virtual

DATA CENTER

Volume 21

TechTarget®
Where Serious Technology Buyers Decide

Considering the Cloud

I**S A MOVE** to cloud computing the best strategy for your organization right now? As with any big change, it's critical to weigh the pluses and minuses before jumping in with both feet.

If you're looking to save on costs, cloud computing might be for you. Instead of investing fistfuls of money in hardware and software and paying even more to maintain it, have a cloud provider bill you for only what you use. Scale it up or scale it down when you need to—it's your choice as the paying customer.

How about the negatives? If you're the type of data center manager that stays awake at night thinking about security and data integrity, then cloud computing may not be the answer to your prayers. A business with its data in the cloud has absolutely no control over where that data resides. That might be a deal-breaker—at least for now.

But keep an open mind. In Stephen J. Bigelow's "The Pros and Cons of Moving to the Cloud," cloud providers looking to expand their market have an enormous incentive to reengineer security models to reassure skittish IT shops. Stay tuned.

Even without cloud computing, virtual data centers have their hands full with security issues. What if one of your virtual machines (VMs) became infected with malware? And what if that malware started to probe the other servers on your network for vulnerabilities to exploit?

The live migration features of VMware and Microsoft are gaining popularity, but even they can pose a security risk unless they are implemented carefully. Microsoft MVP Brien M. Posey helps you sort through the security challenges unleashed by virtualization in "Security in the Virtual Data Center."

Finally, VMs are easy to deploy—maybe too easy. Don't be a victim of your own success. Learn how to identify virtualization sprawl and how to protect yourself against it.

In "How to Spot Virtualization Sprawl," Rick Vanover gives the most common warning signs and offer tips to combat growing infrastructure problems. Act now, and save yourself a boatload of trouble later.

Has security or virtualization sprawl been an issue in your data center? How did you nip it in the bud? Send an email to ccasatelli@techtarget.com, and tell us all about it. ■

CHRISTINE CASATELLI
Editor, *Virtual Data Center*

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

Pros and Cons of Moving to the Cloud

ORGANIZATIONS SHOULD CONSIDER TRADEOFFS AND IMPLICATIONS BEFORE MIGRATING TO CLOUD COMPUTING. **BY STEPHEN J. BIGELOW**

JUST ABOUT every modern business relies on IT to deliver and support critical services that keep the doors open and revenue flowing. But IT is also a huge cost center for modern businesses. Consider that all of your hardware and software must be maintained constantly, increased as businesses expand and completely updated every few years.

Business data must be protected, secured and guarded against disaster. And everything must be overseen by a trained and experienced IT staff. The emergence of cloud computing may very well change this traditional paradigm by providing businesses with subscription or demand-based IT services and infrastructure—treating an organization's IT as any other "utility" such as electricity or water.

Cloud offerings are available today, but the technology and practices are still evolving. Organizations should consider a variety of implications and tradeoffs carefully before making a move to the cloud.

IT'S ABOUT SHIFTING COSTS

A primary benefit to the cloud is cost optimization. Most organizations that adopt cloud technology see a fundamental shift in the way they spend money. For example, the huge sums of capital that would traditionally be invested in hardware, software and labor would shift to recurring operational costs that are tied more closely to the actual use of computing resources from the cloud provider.

The notion of computing as a utility is profound because it allows organizations to pay for services as they are needed. A traditional business might only need access to an application for a few crucial hours on any given day, yet the business would have to buy the entire server, install it, run it 24/7/365 and maintain it to have that application available. By accessing that application through a cloud provider, an organization can buy access only when they need it and scale that access up or down as needs dictate.

"An application that is only in use during the day and has peak use times, say at 9 A.M., 2 P.M. then 5 P.M., is a good fit

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

because you can scale down the application outside of these times to a very small—or no—footprint and scale it as high as necessary during these peaks," said James Staten, principal analyst with Forrester Research Inc.

