2010 State of Virtualization Security Survey

Current opinions, experiences and trends on the strategies and solutions for securing virtual environments

8815 Centre Park Drive
Columbia MD 21045
877.333.1433

Published: April, 2010

Executive Summary

Over a period of 2 weeks in March 2010, Prism Microsystems conducted a web-based survey on virtualization security that was completed by 302 IT professionals across multiple industries and company sizes. The survey was designed to yield data on the current and future adoption of virtualization and to gauge opinions and experiences on virtual environment security concerns, controls, and implementation.

The survey was posted on the Prism Microsystems website, and invitations to participate were sent to Prism Microsystems customers and over 50,000 subscribers to the EventSource newsletter. In addition, the survey was made available to the general public via social media platforms such as Twitter and Linkedin. All responses were automatically collected by a commercially available survey tool. Skipping of questions was not allowed.

Percentages shown in some charts will not add up to 100% because of the option to select multiple responses.

Key Findings and Analysis

1. **Virtualization is widespread but penetration remains low**

- 85% of all surveyed have adopted virtualization to some degree, yet the degree of penetration for the majority (53.46%) is low with only up to 30% of production servers virtualized
- This is expected to increase to over 60% by the end of 2011 for the majority of respondents
- Only slightly more that 10% were currently solidly down the road to virtualization with more than 60% of the available production servers virtualized
- The buzz around desktop virtualization has not translated into adoption, with 59% having no immediate plans to implement the technology

Figure 1: What percentage of your production servers is currently virtualized?

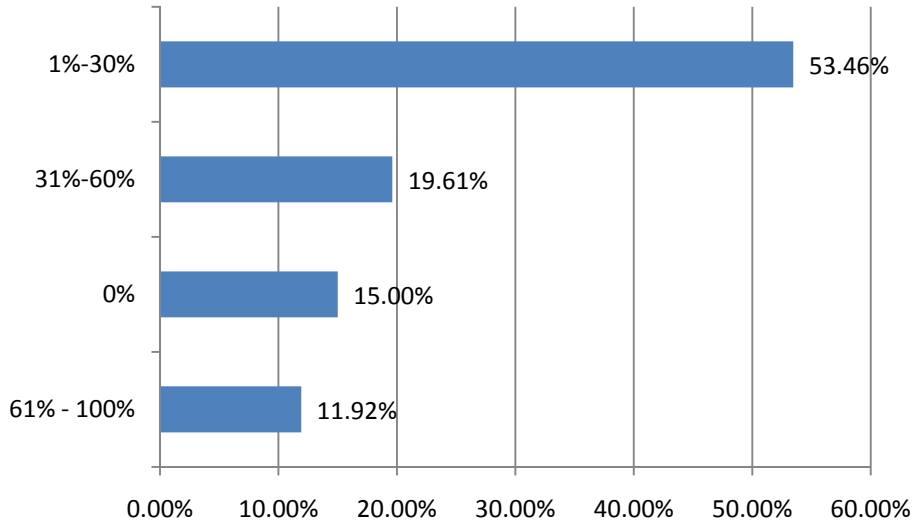
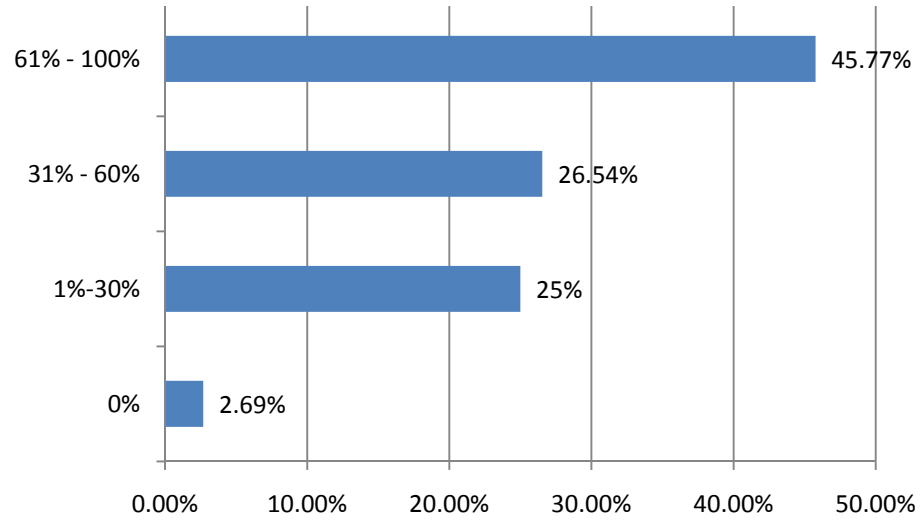
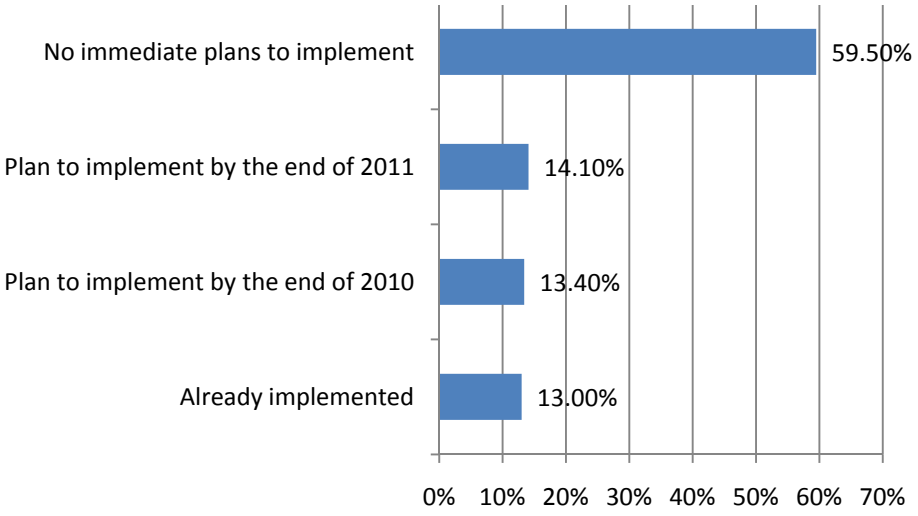


