issue of entitlement sprawl in virtualized environments – it is even harder to keep track of entitlements (including the privileged ones) in these environments. Thus, adding PxM capabilities to virtualized and cloud environments is essential to fulfill compliance requirements and to mitigate risks out of these environments.

> The most important questions are: How secure is information residing in the virtual environment? How to manage access of privileged users in virtual environments and to avoid data leakage? How will GRC policies be carried out?
>
> Solutions Architect, Fortune Global 500 Company

65.3% of responding organizations claim that they are enforcing separation of duties (SoD) for administrative tasks across their virtual environments and platforms. However, other KuppingerCole research clearly shows that there are few technical tools available in the market to enforce such SoD rules specifically in virtualized environments. It also shows that specialized tools to manage privileged access (PxM, Privileged Access-Identity-User Management) are deployed in far less than 65.3% of organizations as a strategic element of IT security. In that survey, less than 50% of the organizations claimed that they have implemented or are implementing at least one approach to PxM. So it would appear that enforcement of SoD rules for privileged access in virtualized environments is mainly achieved through organization and processes but is not sufficiently supported by technology today in most organizations.

Only around half of the organizations in the survey perform regular access certifications for privileged users or are able to adequately monitor and log privileged access. This shows that advanced technologies available to mitigate the risks from privileged access in virtualized environments are not yet widely deployed. However, adding these technologies to the IT security framework is essential to keep the security risks of virtualization under control.

Management and security capabilities for virtualized production environments

The conclusion that virtualization security in most organizations is mainly based on guidelines and processes and is not fully and adequately supported by tools is also demonstrated by the responses to the questions about the way organizations are managing and securing their virtual environments in production today and what they plan for these.

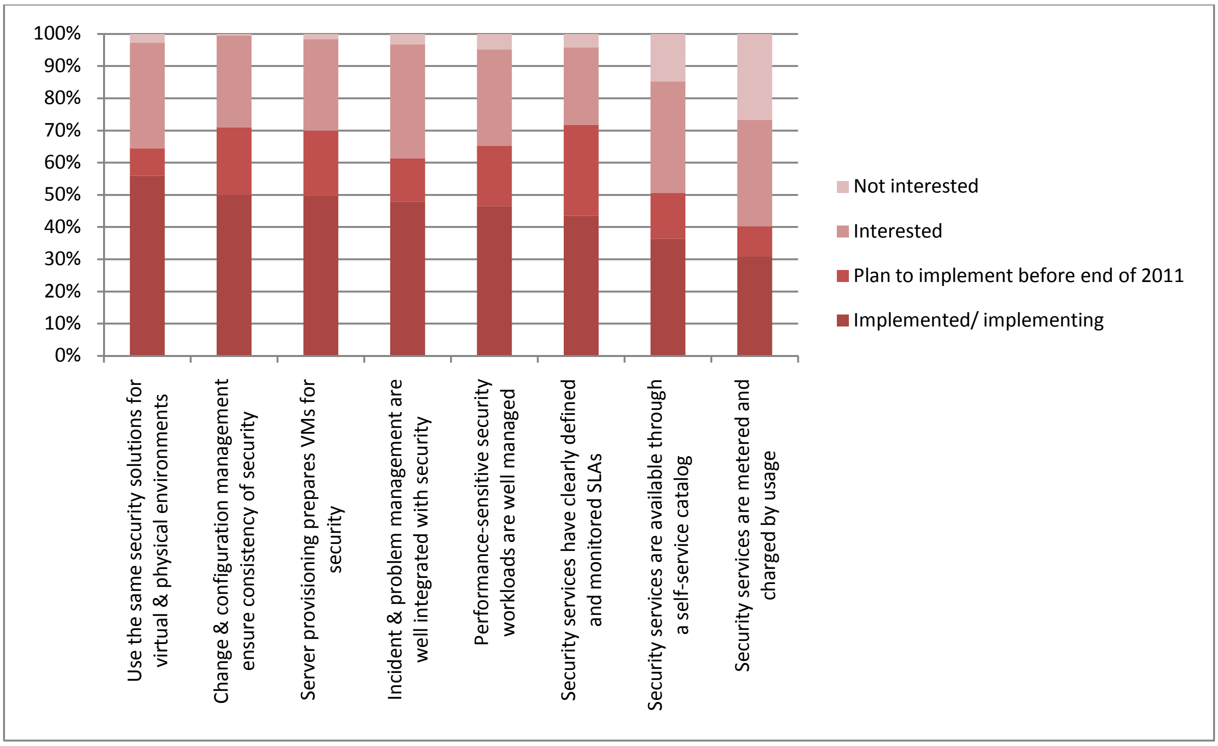

Fig. 11: Management and security capabilities for virtualized production environments

Only 55.9% of the organizations have implemented the same security solutions for virtual and physical environments or are currently in the process of implementing these. In other words, 44.1% have not yet successfully expanded their existing security infrastructure to fully support virtualized environments. Comparing these numbers with the state of virtualization deployments shows an obvious gap where the virtualization infrastructure of IT environments is not adequately secured.

Even worse is the state of integration between virtualization, security, and service management. Half of the organizations have implemented or are implementing the integration of change and configuration management with IT security management. But when it comes to the integration of virtualization security with incident and problem management, applying service levels to virtualization security management, managing performance of security services, or the integration of security services into service catalogs, the implementation rate is consistently well below 50%. From the KuppingerCole perspective, that integration is a key challenge for agile, well-managed IT infrastructures. Each service has a security context, as well as every security service should be well-managed, the same way other IT services are. Service management is used to manage the services, whilst virtualization is a foundation for flexibly providing services. The same obvious relationship exists with security. Service management, virtualization, and security are best understood as sort of a triangle with strong dependencies between all three elements. Without integration, there will be security risks – and without integration between virtualization and service management, IT infrastructures will be less agile due to the inefficient use of virtualized environments which are required to run the services.

> Having consistent and published SLAs to be able to not only measure the concerns around security and data privacy but also have the right virtualized services close to what customers need are key success factors.
>
> Security VP, Managed Service Provider

These results show that the link between IT service management and IT security management in general is understood. There is good news on this score since few organizations responded that they are not looking at the topic. For most areas, the answer “not interested” was well below 5%. The only exceptions are security services as part of self-service catalogues (11.4% not interested), and the metering and chargeback of security services (21.5% not interested). The reason for not providing security services as self services is most likely that some organizations feel that these services are not optional but are a mandatory part of any IT service they provide – whether based on physical and virtual environments. The reluctance regarding metering and chargeback, with only a 31.0% adoption rate, is driven by two factors. One is that chargeback overall is not yet tightly integrated into service management. The second is that many organizations don't see security services as something which has to be explicitly charged back; rather they see it as a fundamental part of the services provided.