> The simple fact is that a business with data in the cloud has absolutely no control over where that data actually lives.

But it's not just a reduction in—or elimination of—hardware purchases that warrants the attention of business owners. All of the overhead associated with owning and operating hardware is also eliminated.

"You also remove the headache of dealing with hardware and the management, asset tracking and memory problems," said Philip Cox, principal consultant with SystemExperts Corp., a provider of IT compliance and security consulting services. "Everything that goes along with maintaining hardware goes away," he said.

Every business that embraces the cloud will need to consider management. Cloud providers usually offer Web-based portals or tools that can aid end-user management, but third-party tools like RightScale, enStratus Networks, Cloudkick and others are pivotal in controlling cloud costs by managing deployment, scaling, monitoring and asset movement.

ASSETS CAN BECOME LIABILITIES

Although the benefits of cloud computing can be quite compelling, there's also a downside that every business must consider. The first major issue is security. The simple fact is that a business with data in the cloud has absolutely no

BENEFICIARIES OF THE CLOUD

ALL SIZES OF organizations can take advantage of cloud offerings, but small and midsized organizations can generally make the cloud transition more quickly and easily than larger organizations with a greater proliferation of different equipment.

"Larger organizations tend to be more heterogeneous," said Phil Cox, principal consultant with SystemExperts Corp., a provider of IT compliance and security consulting services. "Smaller businesses tend to be a little bit more agile. They can go to more of a homogeneous environment, and they can change quicker to adapt to what the cloud can offer." This also holds true for larger organizations with independent departments or divisions that act like small or medium-sized businesses.

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

control over where that data actually lives. This is a deal-breaker for health-care or finance organizations that must retain tight control over their data. There are also security concerns around multi-tenancy, although Staten said that serious breaches have yet to manifest themselves.

The second issue is availability. It's important to realize that a cloud provides no more availability than any other data center. The provider is still vulnerable to outages, congestion, human error, hacking, cyber-attack and other problems.

"All hosters are vulnerable to congestion due to not monitoring resource use as effectively as they should and for not optimizing resource configuration," Staten said.

Even the most conscientious cloud provider may carry planned downtime that may unduly interfere with your business needs. Consequently, organizations with high-availability requirements may have trouble adapting to the cloud.

It's important to realize that a cloud provides no more availability than any other data center.

[redacted]

WHEN GOOD CLOUDS GO BAD

RELIABILITY IS A major concern for cloud users—and with good reason. Business users have no control over the cloud provider, and disruptions in service can have a tremendous impact on every client's business. Consider the Salesforce.com outage that occurred in January. Although the outage lasted for only an hour, it affected both primary and backup systems, which disrupted service to all 68,000 Salesforce.com customers. Luckily, no customer data was lost in the incident.

But even more disturbing than the actual event was the lack of transparency or explanation from Salesforce.com surrounding the incident. Salesforce.com representatives said the company would not provide any information or explanation beyond what had been posted on its status page.

Most IT professionals and business owners recognize and accept the reality of cloud service disruptions, but this kind of closed response may do more to hinder cloud adoption than the actual incident itself. It certainly does little to assuage the concerns of other prospective clients. After all, how can a company trust its operations and data to a provider that won't communicate definitive answers when problems occur? This is an issue that providers and clients will grapple with more as cloud services grow. ■

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

There are broader areas of disruption that can affect cloud users. For example: A regional disaster can take a cloud provider offline for an extended period. Or the provider may go out of business. These are all real possibilities that can have profound consequences for businesses.

In addition, backups and data protection are not automatic with cloud providers, so clients should still establish, review and test their business continuity plans in the event that a cloud provider becomes unavailable or business needs dictate moving to a different provider.

And SLAs don't help much. Cloud providers do little—if anything—to ensure security or availability or response times for their clients. Most SLAs leave large time windows and "best effort" hedges that really don't provide any concrete guarantees for business owners.

