

**Strategies for Securing
Virtual Machines**

- 2** Virtual Threats
- 12** Virtual Security
Do's & Don'ts
- 20** Security for Virtual Servers
- 23** Preparing for
Security Unknowns

Virtualization Security

Space saving and a reduction in energy costs are causing many organizations to move to virtualized environments. We'll outline the security concerns and how to mitigate risk.

BY INFORMATION SECURITY AND SEARCHSECURITY.COM

SPONSORED BY

SOURCEfire®

**THIRD
BRIGADE**
deep security solutions

tripwire

Virtual Threats

BY DENNIS FISHER

Virtual machines may save you money in the data center, but can you ignore their security implications any longer?

Virtualization, like Web services and Wi-Fi before it, is the current darling of IT. Departments in enterprises, small- and medium-sized businesses and universities are deploying virtualization in huge numbers, mainly in the hope of saving money through server consolidation projects and reduced desktop system costs.

And like the other hot technologies of their time, virtualization is being deployed with little or no thought to security. The cost and power-consumption benefits that IT shops can realize through the use of server virtualization in most cases outweigh the real prob-

lems the technology can cause with security and compliance.

“I believe there are some holes in the scheme of things,” says Dennis Moreau, CTO of Configuresoft. “There are complications in how you mitigate threats and remediate problems because of the complexity that virtualization introduces.”

In most cases, IT shops in enterprises and other organizations are aware of some of these security considerations. But for many of them, the cost savings and efficiencies that virtualization delivers are too great to ignore (see “*Virtually Everywhere*,” p. 3).

“Cost is a huge consideration for us,” says VMware user Fred Archibald, network manager at the School of Computer Science and Electrical Engineering at the University of California, Berkeley. “Rack space in the machine room is also a consideration. We don’t have enough power or cooling to operate all of these servers, so it’s simpler to operate and manage a single machine with



“We don’t have enough power or cooling to operate all of these servers, so it’s simpler to operate and manage a single machine with several images on it. But I am concerned about the security.”

Fred Archibald, network manager, School of Computer Science and Electrical Engineering, University of California, Berkeley

several images on it. But I am concerned about the security. We have to have a relatively open network because we're a university, so we take it as it comes."

Virtualization—or, more specifically, the basic premise behind it—is nothing new. The technology to create virtual instances of operating systems has been around in one form or another for years, and has been widely adopted in some vertical industries in which costs and mobility are top priorities. The idea dates back to the days of mainframes and workstations, a model that required all of the actual computing to

be done on the mainframe with the results of the calculations then displayed on the terminal. This multiuser, time-sharing model maximized utilization of the mainframe's resources simultaneously. It proved to be quite efficient and was the standard for years, up through the advent of minicomputers such as the VAX and PDP.

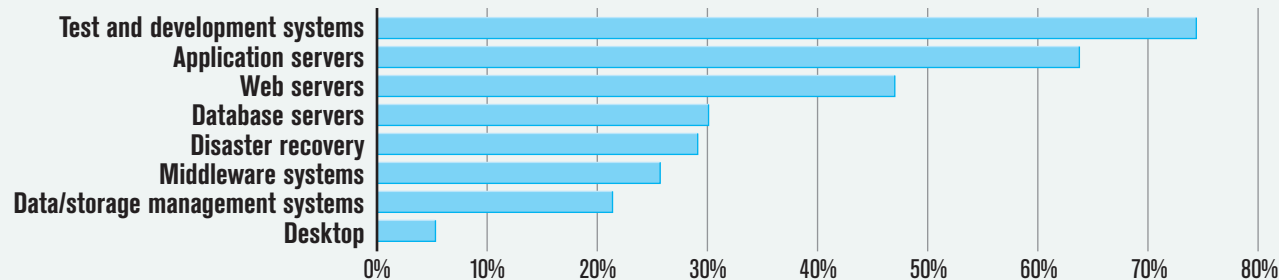
But the age of personal computing, which placed all of the computing resources on users' desktops, eliminated the need for centralized multiuser systems. And as PC storage capacity and power have grown, users have stored more and more data on

Virtualization—or, more specifically, the basic premise behind it—is nothing new.

DEPLOYMENTS

VIRTUALLY EVERYWHERE

Virtual machines are leaving a wide footprint inside the enterprise. Here's where they're being deployed.