Sadly, there is a long way to go to fully integrate IT service management with IT security management. This integration must be done – there has to be security management for services; and security services need to be managed consistently. The biggest challenge today is that too many vendors either support IT service management or IT security management, but do not provide integration between these areas. From the KuppingerCole perspective, such integration is one of the key decision criteria that should be considered when choosing vendors in both market segments.

Adoption of security software tools for protecting virtualized production environments

Finally, participants were asked about the deployment of specific tools for IT security management in their production virtualized environments. Again, the answers show that there is a long way to go – many security activities are obviously still based on manual processes, and are not supported by automated technology, like that for privileged accounts mentioned above.

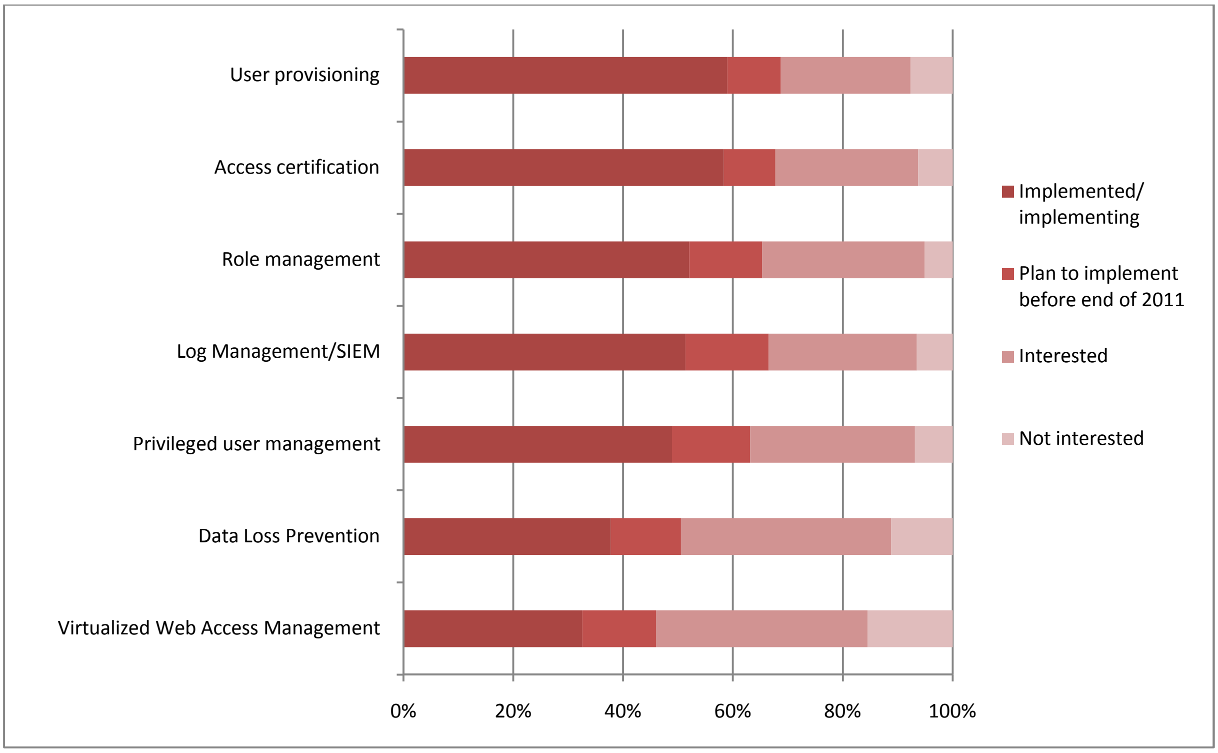

Fig. 12: Adoption of security software tools for protecting virtualized production environments

Responses show that user provisioning is available in 59.0% of the organizations. Given that this is a relatively mature topic, this shows that there are a significant number of organizations that have still not yet implemented this. In the survey provisioning is closely followed by access certification - this is a hot topic at the moment and is relatively easy to implement. Moreover, it is commonly implemented as part of provisioning solutions. Role management is slightly lower with 52.0% of the organizations having implemented this (or being in the process of its implementation). This comes as no surprise given that role management is a common element of user provisioning and access governance/certification projects.

Once again it is interesting to look at what is not yet widely deployed. PxM (Privileged Access-Identity-User Management) is a little below 50%, with few organizations expanding and upgrading their deployments. This shows that most organizations have just recently started to move beyond point solutions for specific environments to an enterprise-wide PxM approach. Log management and SIEM (Security Information and Event Management) are also available in around about 50% of the organizations.

Significantly lower deployment rates are found for virtualized Web Access Management (WAM) infrastructures. The need for WAM as part of virtualization security appears to be somewhat underestimated. This is strange since web applications are amongst the applications most virtualized (figure 13 below). WAM is also an important tool to protect the web interfaces of the virtualization technology, for example of administrative tools. Additionally web access management can itself benefit from virtualization due to the increased scalability that provides.

While web access management may be a side issue of virtualization security, Data Loss Prevention (DLP) is one of the most important technologies to mitigate the risks of data sprawl, i.e. to protect data in the context of usage policies and identities. Only 37.8% of the organizations have implemented this and, surprisingly, 11.2% are not even interested in it. From the KuppingerCole perspective, DLP and IRM (Information Rights Management) need to be considered since consistent data protection is a key element for virtualization security.

The key finding on the current state of virtualization security is that most organizations still have a lot of work to do in that area. This work is both at the organizational and conceptual level as well as in implementing the tools needed to achieve the required level of security in the virtualized environments. Not investing in this area is to ignore the well identified security threats of virtualization. Not investing means taking risks which could be easily mitigated.

7 Virtualization trends for Applications, Hosting, IT spending

The following group of questions covered further aspects around virtualization – the applications which are virtualized, hosting infrastructures, and the plans for IT spending.

Deployment of applications in virtualized production environments

When looking at applications deployed in virtualized environments, there is nothing surprising in the results. The systems most frequently virtualized (80.3%) are application servers, followed by databases (77.8%) and web applications (74.5%). The lowest ratio for virtualization is found for ERP systems – around 55%. These numbers reflect not only the technical feasibility but also the criticality of the systems.