Cox said that the cloud is a lot like the electric company. When the power goes out, it's fixed when it's fixed. And when disruptions occur, there is typically no recourse for clients affected by the outage. If an SLA is breached, the most a customer can expect is a rebate for the charges they would have paid during the outage. The point is that prospective cloud users really need to read and understand the SLA and then map it to their business needs before moving to the cloud.

STRIKING A BALANCE BETWEEN REWARD AND RISK

Experts say that the trick to successfully leveraging the cloud is to understand that it's not an all-or-nothing proposition. Given the limitations and concerns of cloud technology today, it's best to use the cloud with noncritical applications and nonsensitive data.

"If it's down for a day, we can live with it. Or if this data does get compromised in some manner, we're not going to lose our business," said Cox, adding that these direct benefits are ideal opportunities to evaluate the cloud model and provider. Don't put mission-critical data in the cloud, such as trade secrets, and avoid putting regulated data in the cloud such as healthcare—HIPAA-compliant—data, social security data, financial data and credit card—PCI-compliant—information.

> Experts say that the trick to successfully leveraging the cloud is to understand that it's not an all-or-nothing proposition.

Staten said that other types of services, too, should not be placed in the cloud, including any applications that don't work well as a virtual machine or applications that depend on complex clusters, such as Oracle RAC.

The real deal-breaker for potential cloud adopters today is the lack of flexibility and responsibility delineated in the provider's SLA. An SLA is crafted by the provider, and it's designed to protect the provider's interests—a provider sim-

EDITOR'S LETTER
○
PROS AND CONS OF MOVING TO THE CLOUD
●
HOW TO SPOT VIRTUALIZATION SPRAWL
○
SECURITY IN THE VIRTUAL DATA CENTER
○

ply won't take responsibility for anything beyond the uptime for its base services—typically, no more than 99.5%.

Providers make no guarantees of network bandwidth or latency and no guarantees of high availability for your apps or your storage, Staten said. "These all fall back to the IT ops guy who uses the service."

Because a client generally can't negotiate more IT responsibility for the cloud provider, the client has two simple choices—accept what the cloud provider is willing to do or don't use the service.

LOOKING TO THE FUTURE

Cloud computing is not a new idea. The notion of leasing access to applications or IT infrastructure and paying only for what you use is compelling to any business. So why does it seem to be taking so long for the cloud to mature?

There are several aspects. The first is accessibility—adequate and affordable business bandwidth has been around for only a few years. Another consideration is the provider's understanding of the market, identifying the need for new capabilities and learning to optimize those services as the client base grows. It's a natural progression that's still taking place.

"The Infrastructure-as-a-Service market is only 3 years old," Staten said. "SaaS took nearly 10 years to reach critical mass, and some would say it still isn't there yet."

Security concerns need a great deal of attention before the cloud can really become a major force in IT. Typical security models don't apply in the cloud and will have to be re-engineered—to the satisfaction of businesses and regulators—before cloud services really take off. Staten expects cloud providers' infrastructure to improve and become more robust, along with better APIs and support services that allow clients to exert a greater degree of control over the cloud services, utilization and cost.

Typical security models don't apply in the cloud and will have to be re-engineered—to the satisfaction of businesses and regulators—before cloud services really take off.

Ultimately, regardless of what the next few years bring, it's unlikely that the cloud will ever become a universal solution for every IT need. SLAs will continue to be a sticking point for cloud adoption. Continued pressure from clients will eventually prompt more favorable SLA terms—even if consumers wind up paying more for those favorable terms.

