SURVEY

beyondtrust®
Beyond Traditional Security

Survey Results: Virtual Insecurity

May 2013

Executive Summary: Virtual Assets Could Bring Real Risk

Virtualization technologies have reshaped how IT offers and delivers their services to end users. As it is often seen with emerging technologies like cloud and mobile and now virtualization, new risks are introduced to the environment as quickly as new virtual servers and applications are spun up. How can IT keep up, in the face of rapid adoption and demands of virtualization?

We decided to pose some questions to the IT community at large to see how they were managing the security side of their virtualization deployments. Considering how easy it is to replicate and deploy virtual machines, the potential to also proliferate risk is something that should be managed very closely. We were especially interested in what steps virtualization administrators took on their own to verify the security and compliance of their hypervisors and images, as well as what types of tools they relied upon as part of their everyday processes.

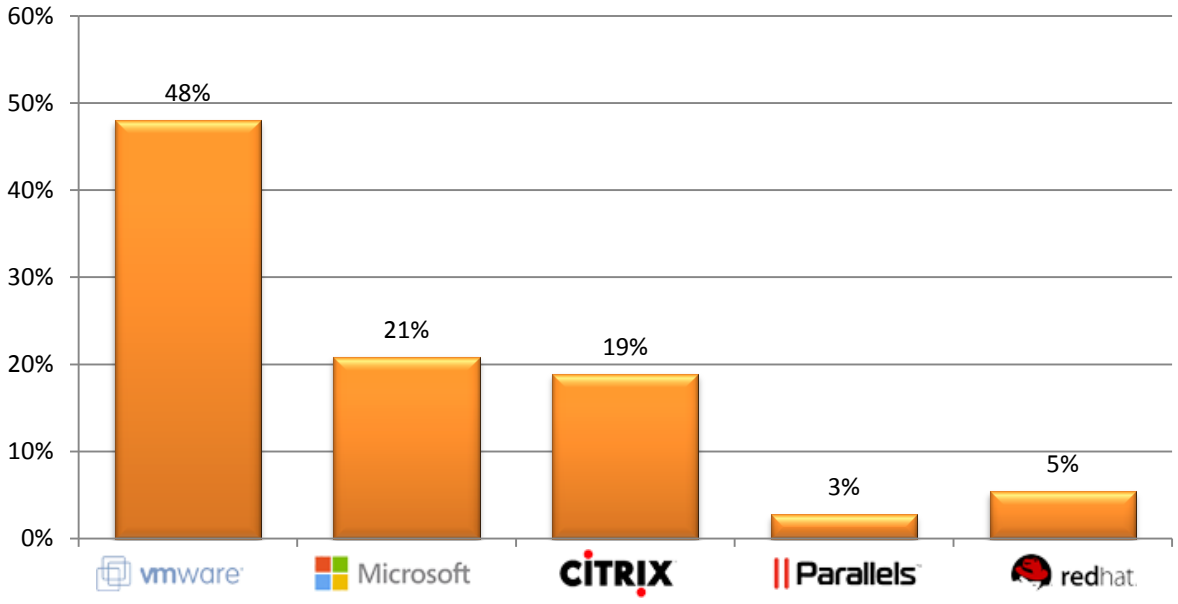
Lastly, we wanted to see if these virtualization administrators are willing participants in the security lifecycle, and if so, to what degree? Given the sophisticated attacks that corporate networks face on a daily basis, does this mean that IT should be asking everyone to do their part – including virtualization administrators?

Survey Information

Survey Opened: April 4, 2013
Survey Closed: May 5, 2013
Total Survey Completions: 448
Survey Targets: Server (Linux, Unix, Windows) Administrators, IT Administrators, IT Architects, and Virtualization Administrators

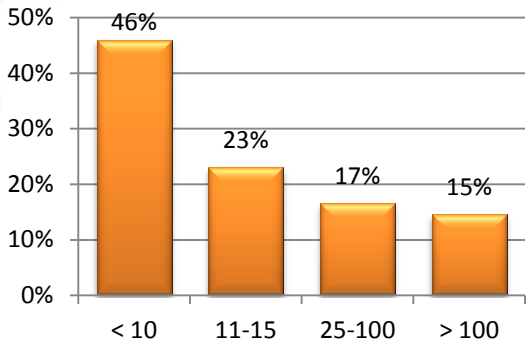
Vendors and Technologies Leveraged

Which virtualization technologies does your organization utilize today?