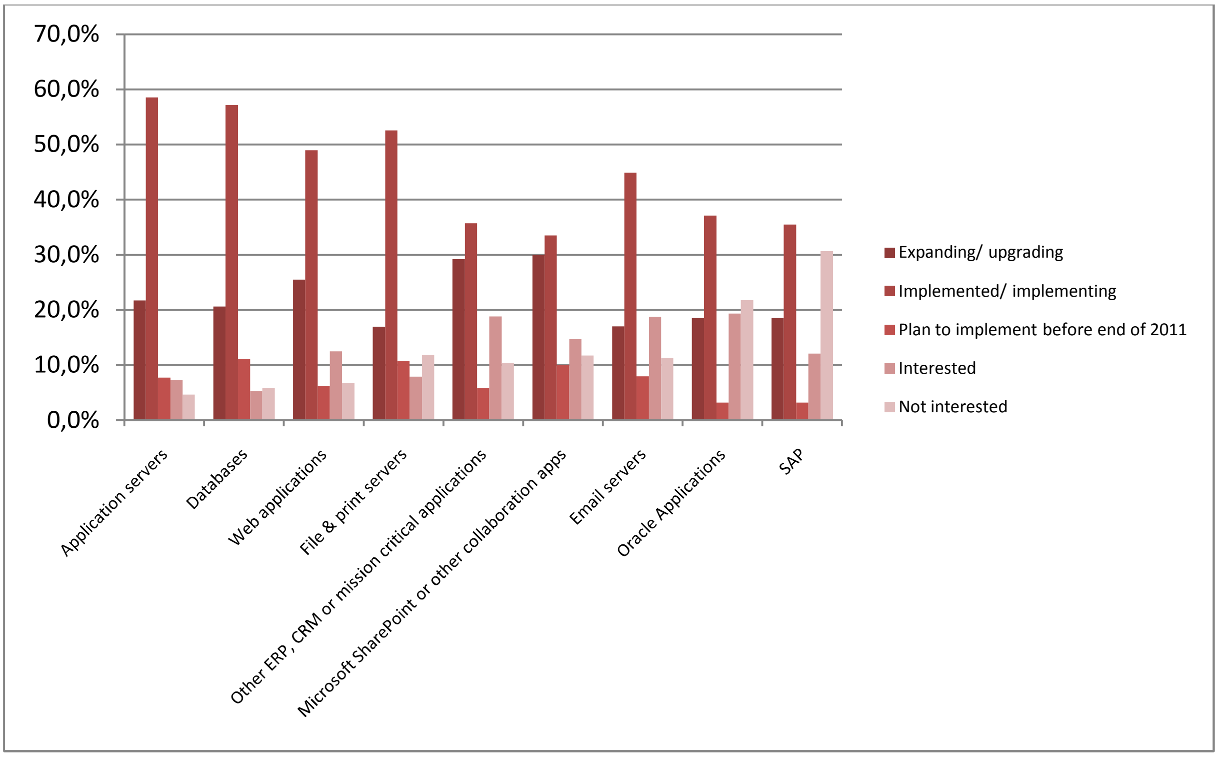

Fig. 13: Deployment of applications in virtualized production environments

Hosting of mission critical applications as of today compared to expectations for end of 2013

The expectation for the end of 2013, compared with the current state, show a slight shift to the Cloud for hosting ERP systems and other mission-critical applications. By 2013, 26.3% plan to host these applications in the cloud, compared with 13.2% today. However 81.2% (instead of 82.9%) of the organizations will continue to host such critical applications in house. The apparent inconsistency of these numbers indicates that many organizations will choose more than one approach. The increase in cloud-based deployments comes mainly from an ongoing migration of existing instances and the addition of new cloud-based services. However, the majority of mission-critical applications will still be hosted privately for a foreseeable period of time.

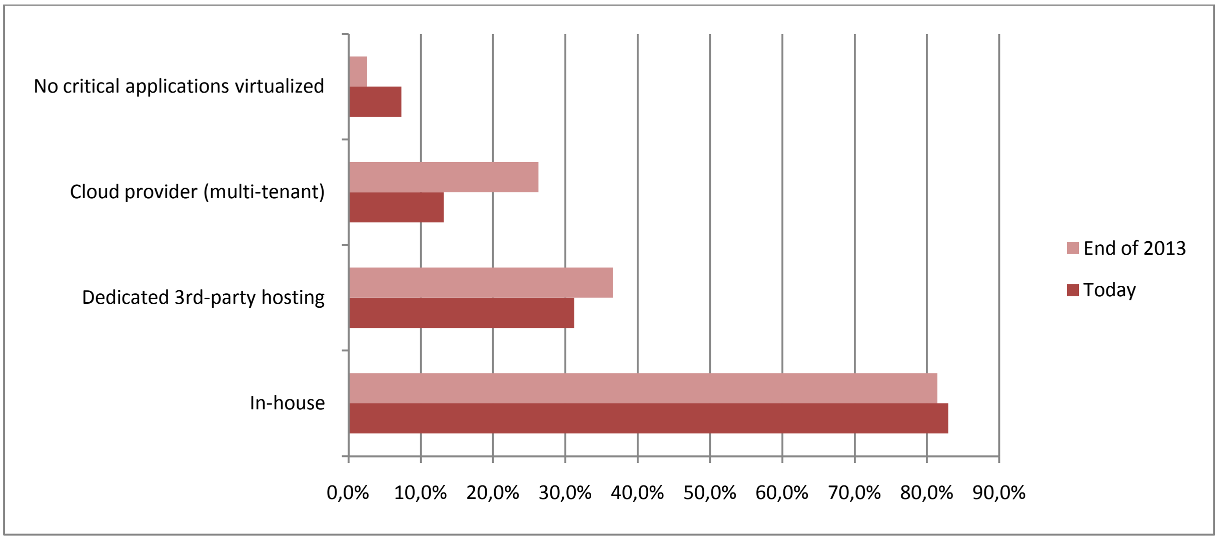

Fig. 14: Hosting of mission critical applications as of today compared to expectations for end of 2013

Use of best practice methodologies and standards to implement virtualization security

When it comes to the use of standard methodologies and best practices to implement security management for virtualized environments, roughly 60% of the participants are using ISO 2700x as a guideline and 70% are following ITIL. Interestingly, about 10% of participants claim that neither standard is sufficient for managing security – which reflects, from the KuppingerCole point-of view, both standards are lacking. Even though security and IAM (Identity and access management) aspects have been added over time, they are not yet sufficiently prominent.

