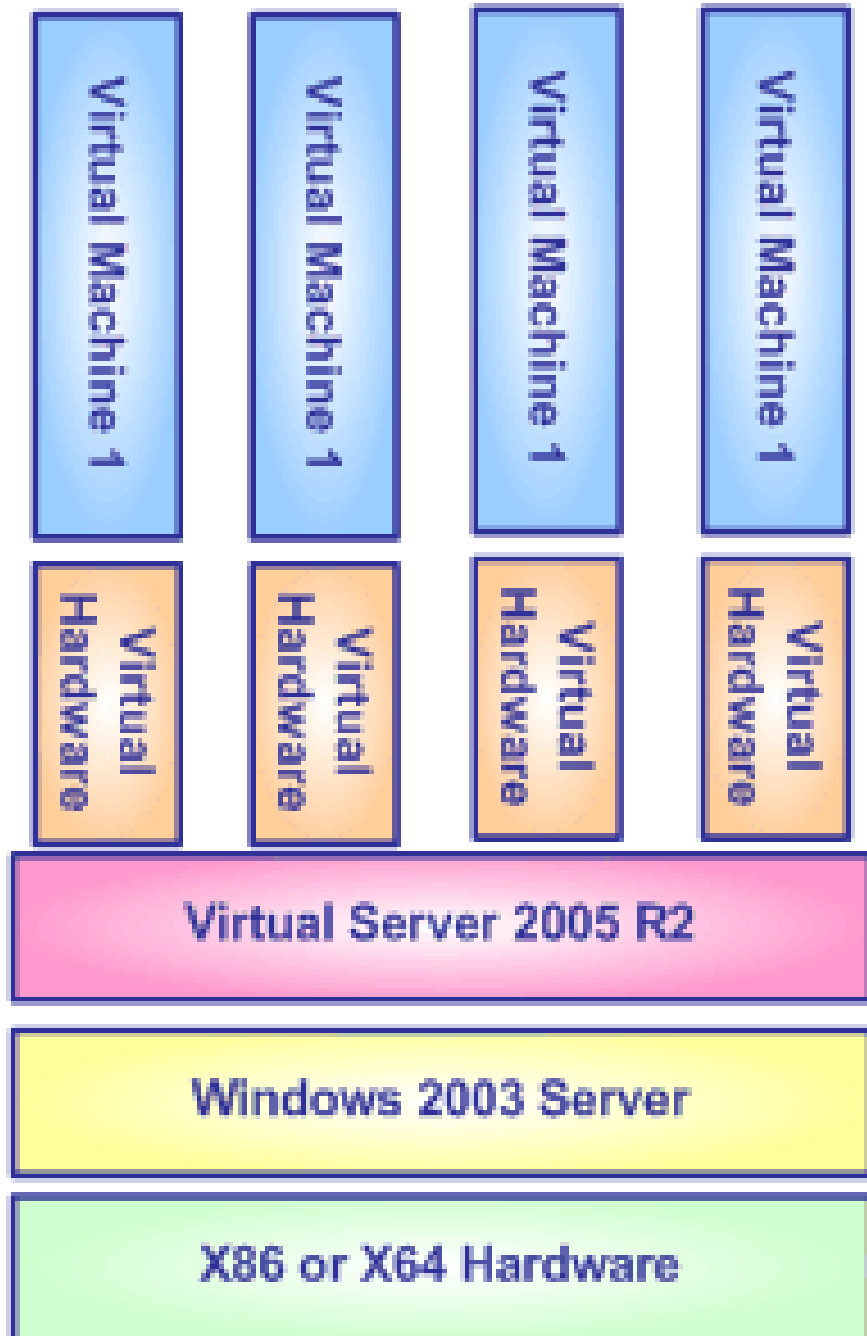


## 5 steps to help secure virtual servers

Prestigious professionals in the field of virtual system security share advice on security. Consider 5 steps when you evaluate virtual system security in your business.



*At the conference of last week's Black Hat group, virtual system security is one of the hottest topics and the focus of discussions. If you want to master the security of your enterprise virtual machine system, consider the following tips of a security strategist Chris Whitener .*

### **Protect your host operating system by using server protection tools and methods .**

Additional operating system features such as quarantine capabilities and strong security between the system's partitions make it easier for you to reduce the host operating system's 'attack surface'.

### **Ensure that the host operating system is as secure as the guest operating system.**

A virtual machine will inherit all the vulnerabilities (vulnerabilities) of the host operating system. Choose a virtualization technology that provides strong security isolation (execution of suspects) between guest operating systems if needed. If organizations see malicious software such as this guest operating system attacking the guest operating system, or without mutual trust between administrators of other guest operating systems, then the virtualization layer must be designed to enforce suspicious ideas.

### **Security policies in the host operating system need to reflect the requirements of the virtual machine.**

Using the host operating system to enforce principle requirements further enhances your trustworthiness. Can rely independently on the admin element on the guest operating system.

### **Manage virtual processes like done with physical resources**

The host operating system security cycle and virtual machine security cycles, both must be effectively managed through a data center. Ideally, virtualization infrastructure should be managed in the same way as managing physical resources. They need software configuration, updates, patches, audits and performance checks, .

### **Be cautious about managing physical infrastructure**

Deploying workflows on virtualization platforms can increase mobility, provide flexibility and agility; however, this does not mean that the physical infrastructure will be ignored. Physical infrastructure has a very important role in supporting good execution of these workflows, besides virtual infrastructure security also depends on physical resource configuration and how Access control mode is currently being implemented in the data center.

You finished reading the article "**5 steps to help secure virtual servers**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.