

A background image showing a laptop on a desk with a speedometer overlay. The speedometer has markings from 0 to 70 and a needle pointing towards 40. The scene is dimly lit, suggesting an office or data center environment.

# Trend Micro Enterprise Security

Data Center Security 

## 10 Reasons Not to Virtualize

*A Trend Micro White Paper | Oct 2011*

*Dave Asprey, VP Cloud Security*



# 10 REASONS NOT TO VIRTUALIZE

## INTRODUCTION

Virtualization and private cloud have enabled server consolidation, created more flexible environments, and saved companies a ton of money. In fact, Trend Micro's recent survey of 1200 companies with more than 500 employees showed that 59 percent had server virtualization in production or pilot. But based on experience with large enterprise users of virtualization, here are the types of situations when you should consider not virtualizing some of your applications.

### I. WHEN YOU HAVE STATIC, PREDICTABLE COMPUTING NEEDS

In this case, you are probably already operationalized and stable, so you will see little benefit to making a change that could introduce more complexity and downtime...unless of course, your stable environment requires an older, no longer supported operating system. When that happens, you do not have much choice but to virtualize anyway and accept the transition costs and complexity.

### II. WHEN YOU CAN'T GET A VIRTUALIZATION-FRIENDLY LICENSE

If you use specialized software with a license that is not supported on virtual machines, you have a conundrum. You could always virtualize and not tell the vendor, but it is inconvenient and maybe even illegal. In either case, it means taking a risk. It also means support problems unless you replicate your virtualized system back onto a physical server just to get the support you need. It is usually less work to negotiate a new virtualization-friendly license with your software provider.

### III. WHEN IT JUST WON'T WORK VERY WELL

There are some applications that just do not work well on virtualization for a variety of reasons. Virtual machine (VM) vendors are getting better at supporting these special cases, and some new technologies, like I/O virtualization, are coming along to make it easier. But in the meantime, watch out for applications with these characteristics:

- High I/O applications like databases or others that require tuning to work with underlying hardware
- Disk intensive workloads. (Or if you do virtualize one of these, use a pass-through disk instead of a virtual hard disk)
- Grid or distributed SMP "number crunching" applications that need high speed interconnectivity
- Applications that require hardware cards for which there is no virtualization driver, or applications that need a dongle
- Graphics-intensive applications (especially ones that need high-end video cards)



## 10 REASONS NOT TO VIRTUALIZE

### IV. WHEN TIME DRIFT WILL HURT YOUR APPLICATIONS

VMs do not store time identical to the physical host, which means that time drift (the VM clock diverging from the physical clock over time) will happen. If even very small amounts of this are going to hurt your applications, they are not candidates for virtualization. Financial real-time trading applications and some industrial control systems are potential concerns.

### V. WHEN YOU WORK FOR A CHEAPSKATE

Like any worthwhile IT project, virtualization requires a budget. If you don't have a way to pay for the project, don't start it. Halfway implemented virtualization without adequate tools and efficient, virtualization-aware security is worse than whatever you have today.

### VI. WHEN YOU'RE ALREADY RUNNING SERVERS AT HIGH CAPACITY

Adding a hypervisor to a pegged server does nothing to help performance. While we have made major progress in the last decade to reduce the CPU overhead taken by a hypervisor, it is still an additional load on the CPU. In this case, buying another server just to provide cycles for a hypervisor is not a good investment. This is why few very high scale sites, like Facebook and Google, virtualize most of their operational servers.

### VII. WHEN YOU DON'T HAVE A WAY TO MANAGE ENCRYPTION KEYS

Encryption keys are easy to manage on physical servers. When secure workloads move around because of virtualization, encryption key management designed for physical servers will not work. The obvious ways to try to solve the problem—using passwords or certificates stored on individual VMs—are not secure. Policy-based encryption key management is a requirement if you are going to run secure applications in physical, virtual, and cloud environments.

### VIII. WHEN YOU USE CLUSTERED APPLICATIONS WITH BUILT-IN FAILOVER

Modern virtualization platforms offer various flavors of high availability (HA) for VMs. Unfortunately, some applications, especially older, mission critical ones, also offer HA features. A good example is anything running Microsoft Cluster Services with a shared disk—setups like this will break in private clouds that allow VMs to automatically move around. If your virtualization platform is providing your HA, your applications should not, and vice versa.



## 10 REASONS NOT TO VIRTUALIZE

### IX. WHEN YOU WANT TO SAVE MONEY USING VDI EVERYWHERE

Servers cost more than cheap desktops. You still have to buy a PC or tablet or thin client—and manage and secure it too. Virtual desktops are great for security and compliance, but they are not a lower cost option for all types of employees.

### X. WHEN YOU ARE RUNNING VIRTUALIZATION PLATFORM COMPONENTS

If your virtualization platform and hypervisors rely on Active Directory or DNS servers, and those servers are virtualized, you will run into a catch-22 situation where you cannot start the hypervisor because it is waiting for services from the VMs that run on it. Ouch. You also need to check whether your virtualization management software (vCenter, etc.) can and should be run on the servers it manages.

## CONCLUSION

Even as you virtualize and access resources through private and public clouds, if you are like most enterprises, there is still a place for dedicated physical servers in your data center. But although you still rely on some physical servers, you should consider new server security with a solution that protects across your physical, virtual, and cloud servers.

Often companies attempt to use their dedicated physical server security across all three environments, but this does not address security risks unique to each environment, and it drives expensive cloud CPU cycles much higher. Instead, look to a solution that can work on all three platforms, but is designed to combat the threats unique to each—while also maximizing performance in each environment. Your data center will be a mix of server platforms, but securing across these servers doesn't need to compromise security or consume excess resources.

## FOR MORE INFORMATION

Follow these links for more information on Trend Micro security solutions:

- Security for physical, virtual, and cloud servers: [Deep Security](#)
- Data protection using encryption with policy-based key management: [SecureCloud](#)

Learn more about securing your journey to the cloud:

- Journey web pages: [www.cloudjourney.com](http://www.cloudjourney.com)
- Trend Micro cloud security blog: <http://cloudsecurity.trendmicro.com/>

©2011 by Trend Micro Incorporated. All rights reserved. Trend Micro, the Trend Micro t-ball logo, and TrendLabs are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. [WP01\_NoVirtualization\_111001US]