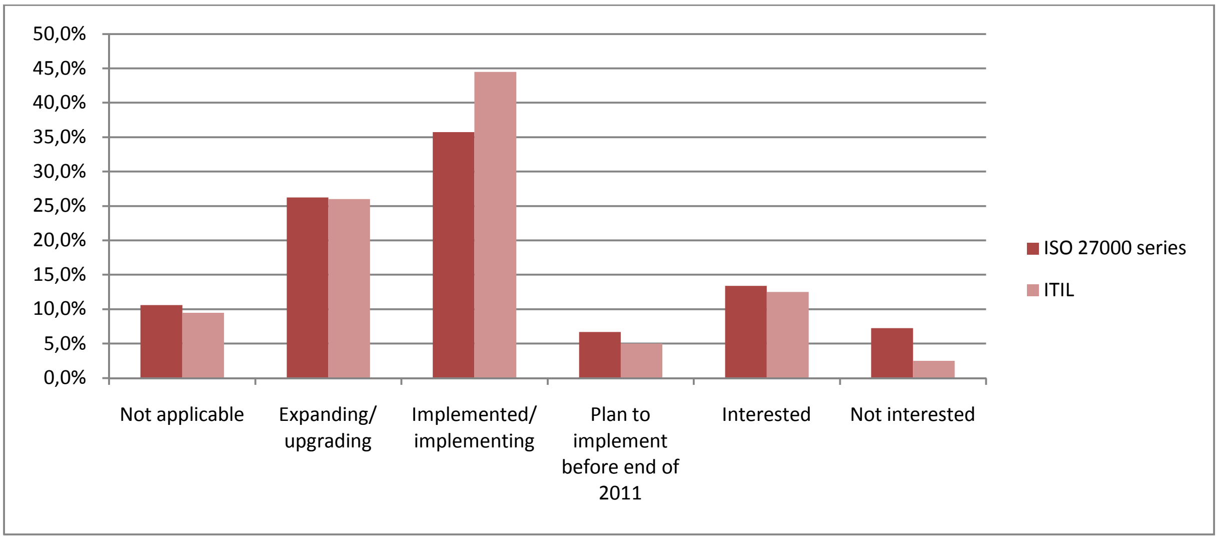

Fig. 15: Use of best practice methodologies and standards to implement virtualization security

Most important offerings that vendors should provide for virtualization security products and services

The question about the most important offerings that vendors should provide for virtualization security products delivered some very interesting results. The respondents were allowed to pick three topics from ten and prioritize them. The highest values chosen as priority 1 were: GRC (Governance, Risk Management, and Compliance) with 17.4%; the ability to manage security across multiple hypervisor platforms with 16.1%; and functionality providing identity as a service with 15.2%. These results fit well with several other findings in this survey:

- GRC is a key issue – it is necessary for understanding and managing the risks and providing sufficient controls for virtualized environments.
- Virtualization security needs to work in heterogeneous virtualized environments and must not be limited to a single platform.
- Identity management is a key element for virtualization security – but it has to be provided as a service.

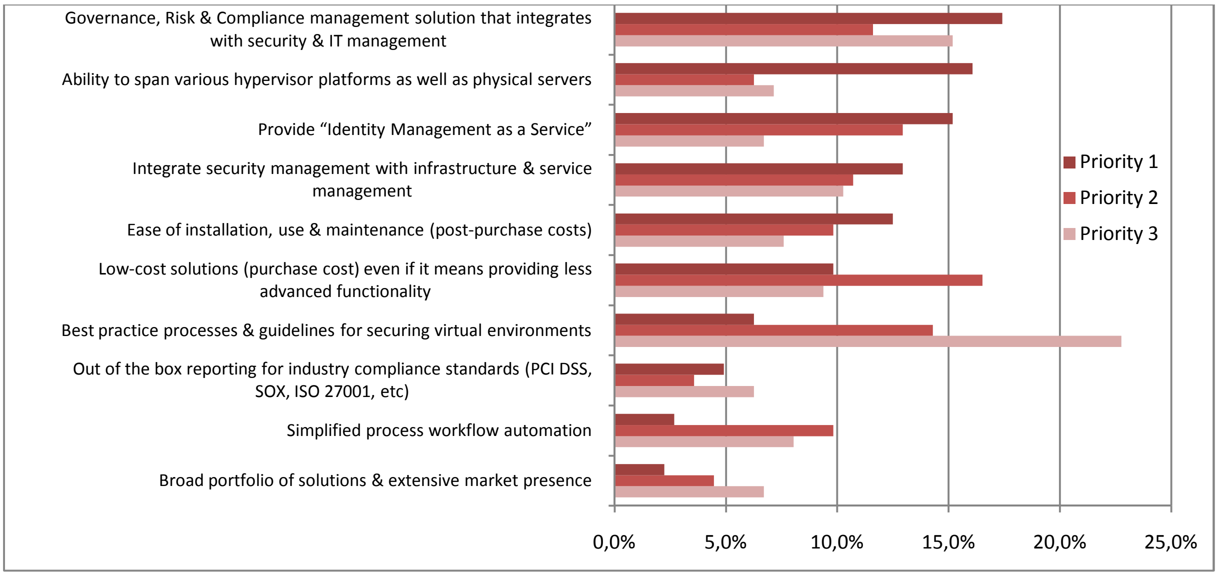

Fig. 16: Most important offerings that vendors should provide for virtualization security products and services

Most important offerings vendors should provide - aggregated priorities

When looking at the aggregated values for Priority 1 to 3, some other topics gain momentum. GRC is still top with 44.2%, closely followed by the expectation that vendors provide best practices, processes, and guidelines for securing virtualized environments (43.3%). This reflects that most organizations are still struggling with how to best implement virtualization security. Third in this ranking is providing low-cost solutions for virtualization security even at the price of limiting functionality (35.7%). This seems to indicate a view that having a little is better than having nothing.