Figure 2: What percentage of your production servers do you expect to virtualize by the end of 2011?



***

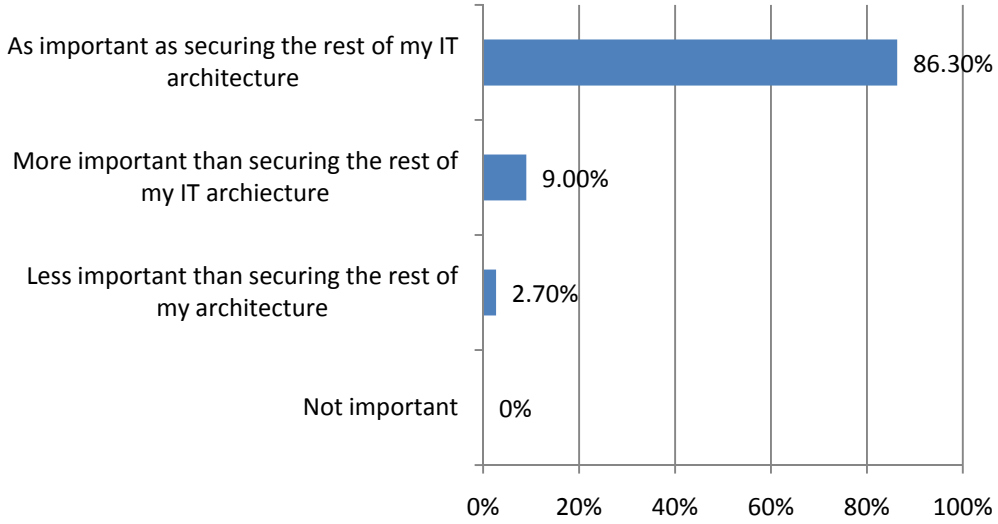
Figure 3: Are you considering implementing desktop virtualization in your organization?



