

## **Is virtualization a black hole in your security?** 5 ways to ensure it isn't

The ease with which virtual computer image files can now be downloaded means there is a much higher risk of end users running unauthorized applications – from games to browsers to beta software – in a virtual environment, making corporate systems and data much more vulnerable than in the past. This paper describes the hidden threats raised by unauthorized, unsecured desktop virtualization, and gives five effective ways to secure yourself against them.

# Is virtualization a black hole in your security?

## 5 ways to ensure it isn't

### Virtualization's appeal

Virtualization technology has been around for more than 40 years but it wasn't until recently that it really took off in the enterprise thanks to its promise of hardware savings and increased agility.

By encapsulating and isolating operating systems and applications from the underlying hardware, virtualization lets IT departments pack multiple independent virtual machines, each with its own operating system and applications, on a single server. This has brought real business benefits to organizations in terms of administrative and cost efficiencies. In addition freely available virtualization software, such as VM Player, has highlighted the potential of virtualization and has led to a boom in the use of virtualized software on the desktop.

### Virtualization in a nutshell

Virtualization separates logical resources from physical resources, allowing multiple systems to be run on one piece of hardware.

This upward trend looks firmly set to continue, with Gartner, Inc predicting "Virtualization will be the highest-impact trend changing infrastructure and operations through 2012".<sup>1</sup>

Enabler	Benefits
Can run more applications on fewer computers, and legacy applications and operating systems on newer desktops	Allows IT to extract more value from its hardware investments and reduces management costs
Can be moved quickly and automatically to new systems	Enables business continuity and disaster recovery in the event of hardware failure
Easier deployment and management of virtual systems	Reduces the administrative complexity
Availability of cheap storage and high bandwidth	Easy to deploy virtual environments on standard servers and computers

Table 1: Benefits of virtualization

## The security issues

The benefits of virtualization might have been recognized but what is not so well grasped is the issue it raises about security. Server virtualization, with its enclosed, managed, highly protected data center environment, is not much more vulnerable than non-virtualization. Similarly, virtual desktops that are managed by IT, are running no significant increased risk. The real thorny security issue today is the proliferation of **unauthorized** virtual software that might be running on your company desktops and roaming laptops for a couple of reasons:

- Product evaluations, games and other software are often distributed on virtual appliances and free virtual machine players.
- Employees deliberately run unauthorized applications in a virtual environment to avoid detection – they might even be running a private business.

There is also risk associated with authorized but unmanaged virtualization, notably the self-contained test and Q&A environments created by developers.

## The hidden threat

All these virtual machines introduce a new set of challenges, security vulnerabilities and management issues that IT has to address in order to protect its infrastructure from viruses, hacking, and other security threats.



*Hidden, unmanaged virtual environments circumvent traditional policies and privileges, and create a black hole in your organization's security system.*



Like smartphones, instant messaging, and other technologies which can sneak into the organization through the backdoor, the hidden, unmanaged virtual environments which your employees deliberately or unwittingly install on their corporate systems without your knowledge, circumvent traditional policies and privileges, and create a black hole in your organization's security system.

Installing a virtual machine on a networked computer is functionally the same as installing a physical desktop computer. So each new virtual machine must conform to your security policies. This means it must have its own anti-virus agents and any other endpoint security software your policies mandate, and must be kept up to date with relevant security patches. Even though the computer probably has all these security measures in place, the virtual machine is, to all intents and purposes, separate and must be patched and secured as a separate computer.

Unfortunately, a user-downloaded and installed virtual machine most probably doesn't conform to corporate security policies, or have your company-deployed security software running. Since you cannot detect its contents, there's no way to find out if it does. Even worse, the virtual machine might contain viruses or other threats that can be used to infect or hack your network. This not only compromises your security but also creates a significant risk that you will no longer comply with the increasing number of legal and industry regulations that require you to protect confidential data.

A typical user will almost certainly not consider this when downloading a virtual machine. And even if they do, there's often no way for them to know what's on the virtual machine until they install it.

## 5 steps for taking control

Despite these formidable challenges, it is possible to secure your network from the dangers of desktop virtualization. It doesn't necessarily require new types of security tools or a whole new approach to security. With the important proviso that your existing management, policy, and technology tools are up to the task of effectively securing a non-virtualized environment, you just need to make sure they also take virtualization into account.