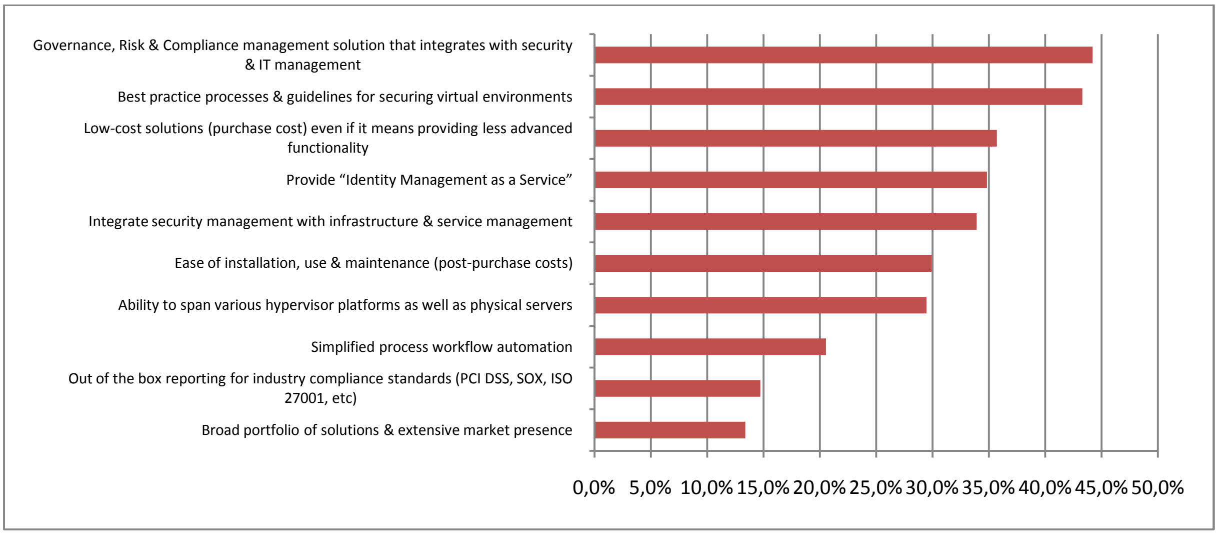

Fig. 17: Most important offerings that vendors should provide for virtualization security products and services (aggregated priorities)

Despite the fact that customers are typically looking for a one-stop-shop, the breadth of a vendor's portfolio is amongst the less important aspects from the customer's perspective (13.4%). That is likely to change over time, as integrated solutions become available; but it is typical for relatively new, immature markets. Also a little surprising is the fact that out-of-the-box reporting for standard compliance regulations like SOX or PCI is rated low (14.7%). The reason behind this is most likely that organizations are looking beyond simple compliance reporting and are increasingly ready to adopt more mature solutions. These advanced capabilities are provided by GRC solutions and therefore there is no need for isolated reporting solutions.

Focus and priorities of organizations within the next 12 months

Another interesting finding from the survey concerns the priorities of IT organizations for the next 12 months. While overall IT spending will increase in only 19.6% of organizations and decrease in around the same percentage, 52.2% of the responding organizations plan to increase their spending on virtualization security during the same period.

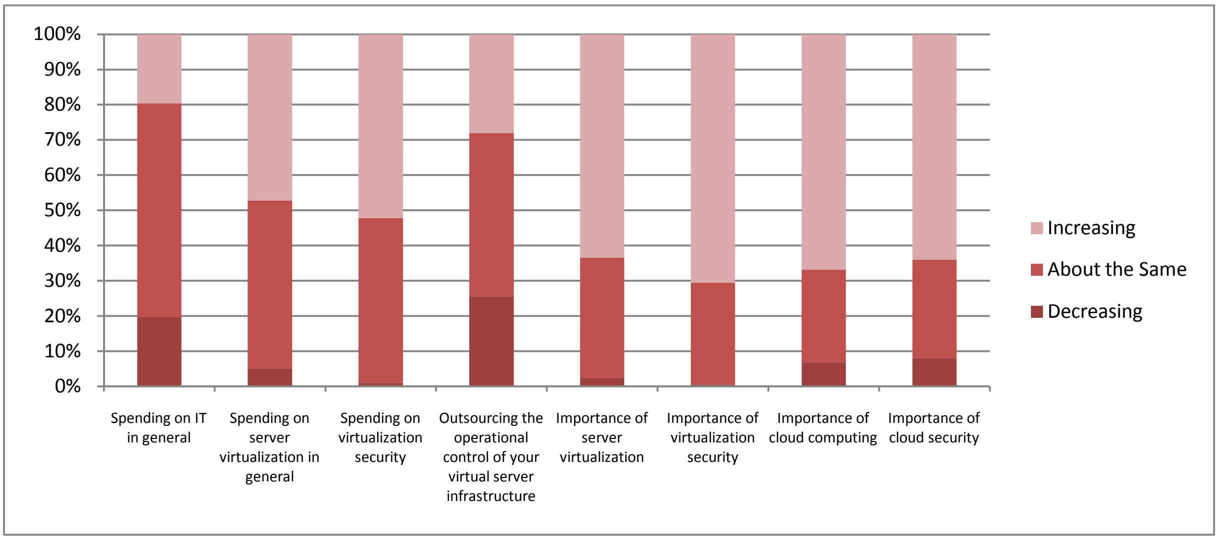

Fig. 18: Focus and priorities of organizations within the next 12 months

These results show that Virtualization security is a key priority for organizations – 66.8% rated it as becoming more important than today during the next 12 months. Cloud Computing and Cloud Security follow closely with a rating of 66.8% and 64.0% respectively. However, most organizations plan to retain the operational control of their environments in house; 28.0% plan to put more emphasis on this, while 25.5% plan to do more internally. This raises another important point: Cloud Computing is a way of externalizing the operation of IT and not about externalizing control. And even when looking at on-premise/in-house private clouds, e.g. IT environmens run as private internal clouds, there is segregation between operation and control. Control still has to be done centrally.

8 Trends and Plans for Private Clouds

The last section of the survey asked about the plans organizations have for private cloud, e.g. applying cloud computing principles, like flexible, standardized, service-based management concepts, to their internal IT.

Current and expected use of private cloud environments

While 18.8% of respondents have private clouds right now, an additional 33.5% of organizations expect to have such environments by the end of 2012. However, 23.9% don’t feel ready to take the step towards a private cloud because of the immaturity of their virtualization practices. The remaining 23.9% either doubts that private clouds are mature or secure enough or doesn’t see a business benefit in implementing cloud models for their internal IT environments.