2. Traditional security solutions, processes and strategies are still being applied to the virtual environment

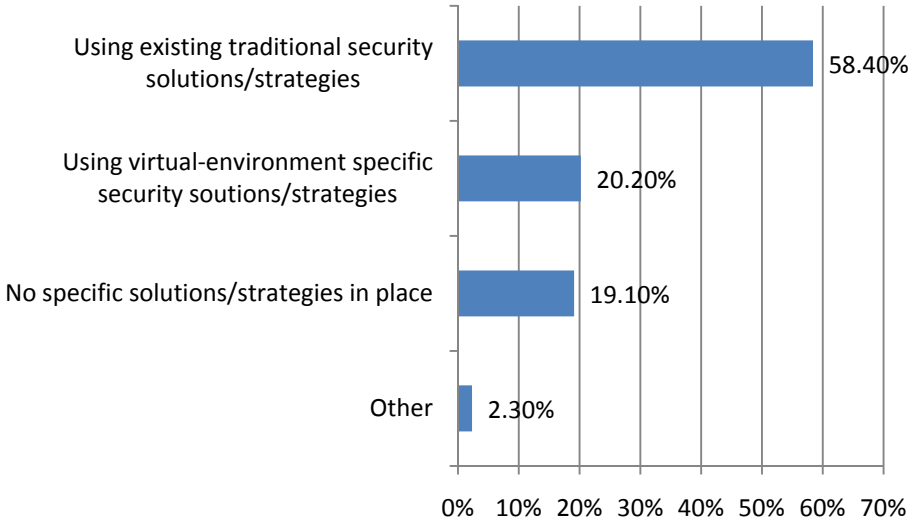
- Predictably 85% of respondents indicated that securing their virtual environment is as important as securing their physical environment (Fig. 4)
- Almost 60% of respondents indicated that they are using existing traditional security solutions to secure their virtual environments (Fig. 5)

Figure 4: How important is it for you to secure your virtual environment?



***

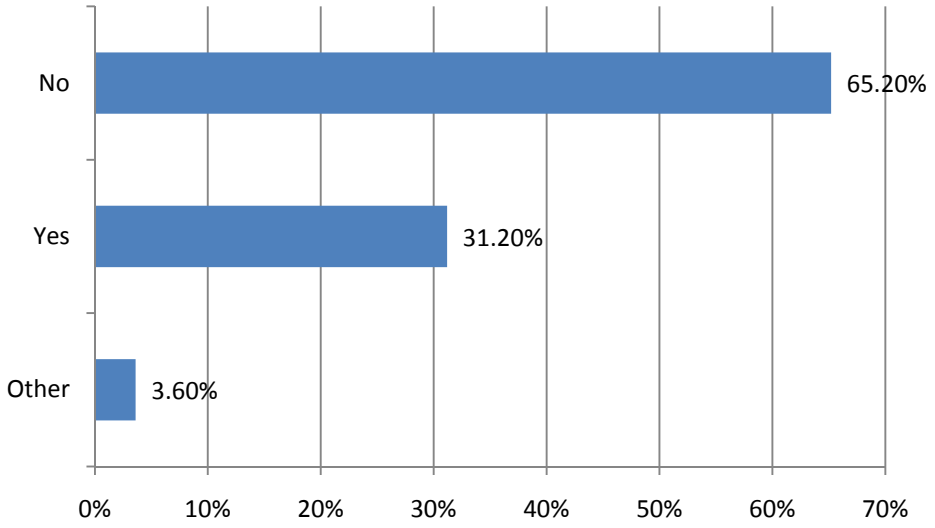
Figure 5: How are you securing your virtual environment?



This approach is problematic considering that virtual environments are characterized by dynamic moves and changes, making it harder for traditional security controls to keep up. Applying technologies, best practices and strategies used for securing physical environments does not provide sufficient protection for virtual environments since several areas are overlooked completely, such as:

- **Separation of duty for administrative activity**: Over 65% of respondents indicated that they have not implemented separation of duty between IT personnel responsible for the provisioning of virtual machines / virtual infrastructure and other administrator groups (Fig. 6), as such giving too much privilege and capability to administrators. This raises the risk for abuse by privileged insiders - a concern that is shared by 34.9% of respondents, who acknowledged the greater potential for abuse resulting from an extended span of control available to administrators (Fig. 7). Beyond the insider issue, compromise of the credentials of the virtual administrator can also provide an outside hacker with the keys to the castle.

