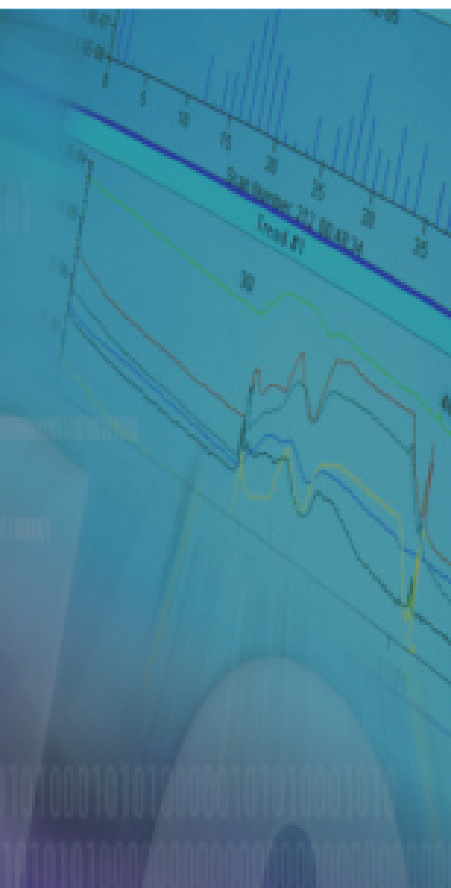


# Understanding the Security Implications of Virtualisation



In association with



an **internet.com** IT Management eBook

# Contents...

## Understanding the Security Implications of Virtualisation



This content was adapted from Internet.com's ServerWatch and eSecurity Planet websites. Contributors: Amy Newman, Andy Patrizio, Larry Barrett and Alex Goldman.

2 2010: The Year of Virtualising Securely



4 Are Virtual Servers Less Secure Than Physical Servers?

6 Security Issues Temper Virtualisation Craze



8 Virtualisation and Security

## 2010: The Year of Virtualising Securely

By Amy Newman

It is a widely held belief that large enterprises are more willing to take a chance on new technologies. After all, they have the cash and expertise. Small outfits, on the other hand, are also prime candidates, as they often have the nimbleness and the need to seek out more creative solutions.

If the results of Symantec's annual data centre survey are to be believed, neither of these groups is at the cutting edge of data centre technologies. Instead, a third group gets those honors — the often overlooked midsize enterprises.

Symantec believes midsize enterprises are driving the adoption of buzz-worthy technologies at this time, virtualisation and cloud computing among them. The survey found technology initiative adoption rates 11 per cent to 17 per cent higher in midsize enterprises than in their small or large counterparts.

Mathew Lodge, senior director of product marketing, Symantec Information Management Group, described this newfound sweet spot to ServerWatch as the "Goldilocks zone." Large enterprises, he explained, may have deep pockets, but they also have more complex needs and thus take longer to evaluate new technologies. Smaller enterprises, meanwhile, lack the resources.

Symantec defines midsize enterprises as those with between 2,000 and 9,999 employees. They comprised 23 per cent of 1,780 survey respondents, Lodge said. Of the remainder, 62 per cent of respondents were from larger businesses and 16 per cent were from small shops.

While the survey results are interesting from numerous angles (particularly with regard to staffing), from the perspective of this column, what is most interesting is where virtualisation sits in terms of priority and adoption.

Virtualisation experience was among the top-three sought-after skills for new employees. The other two important skill sets were networking and security expertise. Virtualisation was not, however, among the top three for key initiatives to be undertaken this year. Here, security, backup and recovery, and continuous data protection

surpassed it. Fourth place, whilst hardly shabby, isn't nearly as exciting as being front and centre.

Has virtualisation lost its luster? Far from it. In some ways, it is a victim of its own success. After years of being among the top-three initiatives, it makes sense that the pace of adoption has slacked a bit. Especially considering nearly 90 per cent of midsize enterprises surveyed now have some level of virtualisation in place, and small and large organisations have more than 75 per cent and 80 per cent, respectively.