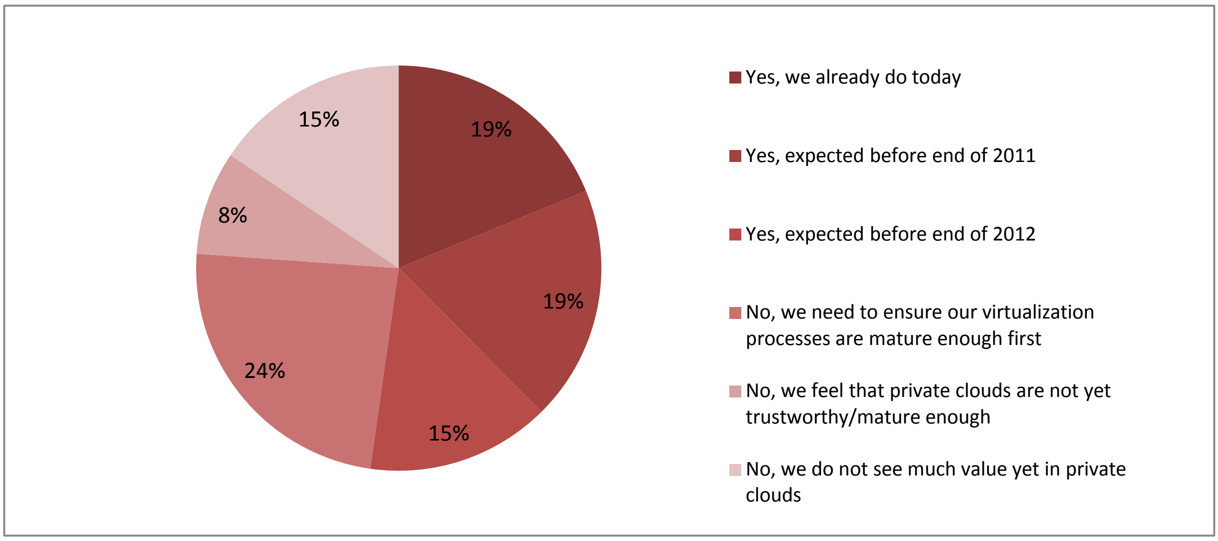

Fig. 19: Current and expected use of private cloud environments

> When buying or offering cloud-based services, it is very important to be clear on the responsibilities of the supplier and the client. Who manages which security aspects and how?
>
> Security Manager, Consulting and Auditing Organization

Inhibitors for moving to cloud computing

When asked for the major inhibitors to move quickly towards a private cloud model, the biggest inhibitors mentioned were: cloud privacy and compliance issues (84.9%), and cloud security issues for external cloud services (84.4%). Interestingly, the security issues for all types of cloud providers are expected by a larger number of respondents to become removed within 2011 – obviously, people expect the security provilems with external cloud services to be more difficult to solve. While 38.5% of respondents expect the security issues to be removed by the end of 2011, only 29.8% of them expect the privacy and compliance issues to be resolved by then. In other words, users expect that privacy and regulatory compliance will slow down the evolution of IT towards a cloud model.

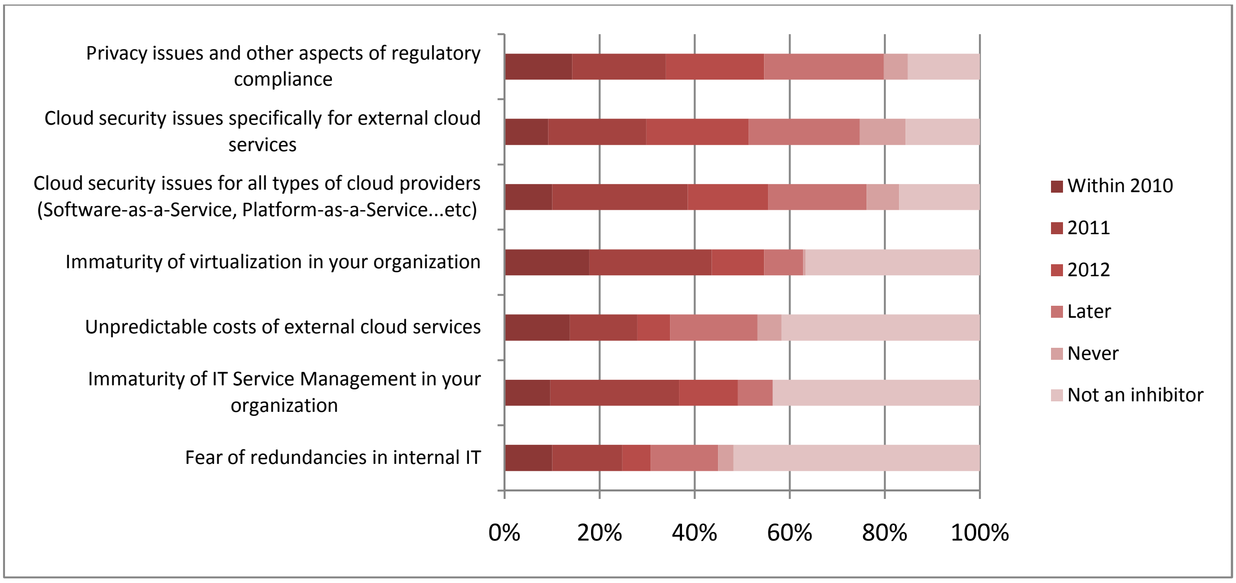

Fig. 20: Inhibitors for moving to cloud computing & when are these inhibitors expected to be removed

On the other hand, factors which are not seen as inhibitors include: the immaturity of virtualization (Not an inhibitor: 36.7%), a lack of predictability of costs for cloud services (41.7%), the immaturity of IT service management in organizations (43.6%), and the fear of redundancies in potentially more efficient cloud infrastructures (51.8%). However, most organizations expect that it will take them around 1-2 years to improve the maturity of virtualization and IT service management in their organizations. From the KuppingerCole perspective, this seems to be somewhat too optimistic and could slow down the (inevitable) migration of IT infrastructures towards cloud computing.