Figure 6: have you implemented separation of duty best practices so that IT personnel responsible for the provisioning of virtual machines and the virtual infrastructure are separate from other admin groups?



- **Protection of the virtualization layer:** The introduction of virtualization creates a new platform that needs to be secured (the Hypervisor and VM Management applications). While industry pundits believe that a massive failure associated with a hypervisor-based attack is somewhat theoretical, for respondents it is a real concern.

    - The top 2 security concerns related directly to the virtualization layer: 56.6% identified "The introduction of a new layer that can be attacked" as a concern, and 58.1% indicated "The potential for the Hypervisor to create a single-point of entry into multiple machines instances" as a concern (Fig. 7)
    - Only 16% of those surveyed indicated that they had no specific security concern with virtualization (Fig. 7)

Figure 7: Which of the following are security concerns for you when it comes to virtualization? (Multiple selections allowed)

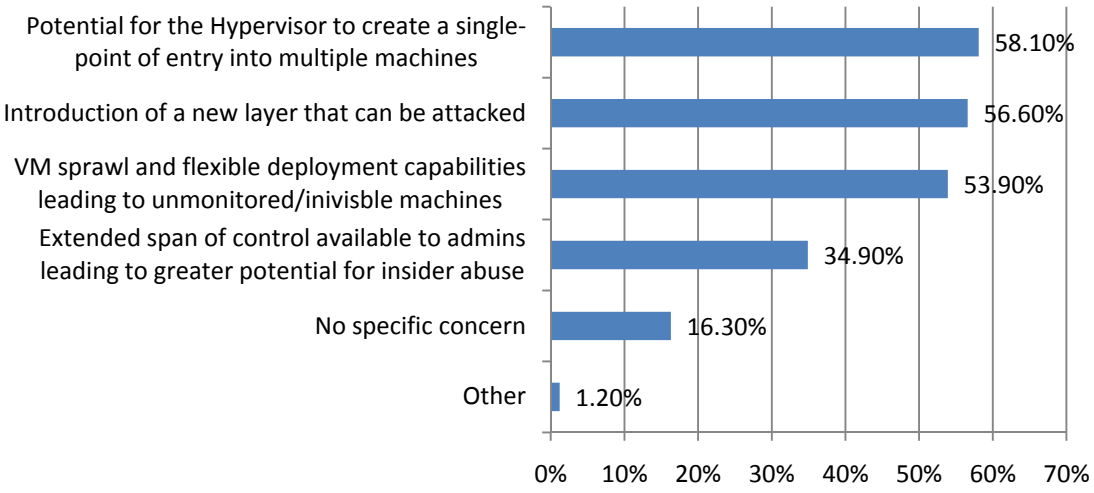


Figure 8: Rank each of the statements below to the best of your knowledge

	Strongly Agree	Agree	Unsure	Disagree	Strongly Disagree
Virtual environments are inherently less secure than physical environments	2.70%	23.50%	21.80%	48.20%	3.80%
Traditional security solutions are sufficient to provide security insight into all layers of the virtual environment (Hardware, Hypervisor, Guest OS)	3.40%	20.80%	24.50%	46.20%	5.10%
Threats exposed by virtualization can be mitigated by using existing processes and technology	5.10%	41.00%	29.50%	20.50%	3.80%
Monitoring the virtualization layer (Hypervisor, VM management apps) of the virtual environment is important for risk mitigation	22.20%	57.30%	16.20%	4.30%	0.00%
Tracking and reporting on unauthorized user activity, data access and privileged user activity is important across the enterprise	44.00%	45.30%	9.00%	1.30%	0.40%