"It's a new option in the IT portfolio," Staten said. "There will always be justification for running your own servers, just as hosting didn't kill the corporate data center." ■

ENHANCED SECURITY
CLOUD COMPUTING
PLATFORM CHOICE
5
APP CUSTOMIZATION
MANAGED SERVICE LEVELS

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

How to Spot Virtualization Sprawl

LEARN THE MOST COMMON WARNING SIGNS AND AVOID LARGER INFRASTRUCTURE PROBLEMS. BY RICK VANOVER

VIRTUALIZATION sprawl can negate the many benefits of virtualization, which include cost savings, operational efficiencies and consolidation. Virtualization is a fundamental shift in how infrastructures are designed, provisioned, managed and operated, but virtual machine (VM) sprawl can create bigger virtualization infrastructure problems down the line. Learn how to identify virtualization sprawl and how to protect against it.

So what is virtualization sprawl? It occurs when the number of VMs on a network reaches the point where the administrator can no longer manage them effectively. VM sprawl warning signs can be remedied, but a single symptom does not necessarily indicate sprawl.

Identifying these symptoms, however, can prevent virtualization sprawl from becoming an issue in the future. Here are some of the most common warning signs of larger virtualization infrastructure problems:

SYMPTOM 1: LACK OF POLICY

The inability to manage consistent VM configurations is a contributing factor to virtualization sprawl. For most environments, operating systems need to have consistent configurations in areas such as administrative access, encryption settings, antivirus or malware protection and network settings. While streamlining these operations can pose problems for physical infrastructures, it can cause even bigger infrastructure problems for virtualized environments.

The inability to manage consistent VM configurations is a contributing factor to virtualization sprawl.

Active Directory (AD) is key technol-

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

ogy to help centralize these configurations. AD allows granular policy control to computer and user accounts. It can centrally manage how an OS—either physical or virtual—exists in the infrastructure.

Having well defined Active Directory principles prevents problems, such as scattered administrative permission assignments, uncoordinated antivirus software installations and configurations, inconsistent encryption settings for core services and unnecessary programs running on VMs.

SYMPTOM 2: UNMANAGEABLE UPDATES

If the second Tuesday of the month causes a scramble to deploy Microsoft patches, it's not going to get easier in a virtualized infrastructure without planning ahead.

Almost all virtualization deployments decrease the amount of physical equipment but increase the total number of OS installations. So, for example, how would this affect manually patching and updating systems after the number of systems double? In most situations, it quickly becomes unmanageable to manually perform Windows Update scans and upgrades on a rapidly growing infrastructure.

A planned approach, however, allows administrators to sleep at night. Tools such as Microsoft System Center and Symantec Altiris centrally deploy up-dates to virtual—and physical—machines with with sufficient policies and an adequate schedule. Although these products are not free, cheaper tools that are less sophisticated can update servers as well.

One option is to make Windows Update automatically run through Group Policy. This includes pushing out configurations that check for updates automatically, either through the registry or a scheduled task. Each server can be configured to automatically update, but this method lacks the central configuration push.

SYMPTOM 3: UNMANAGEABLE INVENTORY

If inventory management practices are not refined, the virtual world can be a nightmare. Take, for example, purchasing physical servers. Before virtualization, most IT groups had one or two people arranging the equipment purchases. With virtualization, however, there are usually more administrators with the permission to create VMs. But will everyone reconcile the inventory the same way? Probably not. But without implementing well defined policies, you may eventually be overwhelmed by the growing inventory.

There are free tools available to help address virtual inventory problems. For VMware environments, there is V-Scout by Embotics and VKernel's SearchMyVM. These products provide different functions, but each bridge the visibility gap in dynamically growing virtual infrastructures.

SYMPTOM 4: LICENSING COMPLIANCE/COST

If the number of VMs increases ahead of expectations, licensing and allocations figures may be at risk. No one wants to

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

be surprised at true-up time for software license inventories for servers or to run into a hard stop because of an exceeded license situation. VMs are quick and easy, but they are not free. One of the best ways to resolve licensing and allocation issues is to have a refined cost structure—or allocation costs—associated with each VM. For many environments, it can be represented as the following:

- **A slice of the virtual infrastructure.** This represents the targeted consolidation ratio divided by the host cost. If you plan on a 15:1 consolidation ratio and a virtualization host's storage costs $30,000, for example, the server hardware and virtualization management slice is $2,000.