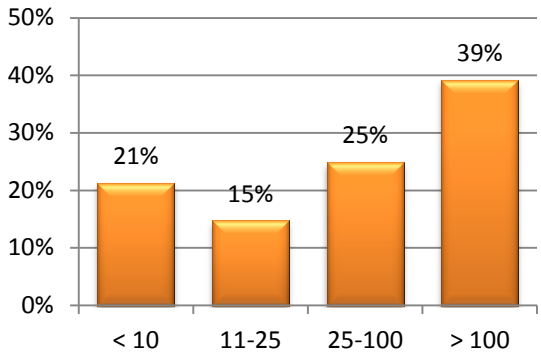


Not surprisingly, VMware leads the pack as the preferred virtualization technology leveraged, however responses do indicate there are several instances of multi-vendor environments, perhaps an indicator of best-of-breed capabilities amongst the vendors for for virtual workload types.

How many hypervisors are in use in your environment today?

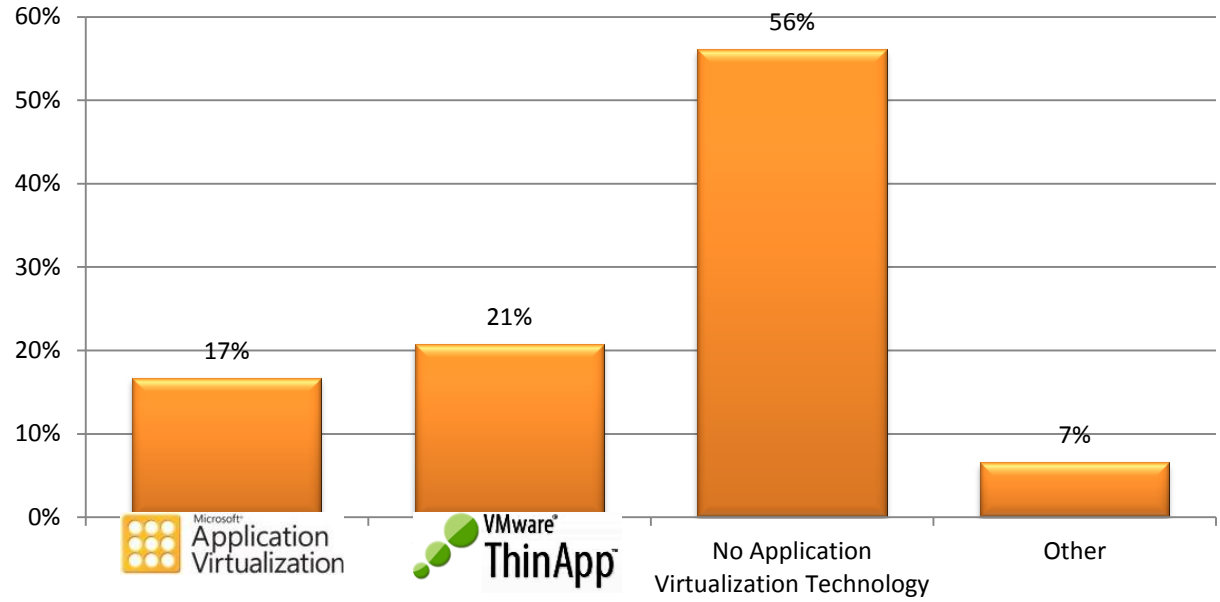


How many virtual guests are in use in your environment today?



From a resource management perspective, it appears that most virtualization administrators are managing 10 or fewer hypervisors; however the number of virtual guests is potentially much higher. Almost 40% of respondents indicated they manage over 100 guests at a time. This is an interesting number to keep in mind as we look at the security best practices these administrators follow later in the survey.