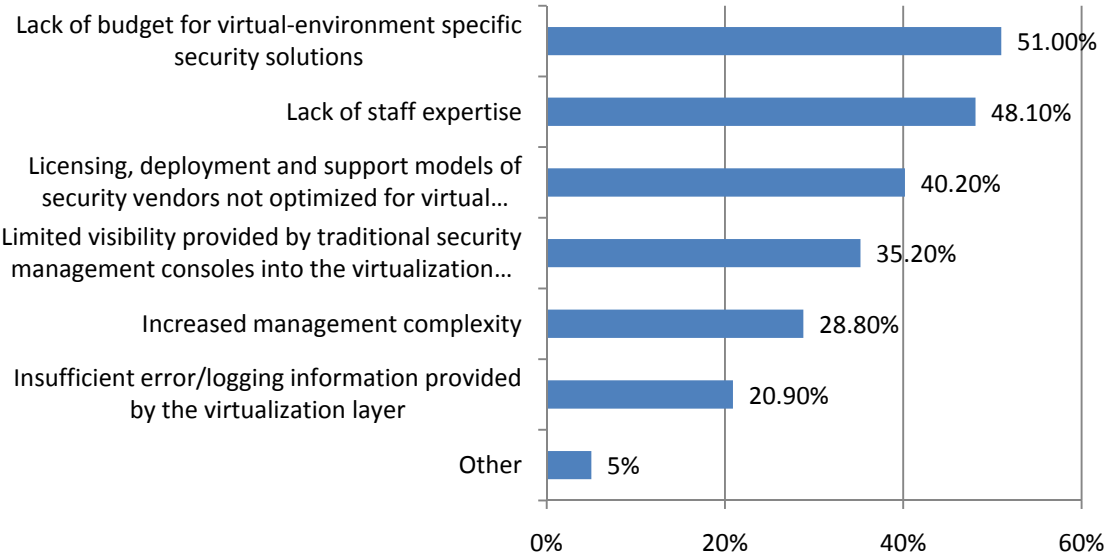
- **Invisible machines:** Flexible deployment and migration capabilities of virtual machines can often lead to a problem of sprawl where VMs grow uncontrollably both inside and outside the IT organization. These invisible/unmonitored machines are a security hazard, especially if they are accessing sensitive corporate data.
    - 53.9% of respondents indicated "VM sprawl and flexible deployment capabilities leading to unmonitored/invisible machines" as a security concern related to virtualization (Fig 7).

What's most interesting is that the majority of respondents seem to be aware that traditional solutions are insufficient to provide security insight into all layers of the virtual environment (Figure 8), yet they still continue to use these solutions, which brings us to ask why?

When queried about the primary inhibitors to effectively securing their virtual environment, the top 3 options selected were: (Fig. 9)

- Lack of budget for virtual-environment specific solutions (51%)
- Lack of staff expertise (48.1%)
- Licensing, deployment and support models of security vendors not optimized for virtual environments (40.2%)

Figure 9: What are the primary inhibitors to securing your virtual environment? (Multiple selections allowed)



3. **<u>Adequate controls on the Hypervisor layer are lacking</u>**

Virtualization software is no different than any other piece of software application. It is bound to contain exploitable vulnerabilities and become a target of attack by hackers as the usage of virtualization technology increases within the enterprise. Considering the privileged level that this layer holds within the virtual architecture, a compromised Hypervisor can provide unfettered access to all hosted machines on a physical server. Complicating the situation is that:

- Security tools and procedures implemented at the Operating System level are blind to issues within the virtualization layer unless they have been designed to specifically talk to this layer
- Traffic between virtual machines on the same box never hits the physical network where network monitoring tools such as intrusion prevent/detection systems reside, rendering them ineffective. Further, log monitoring/SIEM systems that gather data for compliance purposes from these network tools, and not directly from the virtualization layer, receive incomplete information

While 79.5% of respondents agreed that monitoring the virtualization layer is important for risk mitigation (Fig. 8), when queried about the implementation of specific security activities and tools at this layer:

- Only 29% of respondents indicated that they are directly collecting logs from the Hypervisor and only 21% from the virtual management application. (Fig. 10)
- Only 16.90% are reporting on activities and controls at the Hypervisor level, and only 15.70% at the virtual management application level. (Fig 10)

This goes against established best-practices, such as those recommended by Gartner for the virtualization layer**: "Activate full auditing and logging and link these into security information and event management systems."** (*Gartner, 'Addressing the most common security risks in data center virtualization projects,' January 2010, Neil MacDonald)*

The introduction of virtualization also results in the collapse of separation of duties, as mentioned earlier in this document, (Fig. 6) potentially resulting in escalation of privilege, abuse and fraud – especially risky at the virtualization layer because of the critical support it provides to the rest of the virtual infrastructure. Therefore, it is essential that administrative and user access to this layer be carefully monitored and controlled. However, respondents to this survey are largely ignoring this best-practice:

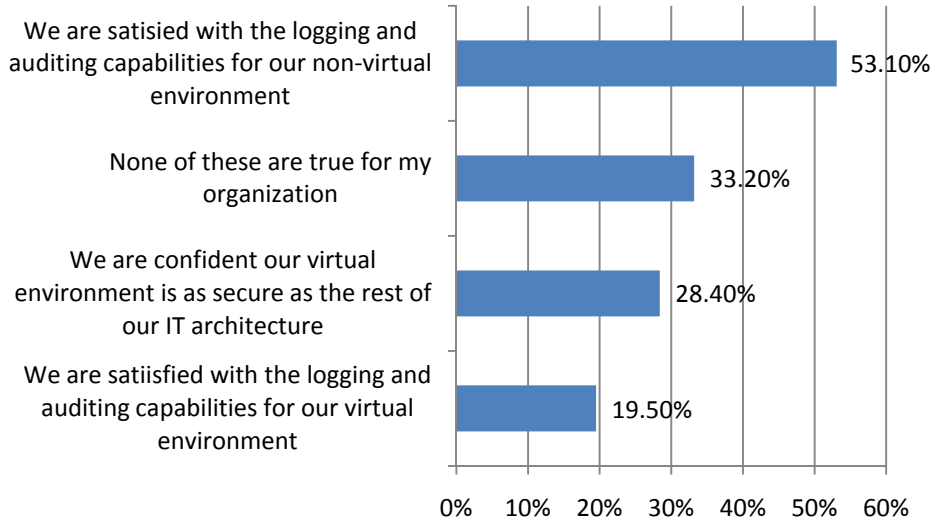
- Only 22.70% are monitoring user activity at the Hypervisor level, and 14.9% at the virtual management application level (Fig. 10)
- Only 17.80% are tracking access to critical data and assets at the hypervisor level and 12.40% at the virtual management application level. A majority (52.70%) have not implemented tracking procedures for any layer of the virtual architecture. (Fig. 10)

Figure 10: Which of the following have you implemented for the various layers of the virtual environment?

	Hardware (e.g. Dell OpenManage)	Hypervisor (e.g. VMWare, Hyper-V)	Embedded Hypervisor (e.g. ESXi)	Virtual Management Appplication (E.g. Vcenter)	Operating System	Not Implemented
Log collection	22.70%	29.30%	13.60%	21.10%	54.50%	24.80%
Automated Log Management/SIEM	14.50%	18.20%	9.90%	10.30%	26.90%	52.50%
User/privileged user activity monitoring	13.60%	22.70%	10.70%	14.90%	45.90%	34.30%
Tracking access to critical data and assets	14.50%	17.80%	7.90%	12.40%	36.00%	46.70%
Reporting on controls and activities for compliance and internal policies	12.80%	16.90%	7.90%	15.70%	41.70%	39.70%

4. **<u>Virtualization is not inherently insecure, however, confidence in virtual environment security is low</u>**
    - 52% of respondents disagreed with the statement that virtual environments are inherently less secure than their physical counterparts (Fig. 8)
    - However, only 28.4% expressed confidence that their virtual environment is as secure as the rest of their IT architecture (Fig. 11)
    - Only 19.5% expressed satisfaction with the logging and auditing capabilities for their virtual environment compared to 53.1% satisfied with the logging and auditing capabilities for their non-virtual environment.