> The primary obstacle for us is regulatory compliance as we are in a heavily regulated industry.
>
> Architect, Forbes Global 2000 Company

Importance of the IT management capabilities for running a virtualized private cloud environment

When looking at the IT capabilities required for running private cloud environments, the top 3 points rated as “very important” are:

- Ensuring compliance with external and internal regulations (47.7%)
- Auditing administrators and operators of external service providers (39.0%)
- Managing the access to information and services consistently for internal and external users (37.2%)

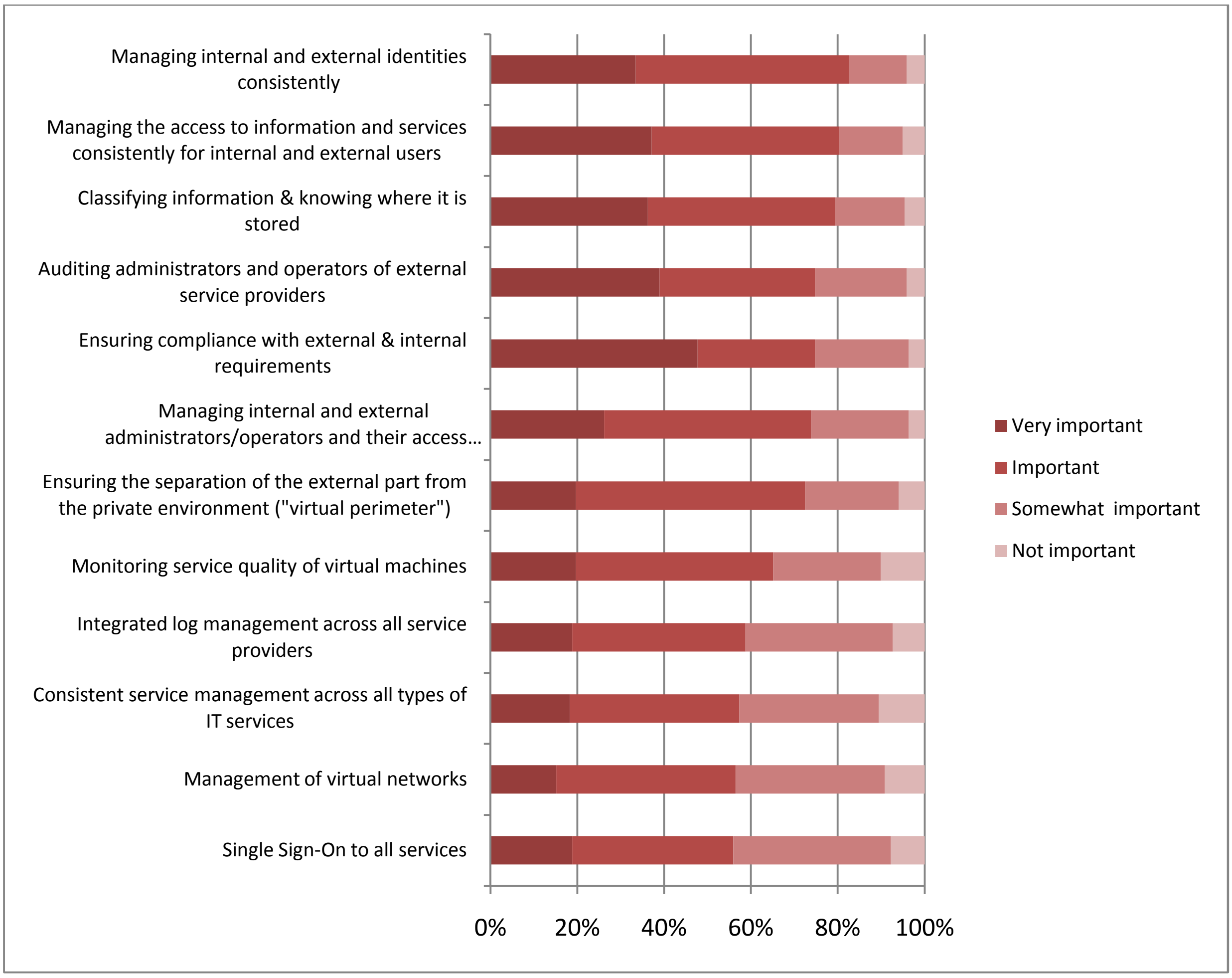

Fig. 21: Importance of the IT management capabilities for running a virtualized private cloud environment

These points highlight that there is no clear distinction between private and public clouds, and that private clouds, whether hosted internally or externally, need to be treated in the same way.

The second point, auditing the administrators and operators of external service providers; once again this supports the case for PxM. The third point highlights the fact that cloud computing requires a consistent strategy for IAM (Identity and access management).

Totaling the responses of “very important” and “important”, reveals that “Managing internal and external identities consistently” (82.6%) is the most important capability. This means having one consistent IAM approach for everything. Managing access to information comes second (80.3%), followed by “Classifying information & knowing where it is stored” (79.4%). Note that, this is not just about knowing where the data is stored, but also classifying information – an organizational task which is essential for successful implementation of virtualization and cloud security. Given that it is widely accepted that organizations need to improve their information classification, it is even more surprising that the value of DLP (Data Leakage Prevention) and IRM (Information Rights Management) for virtualization security is rated so low. Information classification is a prerequisite to information security – and DLP and IRM are the technologies which make real use of classified information to achieve that end.

The externalization of authentication and authorization has the lowest response (54.1%). However, from the KuppingerCole perspective, this is essential to a flexible security approach in cloud environments. Unfortunately, despite there being some products around entitlement management, educating software architects, developers, and IT security professionals about the why and how of externalization is still a long journey.

Other functionalities receiving a low response rating, between 56.0% and 58.7%, are: Single Sign-On, log management integrated across all providers, management of virtual networks, and consistent service management across all providers within a private cloud infrastructure. From the KuppingerCole perspective, the last point is rather critical. Good service management is a key prerequisite for cloud computing, because cloud computing is about the optimized delivery and consumption of services.

Importance of technologies for running private clouds

The last question (figure 22) analyzed the importance of technologies for running private cloud services. The answers correlate well with the findings of the question around IT capabilities discussed above.

The technologies with the highest ratio of “very important” are: server virtualization (48.2%), virtualization management (39.0%), and storage virtualization (38.1%). However, when looking at the combined scores for “very important” and “important”, server virtualization is still top but identity and access management (IAM) now comes second with 81.7%.