- **Operating system licenses.** Although VM cloning, templates and other features allow for quick OS deployment, the licensing burden still exists. Put in the average operating system cost for the edition most frequently used. Also, consider the unlimited virtualization rights option for Windows Datacenter editions.

- **Management software.** If there are associated client costs for patching tools, antivirus software, compliance agents, backup software agents or other titles, these fees need to be added to the infrastructure cost.

Virtualization saves money, but you need to refine your cost model. A clearly defined cost model can prevent VM sprawl, which can create financial repercussions. Furthermore, use this opportunity to clarify the misperception that VMs are free in a virtual infrastructure.

SYMPTOM 5: TOO MANY SYSTEMS TO BACK UP

When a virtual environment grows so fast that the backup infrastructure cannot protect workloads, it can create the potential for disaster. In this situation, it's imperative to identify what needs to be backed up. If a VM runs a Windows service that was developed in-house and you are familiar with the installation process, a rebuild from a template may be a better option than investing the necessary time and storage required to protect the system. Then again, if all your systems need to be backed up, protection difficulties may arise. One possible solution: A provisioning approval process and a cost model can curtail infrastructure growth.

> Having well rounded policies and a defined cost model can protect an organization from virtualization sprawl in a data center.

When noticing these five VM sprawl symptoms, it's best to act immediately. In the planning stages, try to address these problems and other infrastructure issues before a virtualization environment is implemented. Having well rounded policies and a defined cost model can protect an organization from virtualization sprawl in a data center. ■

Virtualisation will be the target of new security threats
continued on page 12C
s to be getting warmer by tomorrow's end.
Today's data is hard to secure, and it's
95% of datacentres are deploying virtualisation
More virtual servers were deployed than physical servers in 2009
By the end of 2013 more than half of server workloads will be virtualised.
Johnson, Globe Staff
60% OF PRODUCTION VIRTUAL MACHINES ARE LESS SECURE THAN THEIR PHYSICAL COUNTERPARTS
THINK CONVENTIONAL SECURITY CAN PROTECT YOUR VIRTUAL ENVIRONMENT?

THINK AGAIN.

Enterprises around the world are relying on virtualisation to increase datacenter efficiency and, unknowingly, leaving themselves more vulnerable. That's because conventional security isn't able to protect virtual machines or see the traffic between them — leaving data and networks exposed. Which is why in 2009 sixty percent of virtual machines were less secure than their physical counterparts. But with Trend Micro™ Enterprise Security, powered by the Trend Micro™ Smart Protection Network™ infrastructure, you can mitigate the risk and maximize the benefits of virtualisation. It's a different kind of security that protects your physical and virtualised environments and helps set the foundation for your company to move confidently into the cloud.

Learn how to protect your virtualised datacenter.
Download the Trend Micro eBook at www.trendmicro.com/thinkagain

TREND MICRO™
Securing Your Web World

Security in the Virtual Data Center

SEPARATE THE MYTHS FROM THE FACTS ABOUT WHAT TO DO TO FEND OFF ATTACKS TO YOUR VIRTUALIZED ENVIRONMENT. BY BRIEN M. POSEY

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

IT SECURITY is facing a bit of a paradox. On one hand, the sheer number of security-related regulations that network administrators must comply with is unprecedented. On the other hand, these times are also a bit like the Wild West because the industry is only just beginning to understand the security implications associated with virtualization. So what should virtual data centers do to address security?

Let's start out by taking a look at the hypervisor, which is used by virtualization platforms such as VMware ESX and Microsoft's Hyper-V. There are a lot of myths surrounding the ability to exploit hypervisors.