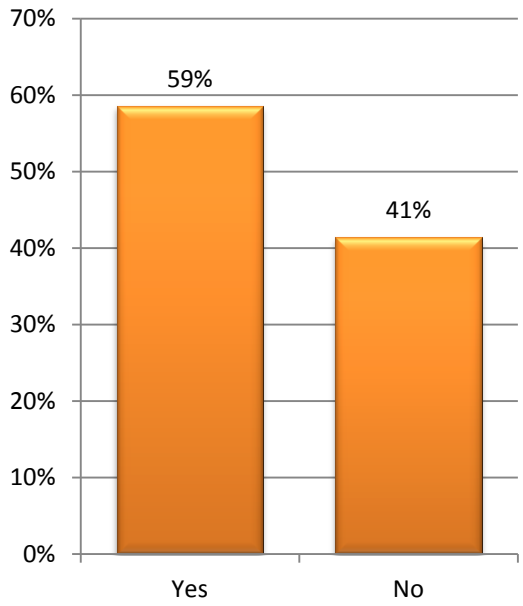
Does your organization currently use any of the following Application Virtualization technologies?



Application virtualization does have a foothold among those surveyed, but over half said it wasn't in use. One contributor to the lack of adoption here might be the fact that not all security scanners can scan virtualized applications for vulnerabilities, as Retina from BeyondTrust can.

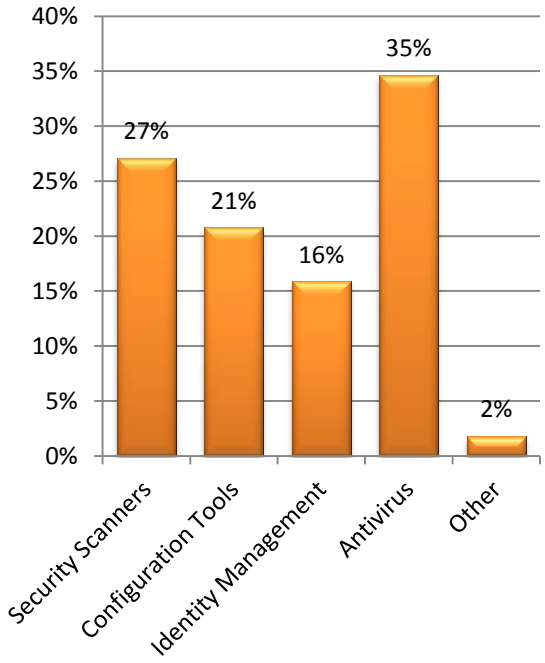
Virtualization and the Security Lifecycle

As part of your virtual systems administration, do you use any security tools regularly?



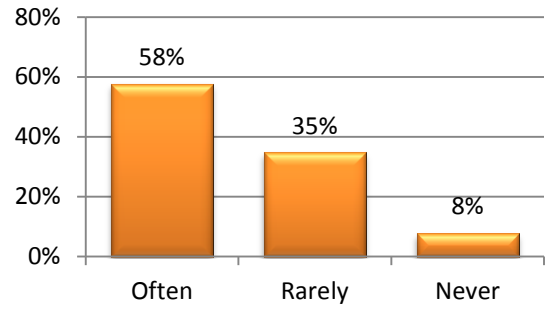
The fact that well over half of respondents said "yes, we use security tools regularly" is very encouraging, but…

What kinds of tools are in use today or are being considered?

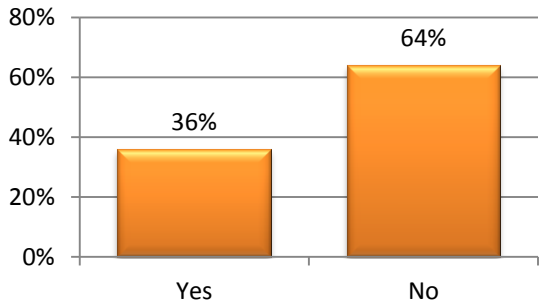


…the most often security technology cited was antivirus. Clearly, antivirus as a security technology is not going away any time soon, but in light of the recent successful, high profile attacks, it's been proven over and over again that AV is no longer a match for the sophisticated methods of attack being employed today. More encouraging is the almost 50% of combined responses that indicate security scanning and configuration management is in use.