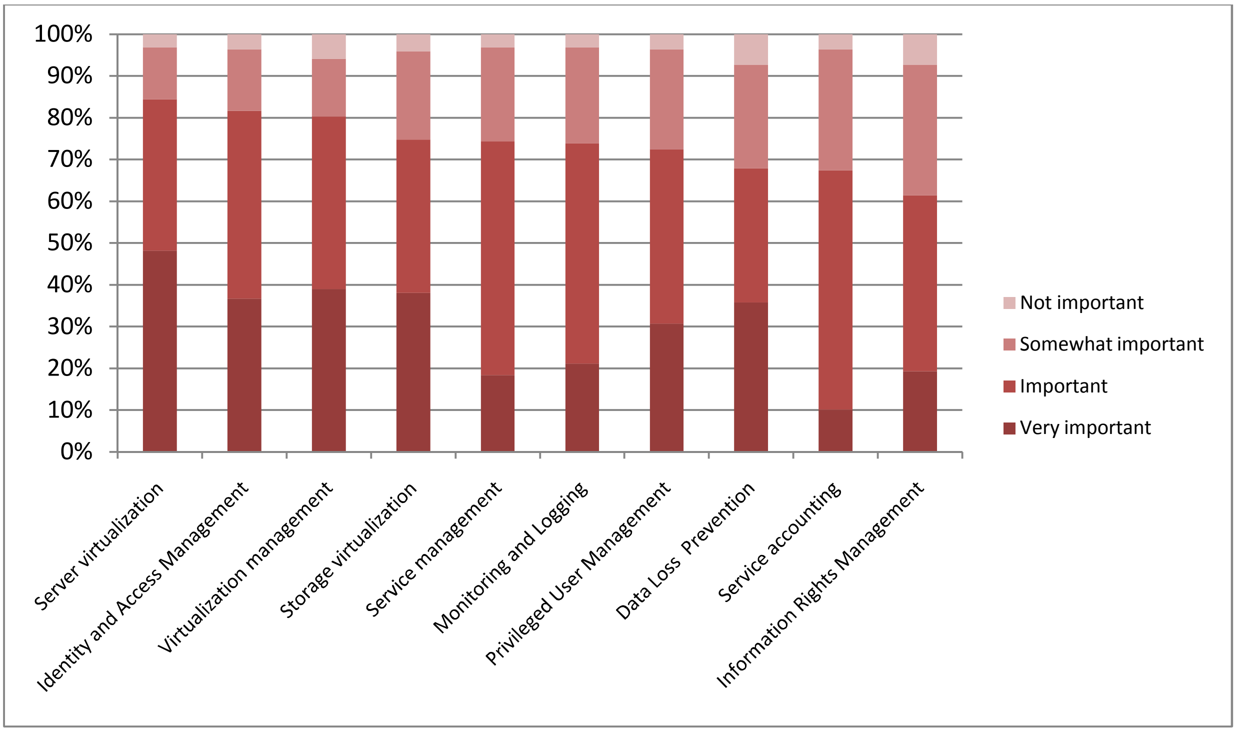

Fig. 22: Importance of technologies for running private clouds

It comes as no surprise, that Information Rights Management (IRM) with 61.5%, Service Accounting with 67.4%, and Data Leakage Prevention with 67.9% have the lowest ratings from the respondents. This is consistent with other results of this survey. Nevertheless, KuppingerCole rates these technologies significantly higher but expects their adoption to be slow.

Overall, the results from this section show that the concept of cloud computing and the dependencies between cloud computing and other IT disciplines like service management are not fully understood. Especially the fact that cloud computing is essentially about the optimized delivery and consumption of services is not widely accepted. On the other hand, there is a clear perception that security and especially IAM and GRC are core technologies for successful cloud computing.

9 Demographics

KuppingerCole conducted an independent survey of the status and plans for Virtualization Security amongst organizations. This survey focused on the organization’s specific requirements for securing their virtualized IT environments. The survey also analyzed how internal IT environments are evolving towards a private cloud model, again with a specific focus on the security issues involved.

The survey was conducted during September/October 2010 as an online survey, with some additional ‘phone interviews. There were 335 participants in the survey. A little over 60% of the participants hold leading positions in their organizations; whilst close to 40% have other roles. 53.9% of the participants are involved or highly involved in the day to day security management of virtualized environments.

38.7% of the organizations have more than 10,000 employees. 25.7% have between 1,000 and 10,000 employees, the rest having less than 1,000. However, the smaller ones include outsourced IT organizations of large corporations as well as Managed Service Providers (MSPs) thus the number of very large IT environments is well beyond 40%. That correlates to the IT spending, with close to 50% of the organizations having IT spending above 5 million US$. The significant number of participants and their distribution across regions, responsibilities, and size provide a valid and current view on Virtualization Security.

Appendix

Short profile of KuppingerCole

KuppingerCole, founded in 2004, is a leading Europe-based analyst company for identity focused information security, both in classical and in cloud environments. KuppingerCole stands for expertise, thought leadership, and a vendor-neutral view on these information security market segments, covering all relevant aspects like Identity and Access Management (IAM), Governance, Risk Management and Compliance (GRC), IT Risk Management, Authentication and Authorization, Single Sign-On, Federation, User Centric Identity Management, eID cards, Cloud Security and Management, and Virtualization. KuppingerCole stands for Thought Leadership in and a deep knowledge of all covered market segments. KuppingerCole supports you in mitigating your risks when making decisions.

Research and Analysis Services

The core element of KuppingerCole research are the reports. KuppingerCole provides different types of reports, from vendor reports and product reports to comparative segment reports and trend reports on emerging market segments. KuppingerCole provides thought leadership and a vendor-neutral view on the status of the markets, products, and vendors through these reports. The large number of existing reports and a significant number of new reports published every year ensures that you can access always the up-to-date information you need for your decisions. Beyond these standard reports, KuppingerCole provides custom research on products and markets.

Advisory Services

Based on our research, KuppingerCole provides advisory and coaching services. KuppingerCole develops and maintains roadmaps for IAM, GRC, and Cloud Computing as a structured, standardized guideline for strategies and deployments, including defined maturity levels based on Key Performance Indicators. With its advisory services, KuppingerCole supports the definition of visions, strategy, and project roadmap. Beyond that, KuppingerCole might assist you in product decisions and project reviews. The proven approach of KuppingerCole focuses on lean, efficient projects, with a structured methodology based on the ongoing research, the publications, and the thought-leading and deep knowledge of KuppingerCole analysts. Please note that KuppingerCole doesn´t provide any implementation services. We are fully focused on vendor-neutral advisory services.

Events

The KuppingerCole flagship event, the European Identity Conference (EIC), is held annually. KuppingerCole's Cloud 2011 and Mittelstandsdialog Informationssicherheit 2011 will be co-located with EIC in May 2011 in Munich. All conferences provide thought leadership and best practices on identity focused information security and IAM, GRC and Cloud Computing. Besides these main events, KuppingerCole is one of the leading provider of Webinars and Virtual conferences around these topics. These online events are free of charge and provide up-to-date insight into hot topics in all research areas covered by KuppingerCole. These online events are complemented on occasion by single-day workshops which provide the opportunity for an intensive dialog with KuppingerCole analysts. With its event services, KuppingerCole provides support to vendors and integrators for custom events, including keynote speeches, content and marketing services, and full service offerings for events.