One myth is that it is possible for an attacker to compromise hypervisors and then take control of the virtual machines (VMs) that are running on top of them. A similar myth is that an attacker may be able to use a weakness in a VM to break out of it—known as an escape attack—and seize control over the rest of the VMs running on the server. Although it is plausible that such attacks could eventually become a reality—there are certainly enough hackers working on them—no such attack methods exist today.

There have been several proof-of-concept attacks in recent years that were designed to install a thin hypervisor as a rootkit and then force the host OS into a VM. The idea was that the rootkit would be able to intercept all communications between the server's OS and the hardware. The good news is that the success of such proof-of-concept exploits is questionable.

At the moment there are no credible hypervisor attacks. But because that could change tomorrow, it is important to apply any patches that your virtualization platform vendor makes available.

AVOID TYPE 2 HYPERVISORS

There are two primary types of hypervisors in use today—Type 1 and Type 2. A Type 1 hypervisor is installed onto the server hardware at the bare-metal level. Type 2 hypervisors are installed on top of

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

a normal server operating system.

There are some advantages to using a Type 2 hypervisor—especially when it comes to performing server maintenance—but you are better off using a Type 1 hypervisor if your primary concern is security.

Experience has shown that the operating systems used beneath Type 2 hypervisors are often neglected, which can make them vulnerable to attack. In fact, I have seen real-world situations in which the underlying Windows operating systems beneath Type 2 hypervisors were not even domain members because all of the domain controllers had been virtualized, and the parent OS was required to boot before the domain controllers could be booted.

Even if your organization does not ignore its parent operating systems, it has long been accepted that one of the best ways to improve security is to reduce the attack surface. Type 1 hypervisors are much smaller than Type 2 hypervisors and, consequently, have a smaller attack surface. As an added bonus, Type 1 hypervisors also tend to perform better than their Type 2 counterparts because resources are not being consumed by a bloated parent operating system.

LIVE MIGRATIONS

Microsoft and VMware both offer a live migration feature that can be used to

OFFLINE VMs: A SERIOUS THREAT TO SECURITY?

VIRTUALIZATION PLATFORMS such as ESX and Hyper-V make it simple to create, delete, suspend and resume virtual machines (VMs). However, it is this flexibility that contributes to an often overlooked security risk.

To understand this, you have to know a little bit about the way hackers work. When it comes to security breaches, zero day exploits are rare. Most of the time, hackers attempt to breach security through the use of known vulnerabilities. Lists of such vulnerabilities are easy to come by. Not only are they posted on hacker sites, but Microsoft provides detailed information about each vulnerability every time it releases a security patch.

With that in mind, consider that most automated patching products are not virtualization-aware. Patch management products have no trouble patching VMs, but they have no way of knowing that a VM is in a suspended state. From the patch management product's perspective, a suspended VM looks like a physical computer that is turned off. The end result is that such machines are not patched.

When a suspended VM is eventually brought back online, it may be missing any number of critical patches. This makes such a machine vulnerable, especially if the network administrators are working under the assumption that every server in the organization is fully patched. ■

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

move a VM from one host server to another without an interruption in service. Although such features are all the rage right now, they can pose a security risk unless they are implemented carefully.

Hyper-V R2's live migration feature, for example, is based on failover clustering. When a live migration is performed, Hyper-V creates a new VM on the target server and then copies the initial memory state from the source server to the target server. When the process completes, any memory pages that have changed during the migration are marked and copied to the target server. It is the copying of memory pages that poses the problem.

Nodes in a Windows failover cluster use two separate network connections. One of these connections links to the normal corporate network, while the other is reserved for cluster-specific traffic, such as heartbeats. By default, Windows uses the cluster's private network for live migration traffic.

However, unless you explicitly deselect the primary network from within the Failover Cluster Management Console, live migration traffic can potentially flow across the corporate network in certain situations. This would give unscrupulous individuals a chance to sniff and read the contents of the VM's memory as the memory pages flow across the wire.