Virtualisation has arrived as a mainstream technology. Efforts are under way in enough organisations that the collective priority is figuring out how to deal with the resulting complexities that increase with it. Thus, the focus has shifted from the technology itself to its implications. Virtualisation changes how an enterprise handles disaster recovery, backup (and other storage needs) and security.

Consider this finding:

Virtual machine protection continues to be a focus for enterprises, with 82 per cent of enterprises considering virtual machine technologies in 2010. Respondents cited granular recovery within virtual machine images as the biggest challenge in virtual machine data protection.

In other words, the technology has a foothold, now the emphasis has shifted to assimilating it into the enterprise.

Symantec, of course, is not the only vendor surveying virtualisation behaviour. IT consulting services and equipment provider CDW released its Server

Virtualisation Life Cycle Report, an assessment of how mature the virtualisation market is.

It, too, found security to be major concern. Of the 387 IT executives surveyed, 17 per cent cited security as the main reason for not transitioning business-critical applications to virtualised servers.

CDW also found that although organisations with more than 100 employees have implemented virtualisation software and processes, they have virtualised only 37 per cent of their data and apps. There is much room for growth within enterprises.

Put all of this data together the takeaway is fairly straightforward: For virtualisation to live up to the hype and meet enterprise expectations, security must take centre stage. If enterprises are as committed to the advantages of virtualisation as they say they are, then this could well turn out to be the year where virtual security takes centre stage. ■

## Are Virtual Servers Less Secure Than Physical Servers?

By Andy Patrizio

The rush to virtualisation has yielded a major vulnerability. According to a study by Gartner, the majority of servers being virtualised are less secure than they were when they were separate, physical servers.

Virtualisation has been used as part of a consolidation strategy to put a multitude of underutilised servers on one physical hardware unit. One modern server with lots of memory can house dozens or hundreds of virtual servers, thus saving floor space and electricity for power and cooling.

But as companies make the move, issues often crop up that weren't anticipated. In its report, Gartner found 60 per cent of virtualised servers deployed between now and 2012 will be less secure than the physical ones they've replaced, thanks to bad practices by IT departments or a lack of proper tools to do the job.

"Most virtualised workloads are being deployed insecurely. The latter is a result of the immaturity of tools and processes and the limited training of staff, resellers and consultants," said Neil MacDonald, vice president and Gartner fellow, in a statement.

Gartner based its findings on surveys taken at Gartner conferences in late 2009, some of which include shocking admissions by IT professionals. For example, about 40 per cent of virtualisation deployment projects did not involve the information security team in the initial architecture and planning stages.

Survey respondents said their operations teams argued that nothing really changed because it's all the same hardware, workloads, and software. But Gartner noted that there is a hypervisor and virtual machine monitor (VMM) that is introduced when workloads are virtualised and it changes the basic operation of the server.

Gartner said the hypervisor is rather vulnerable to attack, and seems to hint that cybercriminals are already targeting the hypervisor, since it enjoys a privileged level of access to the system. The research firm advised IT that the hypervisor layer should be treated as the most critical part of the server platform even though many today pay it no mind at all.

It's still early in the game as far as a broad virtualisation. Gartner estimates that at the end of 2009, only 18 per cent of enterprise data centre workloads that could be virtualised had been virtualised. That will grow to 50 per cent by 2012, and by 2015, Gartner thinks the percentage of unsecured servers will fall to 30 per cent, which is still a large figure.

The company said that security needs to be brought in to the discussion of virtualisation of workloads from the beginning. Gartner also recommends that at a minimum, organisations require the same type of monitoring for virtualised systems as physical systems. Administrative access to the hypervisor layer must be tightly controlled, given how important the hypervisor is. ■