How often are existing image templates used for new virtual images?



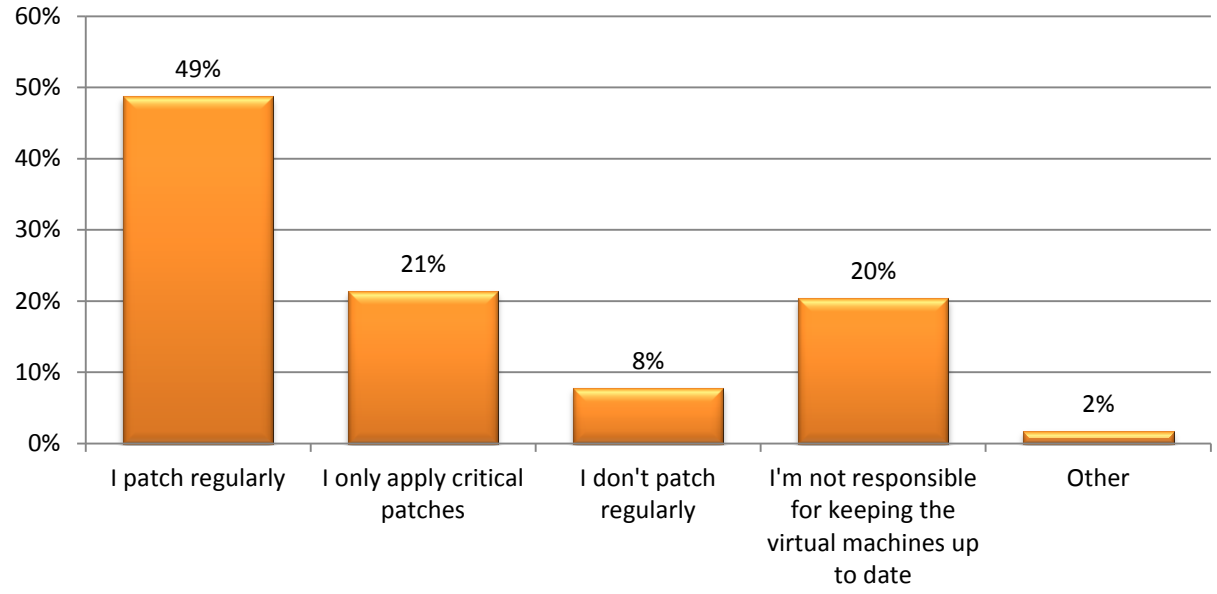
Are there any security controls in place that require a security sign off prior to releasing a new virtual image or template?



These two questions tell an interesting story. Existing templates are often used when creating new virtual servers; however an overwhelming majority of respondents say there are no security controls in place when new templates are created. This could be an area for concern, as these templates could carry some risks with them, either by leveraging outdated unpatched software, or by proliferating mis-configured systems which could lead to security weaknesses.