Here are five effective measures you can take to secure your network from virtual hazards.

### 1 Update your acceptable use policy and educate your staff

Most organizations have acceptable use policies (AUPs) in place with the rules and guidelines users must follow when using their computers and the internet. It's time to update your AUP to address virtualization, spelling out the exact conditions under which virtual software can be installed, what approvals are required, what types of software can be run, and how it must be protected. You also need to spell out the repercussions employees can expect if their unauthorized installations are discovered.

At the same time, it's important to educate your employees on your entire AUP policy, including what the threats are, how they translate into policy, and the true costs and implications of a security breach.

### 2 Limit use of virtual machines only to users that need them

The truth is, in many IT environments, most users have no need for virtual machines on their desktops at all. The best solution is simply to forbid the installation of freely downloadable virtual software on corporate desktops or laptops.

The situation is different with regard to the "professional" virtualization tools that users, such as developers, need for software testing or other purposes. Permission to use virtual machines should be limited to this small group of users who truly need them and who can be trusted to ensure that the use of all virtual technologies conforms to corporate security policies.

### 3 Keep your virtualization and security software up to date

Make sure every known virtual machine includes the same personal firewalls, anti-virus, intrusion detection and other client security software as your physical desktops and laptops. Vendors are starting to develop security software that can sit underneath the virtual machine layer by integrating with the hypervisor – the means by which virtualization is possible – but these solutions still do not provide the in-depth context and sensitive behavioral analysis necessary to detect the latest malware in action.

Network access control (NAC) software on each computer can help, depending on configuration (virtual machines can operate in a bridged mode where they connect directly to the network, or can masquerade as the host making NAC difficult), as it can block network access until a physical or virtual machine is up to date according to corporate policies.

As with any software, virtualization software itself can be exploited, so it's important also to keep all your known virtualization software and applications updated with appropriate security patches from the vendor. Some centralized patching solutions may not provide detection or patch remediation capabilities for virtualization products, meaning that your administrator will have to define policies for the virtualization vendor's update tools.

#### 4 Choose security products that support virtualization

Things to consider when looking at security products that support virtualization include:

- Does the security vendor supports the virtualization software you want to use?
- Are there any known conflicts with existing virtualization platforms?
- Does the security software allow you to control the use of virtualization software?

#### 5 Create and maintain a library of secure virtual machine builds

One of the surest ways to ensure developers and testers create virtual machines that meet your security requirements is to make it quick and easy to do so. Create a repository of virtual machine builds with all the configuration settings, security software, and software patches required by your security policy that users can simply download use, and reuse as necessary.

#### What lies ahead?

Today the security problems with virtualization are centred around the difficulty of identifying and protecting the unauthorized virtual environments that emerge on the corporate network. This will remain the case but in the future the threat is likely to expand.

Threats that specifically target virtual machines, such as the RedPill hacking tool and the rootkit BluePill, have raised concerns about the threat to virtual machines themselves. This type of threat which attacks the hypervisor are in reality merely proofs of concept. However, as virtualization increasingly replaces today's infrastructure, becoming more supported in the operating system and used by more applications, it is highly likely that we will see more hypervisor attacks become much more of a real threat.

#### Conclusion

Virtualization can represent real value, particularly at a time of increasingly constrained IT budgets and its mushrooming popularity looks set to continue, transforming the way computers are used in the enterprise. While organizations deploying managed virtual desktops are running no significant increased risk, unauthorized desktop virtualization brings a host of security challenges to IT. By incorporating virtualization into your overall security strategy, you can protect your network from its dangers while profiting from its benefits.

## Sources

- 1 [www.gartner.com/it/page.jsp?id=638207](http://www.gartner.com/it/page.jsp?id=638207)

---

## Sophos solution

Sophos Endpoint Security and Control uses a unified single client to proactively protect against malware and hackers, as well as controlling removable storage devices and the installation and use of unauthorized applications including virtualization applications such as VMWare Player, Virtual PC or Citrix Xen.

You can use the free Sophos Application Discovery Tool to scan your network for unauthorized applications. Visit [www.sophos.com/products/free-tools/sophos-application-discovery.html](http://www.sophos.com/products/free-tools/sophos-application-discovery.html)