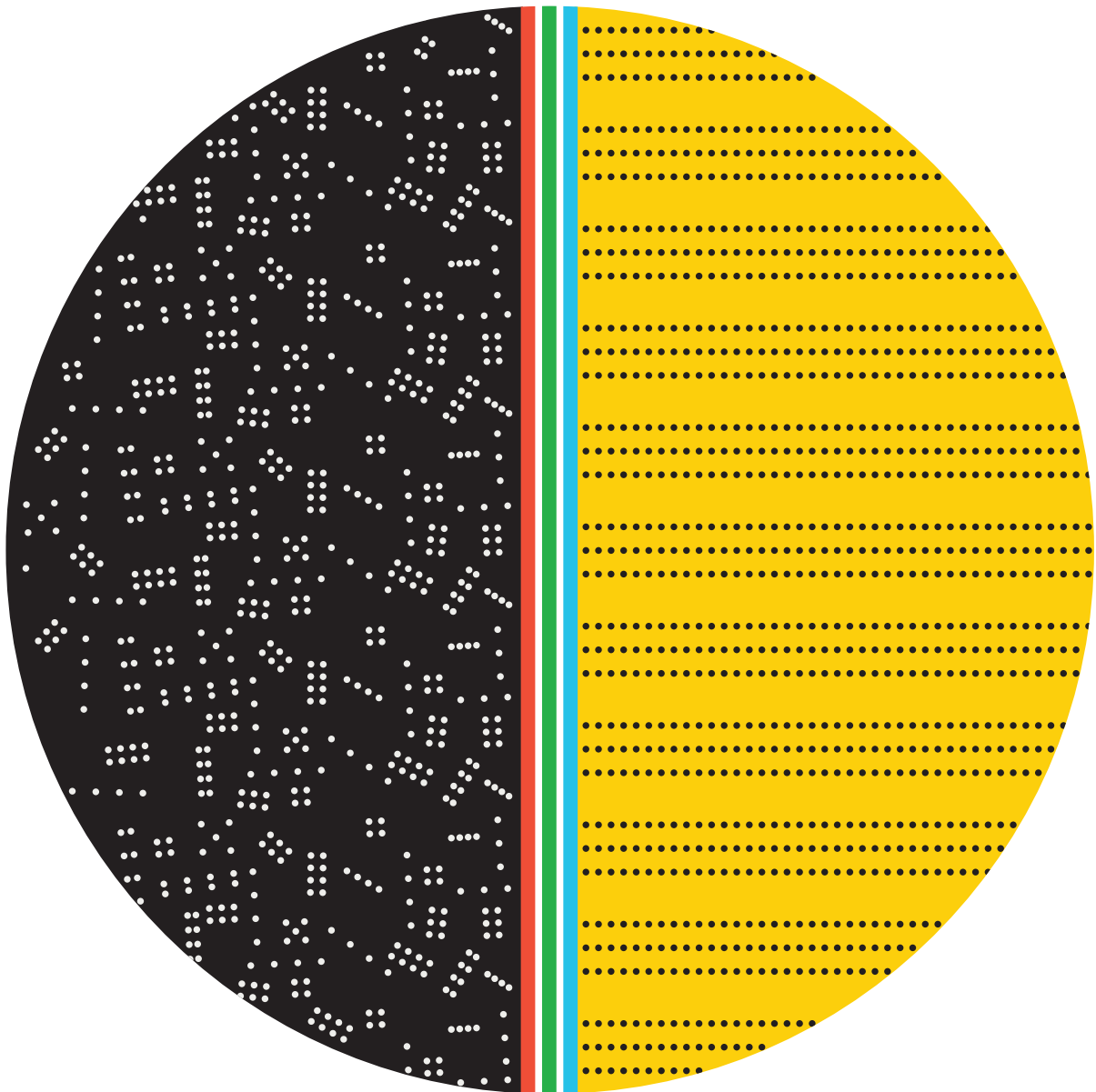


Smarter technology for a Smarter Planet:

## How to manage thousands of things you can't touch.

Today, many companies are finding out the hard way that virtual image sprawl can be just as complicated as the physical server sprawl virtualisation was created to solve. IBM can help you manage, simplify and even automate your virtual environment with a broad range of solutions designed to give you visibility and control over servers, storage, applications and all your other virtual resources. So you can have resources up and running in minutes instead of days, driving up efficiencies and setting the stage for new delivery models like cloud computing. Our open approach to virtualisation has helped customers reduce capital and operating costs by up to 30% and is an essential building block of a smarter, more dynamic infrastructure.