REGULATORY COMPLIANCE CONSIDERATIONS

THESE DAYS, more and more organizations find themselves being required to comply with various federal regulations governing the way that their computer systems are managed and maintained. Although the specific requirements can vary widely from one regulation to another, the general intent of the various regulations is to control access to network resources.

Complying with federal regulations is never easy, but the task can become much more complex in a virtual data center. Consider, for example, the use of management tools such as VMware's vCenter Server or Microsoft's System Center Virtual Machine Manager. These tools are designed to provide administrators with a comprehensive view of all of the organization's VMs, allowing those VMs to be managed through a single console.

In some cases, these handy tools may affect an organization's compliance status because they bypass barriers that may have previously been used to restrict physical access to certain servers. As such, it is important to determine exactly what the requirements are concerning your organization's use of virtual server management tools. In some cases, you may find that you have to place some of your virtual servers into a dedicated Active Directory forest to prevent them from being accessible to management tools operating within the organization's primary forest. ■

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

VIRTUAL NETWORKS

Without a doubt, the biggest gaping hole in virtual data center security has to do with virtual networks. It seems that just about everybody has a definition of what a virtual network is. For the purposes of discussion, though, let's define a virtual network as a logical set of network connections between VMs residing on a common host server. These types of virtual networks allow communications with each other without placing any traffic on the physical network. Herein lies the problem.

Imagine for a moment that one of your VMs became infected with malware. Let's also pretend that this malware was designed to begin probing the other servers on your network for vulnerabilities that it can exploit.

If this type of situation were to occur on a physical server that was linked to the network by a physical connection, the malware's activity would most likely be thwarted by your network's IDS. But if the attack happens on a virtual network, then the packets associated with the attack are never even exposed to the physical network. So your IDS remains blissfully unaware of the attack.

This principle can also apply to situations in which the virtual network is connected to a physical network. In that situation, traffic flowing between VMs on a common host server would typically be routed through the virtual network, while any traffic destined for the outside world would flow across the physical network. Traffic between VMs is still "off the radar" in spite of the existence of physical network connectivity because the virtual network is treated as an isolated segment.

Thankfully, virtualization vendors have finally gotten wise to these types of security issues and have begun designing products that can scan traffic flowing across virtual network segments for various security problems. VMware for example, has released VMsafe, an extensible engine that allows security vendors to develop tools that protect VMs and virtual networks while leveraging VMware code. Catbird has developed a VMsafe-based product called Catbird V-Agent that acts as a VMware certified virtual appliance running within a VM. Its job is to detect and prevent virtual network security threats from the inside.

> Without a doubt, the biggest gaping hole in virtual data center security has to do with virtual networks.

As you work to harden your environment, you should keep in mind that every major virtualization platform vendor provides a product-specific security best practices guide. It is important to remember that not every recommendation will apply to your data center.

Finally, check at least once a month to see if your virtualization platform vendor has released a revised edition to their best practices guide. As security threats change, vendors revise their best practices recommendations. Stay on top of them to be safe. ■

EDITOR'S LETTER

PROS AND CONS OF MOVING TO THE CLOUD

HOW TO SPOT VIRTUALIZATION SPRAWL

SECURITY IN THE VIRTUAL DATA CENTER

ABOUT THE AUTHORS

Stephen J. Bigelow, a senior technology writer in the Data Center and Virtualization Media Group at TechTarget Inc., has more than 15 years of technical writing experience in the PC/technology industry. He holds a bachelor of science in electrical engineering, along with CompTIA A+, Network+, Security+ and Server+ certifications, and has written hundreds of articles and more than 15 feature books on computer troubleshooting, including *Bigelow's PC Hardware Desk Reference* and *Bigelow's PC Hardware Annoyances*. Contact him at sbigelow@techtarget.com.

Rick Vanover (VCP,MCITP, MCSA) is an IT infrastructure manager for Alliance Data, a financial services corporation in Columbus, Ohio. Vanover has more than 12 years of IT experience and specializes in virtualization, Windows-based server administration and system hardware. Follow him on Twitter @RickVanover.