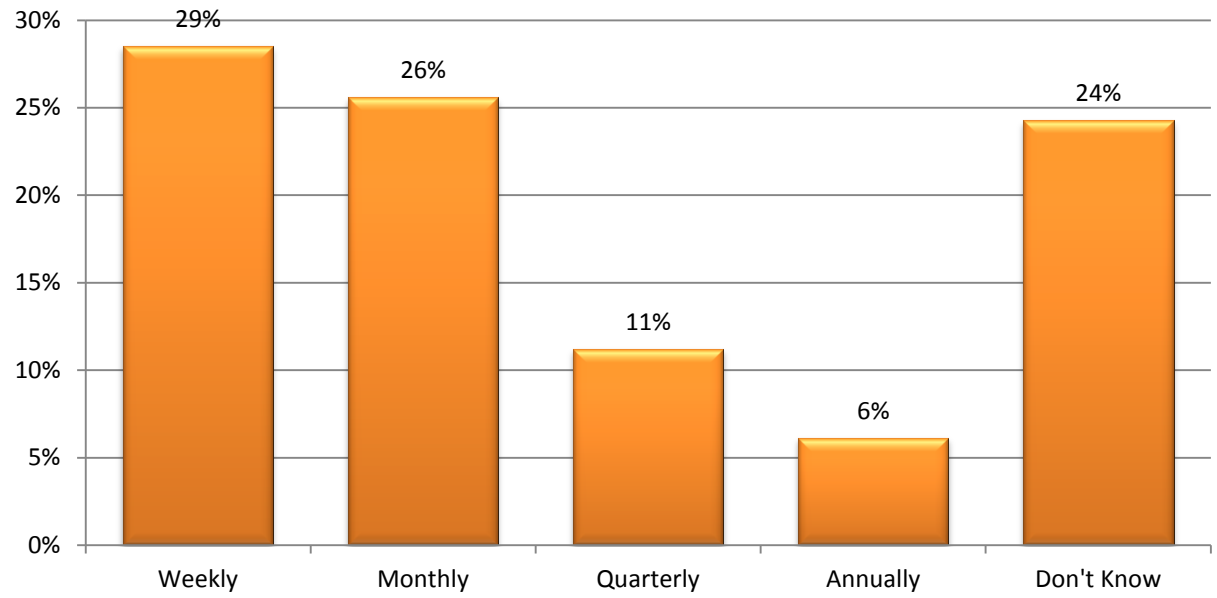
Some Encouraging Findings

How do you keep your hypervisors up to date with available patches and hotfixes?



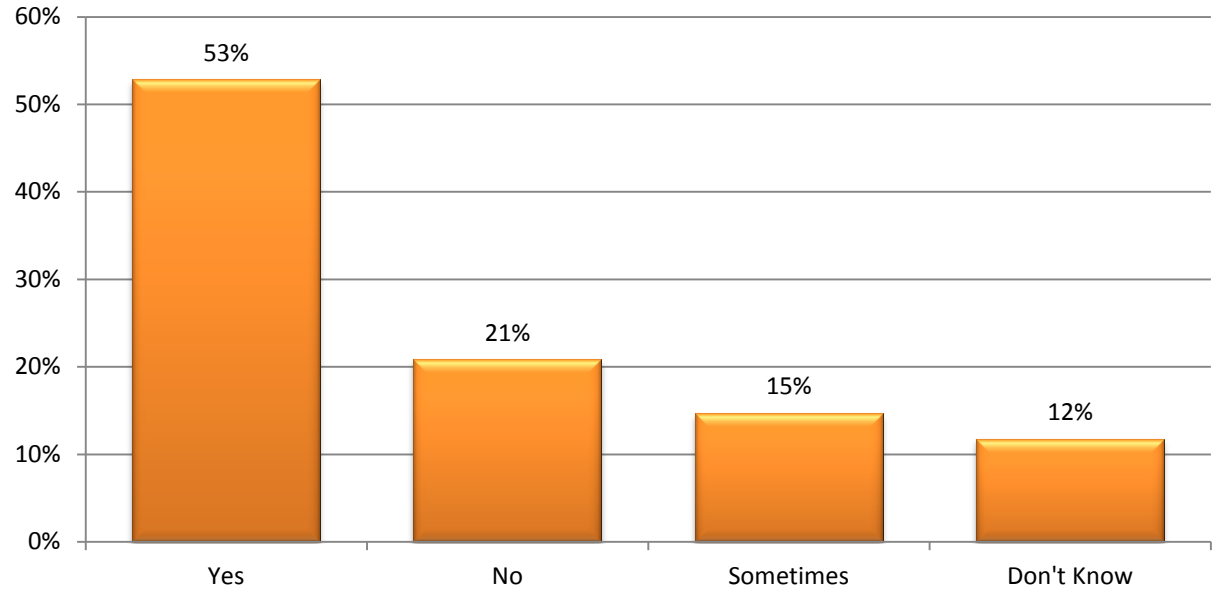
Almost half of respondents patch their virtual systems regularly. Patching systems on a regular schedule is an effective way to reduce the risks associated with managing computing assets.