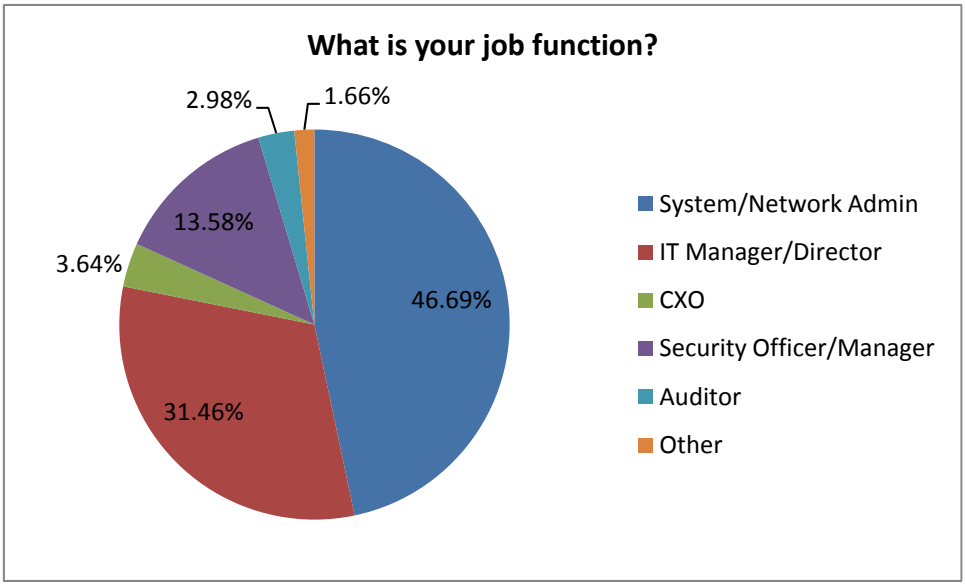
Figure 11: Which of these apply or are true for your organization? (Multiple selections allowed)