Brien M. Posey has received Microsoft's Most Valuable Professional award six times for his work with Windows Server, IIS, file systems/storage and Exchange Server. He has served as CIO for a nationwide chain of hospitals and healthcare facilities and was once a network administrator for Fort Knox.

TechTarget
Where Serious Technology Buyers Decide

Cathleen Gagne
Editorial Director
cgagne@techtarget.com

Matt Stansberry
Executive Editor
mstansberry@techtarget.com

Christine Casatelli
Editor
ccasatelli@techtarget.com

Marty Moore
Copy Editor
mmoore@techtarget.com

Linda Koury
Art Director of Digital Content
lkoury@techtarget.com

Jonathan Brown
Publisher
jebrown@techtarget.com

Peter Larkin
Senior Director of Sales
plarkin@techtarget.com

TechTarget,
117 Kendrick Street
Needham,MA 02494
www.techtarget.com

LINKS FROM OUR SPONSOR

HITACHI
Inspire the Next

- Hitachi IT Operations Analyzer Delivers Performance and Availability Reporting for IT Generalists

- Hitachi IT Operations Analyzer: Root Cause Analysis for Supporting Fault Identification

About Hitachi Data Systems: Hitachi Data Systems leverages global R&D resources to develop storage solutions built on industry-leading technology with the performance, availability and scalability to maximize customers' ROI and minimize their risk. By focusing on the customer's perspective as we apply the best hardware, software, and services from Hitachi and our partners, we uniquely satisfy our customers' business needs. With 2,900 employees, Hitachi Data Systems conducts business through direct and indirect channels in the public, government and private sectors in over 170 countries. Its customers include more than 50 percent of Fortune 100 companies.

LINKS FROM OUR SPONSOR

layeredtech®

- **Layered Tech: Superior Choice**
  Contact us today for a no-obligation 30-day trial on any of our range of cloud computing solutions. That’s CHOICE, one of our 5 levels of superiority.

- **Layered Tech: Superior Value**
  Alleviate your migration costs with a no-obligation 30-day cloud solution trial. That’s VALUE, one of our 5 levels of superiority.

- **Layered Tech: Superior Vision**
  Envision your company’s cloud computing future with a no-obligation Virtualization Assessment. That’s VISION, one of our 5 levels of superiority.

About Layered Tech: Talk about something super! Our new Virtual Private Data Center (VPDC) is a new hybrid, combining the best of both cloud computing and managed hosting solutions for your enterprise, with benefits never before available either in the cloud or with dedicated hosting alone. In addition to cloud computing’s amazing availability, processing power and scalability you’ll get enhanced security, a choice of managed service levels, and the flexibility to customize apps via a proprietary API. And it’s all available for the first time in one integrated package from the recognized leader in virtualization. Ready for a super powerful, super scalable hosting solution for your enterprise? Contact us today at info@layeredtech.com or 1-866-584-6784.

LINKS FROM OUR SPONSOR

TREND MICRO™

- Cloud Computing Security: Making Virtual Machines Cloud-Ready
- Meeting the Challenges of Virtualization Security: Server Defense for Virtual Machines
- Trend Micro Deep Security: Protecting the Dynamic Datacenter

About Trend Micro: Trend Micro is both a market leader in Internet content security and a security innovator. Always proactive, Trend Micro is leading the security industry by recognising the unique challenges of virtualisation and developing dedicated security solutions for virtual environments. While virtualisation offers many benefits to our customers, it also poses several unique security challenges. Trend Micro addresses these challenges with dedicated security for virtual infrastructure and is working with virtualisation innovators like VMware to protect virtual machine environments. Trend Micro helps organisations benefit from virtual computing by deploying security that's designed to meet these specific challenges, allowing our customers to fully realise the cost and productivity advantages of virtualisation without compromising the security of their data centre.