SOURCE: Enterprise Management Associates

their machines, making them the primary targets of attackers. This, along with the need to reduce the number of physical servers in data centers to save money on hardware and power costs, has led to the current fascination with server and desktop virtualization. Indeed, a recent study by analyst firm Enterprise Management Associates (EMA) found that almost 75 percent of enterprises have deployed virtualization in some form.

TOUGH PILL TO SWALLOW

Security experts say that, although the concept of virtualization is decades old, the current usage models are still relatively new

and the security implications have yet to be fully worked out.

“The security issues really depend on the usage model,” says Nate Lawson, a senior security engineer at Cryptography Research in San Francisco, who has done research on the security models of virtual machines. “In server consolidation projects, there’s no firewall between the virtual machines, so if one gets compromised, it can be a platform for attacks on the others. Also, some people may be putting two different virtual machines with different security levels on the same host. No one has really done a full security analysis of VMware, so it’s possible that a well-designed attack could allow a

“In server consolidation projects, there’s no firewall between the virtual machines, so if one gets compromised, it can be a platform for attacks on the others.”

Nate Lawson,
senior security engineer,
Cryptography Research

THREATS

REAL OR PERCEIVED?

Details about attacks on virtual machines are sketchy; below are a few proof-of-concept and a traditional attacks that could impact your VM deployments.

Threat	Characteristics
Blue Pill	Utilizes the SVM/Pacifica virtualization technology in AMD chips to create a virtual machine in which the operating system executes and is controlled by a thin hypervisor.
SubVirt	Virtual rootkit that is permanently resident on the physical machine and sits under the machine’s OS.
Denial-of-service	Uses single or multiple virtual machines to consume all of the system resources of the host machine.
Trojan	Compromises the virtual machine manager, giving control of the VMM and any guest operating systems to attacker.

compromised virtual machine to escape from its partition.”

Details of confirmed attacks against virtual machines are sketchy at best, mainly because enterprises typically are reluctant to speak publicly about such incidents. (See “*Real or Perceived?*” p.4.) But security researchers have been actively working on methods for subverting VMs, and some of these theoretical attacks have drawn attention.

At last year’s Black Hat USA Briefings in Las Vegas, security researcher Joanna Rutkowska gave a presentation in which she described a stealthy piece of technology she’d been working on called Blue Pill. Sometimes erroneously called a virtual machine rootkit, Blue Pill is in fact a VM that installs itself on a host machine and then acts as the hypervisor, which controls the resource allocation and the interactions of the various virtual OS instances. This can be accomplished without restarting the target system, and there is no perceptible drag on the system’s resources, making it quite difficult to detect. Rutkowska’s technique relies on the SVM/Pacifica virtualization technology in Advanced Micro Devices’ 64 bit chips.

Although Blue Pill is still in the prototype stage, Lawson believes it has serious poten-

tial in the real world. “Once researchers understand this and it’s weaponized, you will see more things like this,” he says.

Indeed, researchers from Microsoft and the University of Michigan published a paper last year that describes a theoretical VM rootkit, called SubVirt, designed to sit under the VM hypervisor and observe and log all of the VM’s activities. Although SubVirt is simply a proof-of-concept exercise at this point, security researchers say there is little doubt that something like it is either already in the wild or soon will be. The special characteristics of VMs and the way they are often deployed—as controllers for mission-critical servers in data centers—can create maddening problems for administrators when machines are compromised.

“You have the threat now of these virtual machine rootkits that can lurk beneath the guest OS and applications, and you’re reluctant to reboot your entire virtual server farm in order to fix it,” says Moreau.

BALL IN VENDORS’ COURT

All of this, of course, begs the question: What can enterprise IT shops do to keep control of VMs in their environments? One of the main tools that administrators have

“You have the threat now of these virtual machine rootkits that can lurk beneath the guest OS and applications, and you’re reluctant to reboot your entire virtual server farm in order to fix it.”

Dennis Moreau,
CTO, Configuresoft

at their disposal is about as basic as it gets: group policy. In Windows environments, administrators can set group policy to prevent the installation of VMs, which can help stop developers, testers and other technically adept users from putting up unauthorized VMs. But this approach has limitations, not the least of which is that Windows group policies only apply to Windows machines. Most popular virtual machine applications, including VMware and Xen, can run on non-Windows machines. (See “Pick Your OS,” below.)

Also, group policy doesn't apply to code running on .NET frameworks or in macros,

and it is powerless to stop a new box, preinstalled with a VM, on the network.