How often are security scans performed on virtual assets?



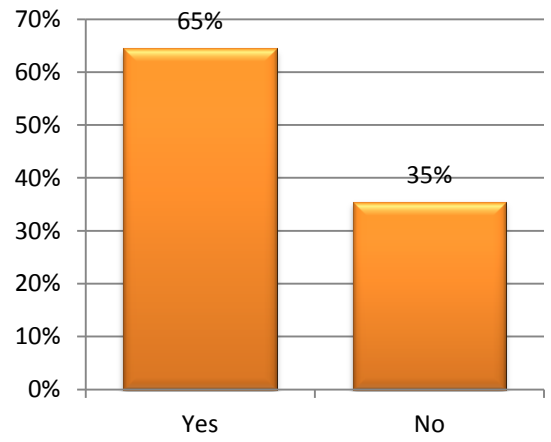
Almost half respondents indicated that security scans of virtual systems are taking place at least monthly, with almost 30% performing that critical task on a weekly basis. Interestingly enough, and probably a strong indicator that there still continues to be a division of labor (and quite possibly, communication) between Security and Operations, a quarter of those surveyed said they don't know how often scans are carried out on their assets.

Are virtual assets included as part of regulatory compliance audits and reporting?

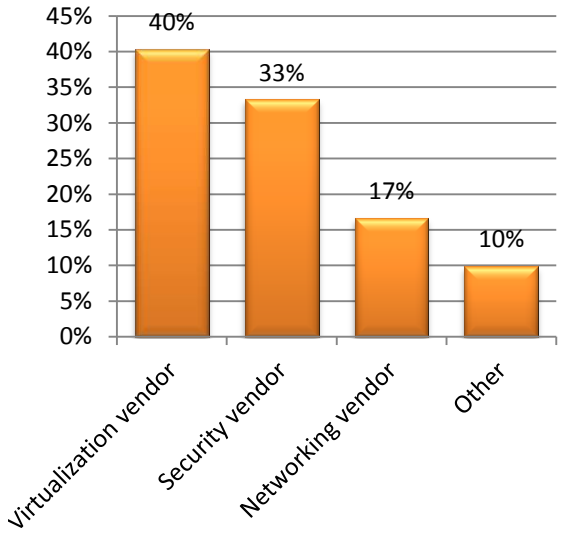


One driver for a heightened sense of urgency and visibility around security virtual systems is their inclusion into reporting for regulatory compliance. Virtual assets, at the end of the day, are still assets and must be accounted for and their risk measured for their part in the IT lifecycle. Over half said that yes, those assets were included in the reporting. Interestingly, roughly 12% said they didn't know – not a good omen for their eventual audit results.

Have you followed any security hardening best practices on your virtual infrastructure?



If you did follow security hardening best practices for your virtual infrastructure, what was the source of those best practices?



It's encouraging that almost 65% of those surveyed did in fact follow some sort of hardening guidelines, either from the virtualization vendor themselves or from a security or networking vendor. Hardening guides are great resources for administrators, who while might not be full-fledged members of the security team, so that they can do their part to reduce risk on an ongoing basis.

Summary

It's clear that virtualization is a technology which has impacted IT to the highest degree. The efficiency and cost gains realized are without question. Given it's pervasiveness within corporate networks today, it also has the potential to increase an organization's risk. Given the results of this survey, it's clear that there is more work to be done to ensure the ongoing security of virtual systems.

One step in this direction is to enable (and hopefully inspire) the teams on the front lines – the virtualization administrators themselves. It's for this very reason that we developed our Retina Network Security Scanner Plug-in for VMware vCenter (available for free download here: http://go.beyondtrust.com/vcenter). This security tool, based on the industry's most proven vulnerability management technology, identifies the risks that may be resident on the virtual assets in use by your organization today. Completely integrated with vCenter, it allows virtualization administrators to stay in their current workflow, and doesn't require them to learn any new security technologies. It was designed with a "point and click" approach to enabling any member of the IT staff to help identify and reduce the risk in virtual assets.