

[Technology + Management Smarts]

[Technology Trends]

Sustainability, Sprawl, and the Biggest Security Mistake in Virtualization

Data storage is an ongoing challenge in an increasingly information-rich world. Add to that the push for sustainability, and lining up additional, more powerful servers on your network is both costly and out of line with your green strategy.

Sustainability

Network servers draw massive amounts of power, require floor space, and have cooling requirements. Virtualization, on the other hand, allows a single server to perform multiple tasks, without violating the best practice of having single use machines. It has become a mainstay in corporate America over the past five years.

“Advancements in virtualization technologies enable enterprises to get more computing power from the underutilized capacity of physical servers. The traditional datacenter footprint is shrinking to enable cost savings and greener IT through server consolidation,” said a recent Trend Micro white paper, *Making Virtual Machines Cloud Ready*.

Mark Tomaselli, CIO for First American Equipment Finance, agreed. “Virtualization requires far fewer physical machines. With virtualization, we can move applications from

server to server for maintenance – while they are in use – without a service interruption.”

Sprawl = Hidden Costs

One of the surprising downsides of virtualized machines is *actually the ease at which a server can be created*, causing “server sprawl.”

One company had 400 physical servers, which were later consolidated to 50 virtualized servers on about 5 physical machines. Then, over time, there were 600 virtualized servers set up (200 more than the starting point), all requiring maintenance, support and software licensing.

“Discipline is required with virtualization,” said Tomaselli. “Servers can be set up very inexpensively and easily, but there are hidden costs associated with each one.”



[continued on page 2](#)

Security in the Cloud

The internet is clearly the next evolutionary step in virtualization. Imagine this: what if your IT environment could manage itself, based on usage – like a utility – and you only had to pay for what you used? That is the goal of cloud virtualization, operating as intended.

According to Trend Micro: “Relying on cloud computing, enterprises can achieve cost savings, flexibility, and choice computing resources. They are looking to cloud computing to expand their on-premise infrastructure by adding capacity on demand.”

Providers like Amazon.com and others lease virtual server space on their massive and sophisticated system, and they also make it available for purchase.

Pay-as-you-go network power may sound like a dream come true, but as you well know, handling security in the cloud requires careful planning and constant maintenance to avoid costly mishaps.

“The cloud is obviously a multi-tenant environment, and controlling access is a major challenge.”

*- Mark Tomaselli, CIO
First American Equipment Finance*

Avoid the Biggest Virtualization Security Mistake

As these groundbreaking cloud virtualization technologies continue to become available, security is struggling to keep pace. According to

Network World, the biggest virtualization security mistake you can make is “not understanding that virtualization has pulled the rug out from under everyone’s security footing.”

Many companies incorrectly assume that virtualization security begins and ends with VLANs. But the reality is that cloud virtualization architectures change everything by opening new pathways that can be exploited. And, the simple matter of handing over the storage of your virtual business assets to a third party - outside of the walls of your office - can be a terrifying prospect.

In developing the security for these cloud-based virtualized machines, it is important to understand that virtualization architectures open many new pathways that must be protected. And only now are specialized security products for cloud-virtualized environments coming to market.

“The cloud is obviously a multi-tenant environment, and controlling access is a major challenge,” said Tomaselli.

Thinking about a multi-tenant environment is like thinking about an apartment building. If one of the tenants is robbed, will the robbers gain access to your apartment as well?

“Extending virtual machines to public clouds causes the enterprise network perimeter to evaporate and the lowest common denominator to impact the security of all,” said Trend Micro. “The inability of physical segregation and hardware-based security to deal with attacks between virtual machines on the same server highlights the need for mechanisms to be deployed directly on the server, or virtual machines.”

[continued on page 3](#)

Deploying this line of defense at the virtual machine itself enables critical applications and data to be moved to cloud environments. And as powerful systems like Salesforce.com and Office 365 are virtualized in the cloud, the stability and safety increases substantially.

Although the lure of immediate cloud-based computing resources is strong, it is crucial to look before you leap into internet-based computing. Before you deploy important corporate data and applications into the cloud, take a hard look at security risks from every angle, and ensure your business intelligence is protected. ➤

About Technology + Management Smarts

Technology + Management Smarts is a quarterly electronic publication developed for select customers of First American Equipment Finance. First American is an equipment lessor that excels at providing simple, innovative financing solutions for complex projects that combine products and services from multiple vendors and service providers into a single equipment lease. Headquartered in New York, with offices in Chicago, Los Angeles, and Naples, Florida, First American has satisfied customers in all 50 states. Visit us at www.fae.com.