A smarter business needs smarter software, systems and services.  
Let's build a smarter planet. [ibm.com/virtualisation/uk](http://ibm.com/virtualisation/uk)



IBM, the IBM logo and the planet icon are trademarks or registered trademarks of International Business Machines Corporation in the United States, registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at [www.ibm.com/legal/copytrade.shtml](http://www.ibm.com/legal/copytrade.shtml) ©2009 IBM Corporation. All rights reserved.

# Security Issues Temper Virtualisation Craze

By Larry Barrett

IT consulting services and equipment provider CDW served up some statistics that indicate that while enterprise customers recognise the inherent financial and energy savings derived from virtualisation, they're still a bit gun-shy when it comes to virtualising their most critical applications and data repositories.

CDW's Server Virtualisation Life Cycle Report, an extensive examination and survey of just how mature the virtualisation market has become — or not — in the past decade.

A total of 387 information technology executives and companies took part in the survey, with results that revealed both their appreciation for the benefits that virtualisation software can deliver and their apprehension to commit their most vital data runs to a technology that's still viewed as a work in progress.

"Server virtualisation was one of the most important data centre developments of the past decade, with organisations embracing it enthusiastically for its benefits in cost, IT productivity, business agility and resilience," Scott Severson, director of CDW's server and storage solutions group, said in a statement. "What we found in this study, consistent with what we see in our customers' experiences, is that most adopters have captured the low-hanging fruit and are building their trust in virtualisation platforms as they consider how to capture more of virtualisation's promise."

To wit: Organisations with more than 100 employees have implemented virtualisation software and processes "at some level" but still only 37 per cent of their data and applications are running on virtualised servers.

And while 54 per cent of these companies have completed their virtualisation deployments, respondents said concerns about the security of virtualised environments preventing in-house IT honchos from

abandoning their physical servers entirely in favor of software applications that can reduce their overall datacentre footprints by as much as 90 per cent.

A full 17 per cent of the 387 IT executives surveyed said security was the main reason they haven't transitioned much of their business-critical applications to virtualised servers, while another 17 per cent said their hardware still doesn't support virtualisation applications.

More telling, 62 per cent confessed that despite all the well-documented benefits of virtualisation — particularly the reduction in energy consumption, the ease of configuring and managing servers and the freeing of cash to pursue other IT projects — they still have a ton of applications that they don't feel comfortable running on virtual servers because of the criticality of the data and applications' functions.

This somewhat schizophrenic outlook is reflected by the fact that 89 per cent of those surveyed said they employ



## Understanding the Security Implications of Virtualisation

a “virtualisation first” strategy — a requirement that network users first prove a new application doesn’t work in a virtual environment before the company will buy a dedicated server to support it.

Also, 99 per cent of those queried said they give their CTO a passing grade in their adoption and implementation of virtualisation technology, and 85 per cent said they believe their IT departments are appropriately staffed and trained to manage a virtualised server environment.

However, for some enterprise IT managers, it’s still not enough.

“Anything drastically related to secure information, I haven’t been comfortable with total changeover of payroll and other similar applications just yet,” one respondent said.

Despite the apprehension, 95 per cent of businesses that have implemented virtualisation believe they are saving significant money as a result, and 94 per cent are measuring their success in terms of IT productivity, business agility and reductions in IT energy consumption.

“IT organisations continue to face immense cost pressures and productivity demands from their internal clients,” Severson added. “Based upon the successes and benefits they have already seen from server virtualisation, we expect continued, steady expansion of virtualised environments as user trust builds and the software vendor community adapts to serve customer demand.” ■

# Virtualisation and Security

By Alex Goldman

Virtualisation isn't easy, and security issues, which make a complex process harder, are all too often ignored in the haste to deploy this technology.