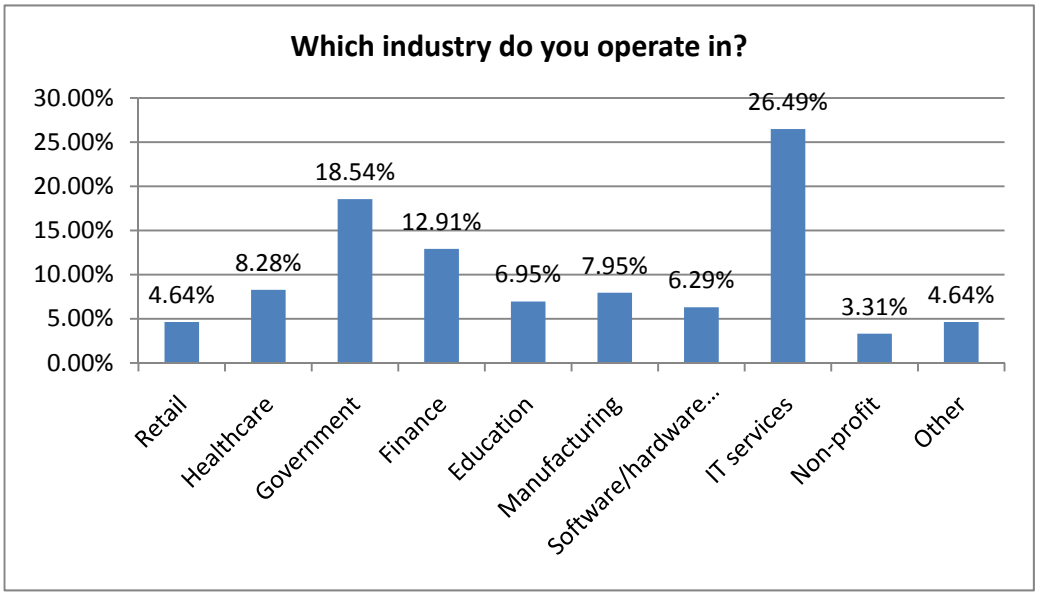


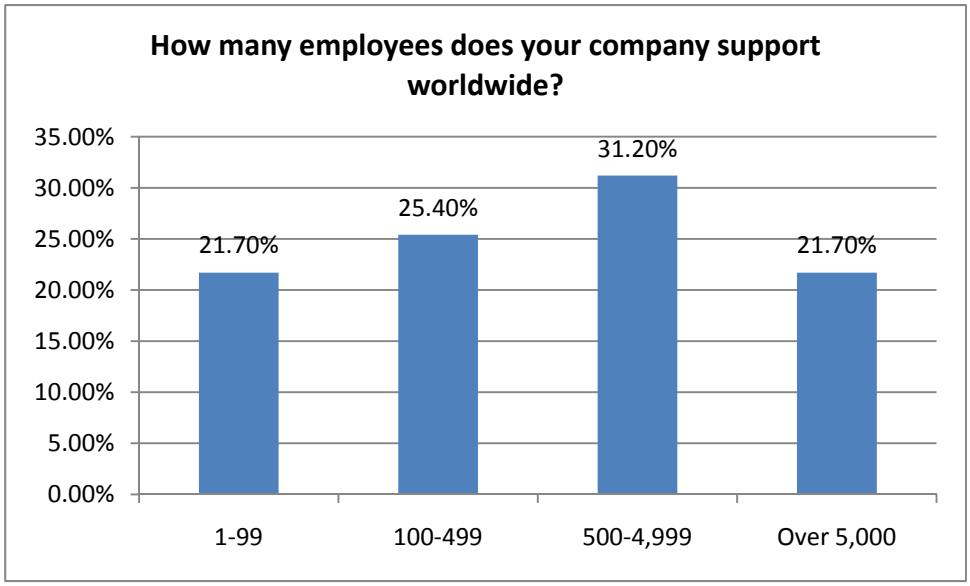
While we agree that virtualization is not inherently insecure, its introduction does change the playing field when it comes to security. There are new attack vectors, new operational patterns and complexity, changes in the IT architecture, and changes in deployment life cycles – consequently approaches to security monitoring and breach prevention must adapt.

The low level of confidence expressed in the security of their virtual environments by survey respondents indicates that with the rush to adopt virtualization, many known issues are being overlooked, and in many cases best practices are being ignored whether it is because of the immaturity of existing security tools, or a lack of staff expertise and budget.

Demographics







Conclusion

Is security a hidden cost of virtualization? A majority of respondents agree that traditional security products and solutions are inefficient to provide visibility into the virtual environment. Yet they continue to use these solutions, citing lack of budget as a primary inhibitor. The implications are two-fold:

- There is a significant gap between the speed at which companies are willing to deploy virtualization and their security readiness to address the added complexity that virtualization introduces
- In the rush to adopt virtualization, security investments are not being factored in to project budgets. Hidden expenses are never welcome, and by ignoring what could later add up to be significant collateral costs, companies may not realize the ROI and cost-savings initially calculated for their virtualization projects.

The responses to this survey also indicate that security is an afterthought - while respondents are mostly aware of the security implications of virtualization and the need to change management approaches, the current stance seems be one of reactive firefighting rather than proactive implementation of best practices. As more and more critical applications are migrated to the virtual environment, companies will need to rethink their processes and draft strategies to address risks across both physical and virtual environments in order to ensure compliance and security visibility in an increasingly hybrid datacenter.

About Prism Microsystems

Prism Microsystems delivers business-critical solutions that transform high-volume cryptic log data into actionable, prioritized intelligence to detect and deter costly security breaches and comply with multiple regulatory mandates. EventTracker, Prism's leading Security Information and Event Management (SIEM) solution provides coverage for both physical and virtual environments, delivering a single point of control to monitor the entire IT infrastructure - from servers to workstations, operating systems to applications, network devices to hosts, and physical assets (including USB devices, racks, and server hardware) to hypervisors (i.e. those from VMware, Microsoft's Hyper-V, and management applications such as Dell OpenManage, VSphere, and System Center).