To those planning virtualisation deployments now, Steve Orrin, director of security solutions at Intel, had a simple and useful piece of advice. "Don't go after the high-value, mission-critical stuff first. Start with something valuable that's worth the investment but not something so critical that it's a serious issue if it goes down."

"With any new infrastructure, there will be mistakes and challenges," he added. "Learn and then apply that learning to high-value systems."

At the ISACA International Conference Orrin gave a talk called "From Virtualisation vs. Security to Virtualisation-based Security" where he discussed the idea that security should be able to help virtualisation deployments and not obstruct them.

## Save Cash But Don't Cut Corners

If security is often an afterthought in these deployments, that may be because the goal is all too often purely cost savings, as opposed to taking advantage of the increased agility that virtualisation offers, according to Orrin.

"Managers need to try to understand what virtualisation means to them," he said. "There are security issues —

and there are operational issues that are just as hard as the security issues — that crop up when you move out of the world where every server has one application."

The elements of security become more complex when applications are moving from server to server, changing the resources they use and even their location. "You need different levels of security for different virtual machines (VMs). People went from 20 boxes to one big box and

now mission-critical applications are running on the same machine as experimental apps and little IT and HR apps. How can one security policy cover them all?"

But most deployments are even more complex than that. "In most organisations, it's not 20:1 consolidation and that's it," he said. "Organisations have multiple data centres in multiple geographies and managers also want to consolidate data centres."

## No Single Security Policy

The solution, Orrin said, is to have a security policy that delineates many levels of security (perhaps high, medium and low) and to implement virtualisation gradually.

If it's done well, there can be compliance benefits. "I've seen examples where people find it easier to apply security controls and represent them to auditors," Orrin said.



## Understanding the Security Implications of Virtualisation

But it's not easy to do it well. There's a new software layer, the hypervisor, plus a VM manager (VMM) to secure. Virtualisation technology can help.

"VMsafe and [similar tools in Xen] allow you to leverage the VMM so that one VM can do antivirus for the other VMs. The goal is taking your existing security mechanism and making it virtualisation-aware," Orrin said.

Making antivirus virtualisation-aware is one thing; making a firewall virtualisation-aware is tougher. "A firewall in the cloud cannot run the same level of protection, especially if the hypervisor runs some communications between VMs," Orrin said.

"In response, some people redirect all network traffic out to the network [instead of allowing VMs to route packets directly to each other]," Orrin added. "Some vendors like Cisco and Juniper want you to do that but then you're not taking advantage of the efficiencies that virtualisation can deliver. Virtual appliances (from an efficiency perspective) make a lot of sense but if you talk to the people who have built it out, there are limitations even there."

Can mainframes simplify virtualisation? "The mainframe is the ancestor of all virtualisation," Orrin said. "IBM likes to talk about it, but if you have Linux or Unix side by side with a mainframe, the mainframe has its own facilities for access control and process isolation and it breaks down when you try to mix the mainframe with a client-server architecture and VMware."

Orrin claimed to like the idea of mainframes. "I'm a mainframe advocate. I've seen the beauty and power of the mainframe," he said. "That said, it's not a Windows or a Unix server."

He added that in a rare case where all of an enterprise's mission-critical software resided on a mainframe, it could be a valuable part of a virtualisation deployment.

Another key security issue that is unique to virtualisation, Orrin noted, is that in many virtualisation deployments, the templates of commonly used VMs are stored and then copied and provisioned as necessary.

"People spin up VMs based on one gold copy. If someone manages to attack the gold copy, they can cause damage to the system based on every instance. Security software looks at what's running but gold copies aren't running, so you need to be able to investigate them. A VM at rest is just a large ISO file."

He added that companies make products to provide the necessary security. "They offer change control and management and attestation of a VM before provisioning. During migration, a VM can be attacked on the wire. There are even examples of attacks on a VM that's in transit between two servers. The attack changes the security bits in transit. So to protect VM integrity, they make sure that the VM that's being provisioned is the original, that it has not been altered."

"The good news is that there are tools and technologies to solve the problems," Orrin concluded. "IT just needs to apply the appropriate tool." ■