But for the most part, the burden of securing virtual machines falls on the vendors themselves. Because the technology is fairly complex, many administrators shy away from making changes to the way VMs run and instead rely mainly on the native security of the virtualization software or operating system. Andi Mann, an analyst at EMA, says the vendors to this point have paid scant attention the security of their virtualization offerings.

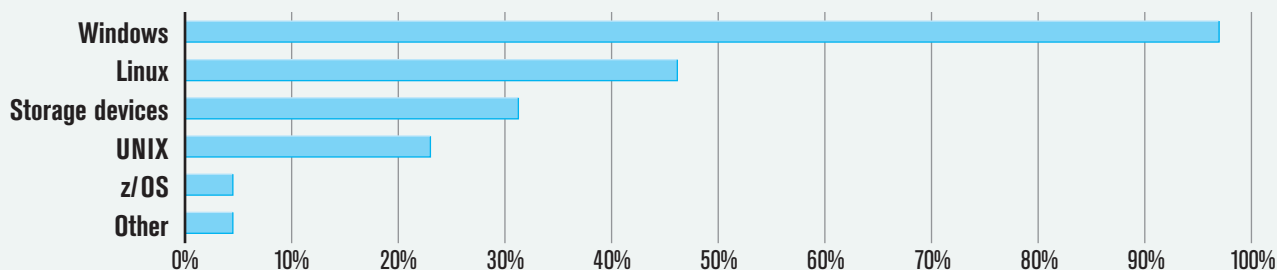
“It's a significant issue. Generally you're finding that the major players are not think-

Because the technology is fairly complex, many administrators shy away from making changes to the way VMs run and instead rely mainly on the native security of the virtualization software or operating system.

PLATFORMS

PICK YOUR OS

Windows is the most popular OS targeted for virtualization, but this technology is not exclusive to the Microsoft platform.



ing about security or even management,” Mann says. “But I’ll tell you who is thinking about it, and that’s the people who write viruses and other tools. There are a lot of issues on the server side because you don’t have that hardware protection that you used to have. There are some extremely damaging opportunities in virtual machines, and people are not looking at it.”

Officials at VMware challenge this notion, saying that server virtualization increases security in most cases, especially when a hypervisor is used.

“There is better security through the better isolation of the operating systems,” says Raghu Raghuram, vice president of product solutions and marketing at VMware. “Having a specialized hypervisor is important to ensuring security. Our virtual machines only communicate through the network, and what happens in one virtual machine doesn’t spread to another one.”

VMware’s offerings have a number of features designed to prevent abuses of the virtual machine infrastructure, including the ability to set limits on the amount of resources that any one VM can use to prevent DoS attacks. The company’s Assured Computing Environment enables customers

to use built-in security policies to set expiration dates for, and turn off device access to, virtual machines.

For its part, Sun Microsystems has made a number of changes to Solaris designed to make it easier for customers to use the operating system to support virtualization. The company has added an extra layer of protection in Solaris that allows executable programs to see the address space that is allocated to each application. There is also an option that allows customers to create a “no execution” area in memory to prevent buffer-overrun attacks. And, customers have the option of turning off virtualization in the BIOS in Solaris, which prevents virtual machines from running.

THINK THIN

The recent surge of interest in virtualization has meant big business for vendors like Sun, IBM and Novell, as well as a host of smaller vendors, who sell virtualization software and services. Much of the business these companies have seen so far has been in the data center as part of server consolidation projects. But experts expect that to change in the coming months and years as more organizations tire of losing laptops and having care-

“There is better security through the better isolation of the operating systems.”

Raghu Raghuram,
vice president of product
solutions and marketing,
VMware

less users foul up their machines beyond all recognition with spyware and viruses.

Sun and IBM in particular have well-developed architectures designed to enable customers to use thin clients on the desktop and large pools of virtualized server resources on the back end.

Such architectures are seen by experts and customers as net positives for security for a number of reasons, mainly because thin clients hold no data. Instead, the client machines are essentially little more than terminals that enable users to access their desktop images, which are hosted on a server. The EMA study found that 52 percent of enterprises that have deployed virtualization cite security as a main driver for their decision.

“There are important security reasons for deploying thin clients. The biggest one probably is the close control of data on the endpoints,” says Patricia Bolton, CTO of IBM Global Services’ End User Services Group.

“There is no data on the endpoints in this configuration, which is key because a lot of businesses now are concerned about the proliferation of sensitive data within their organizations,” she says. “Every time you hear about a laptop being stolen, that’s the big concern.”

Bolton points out that many organizations in recent years have eliminated all of the labor costs they can in IT, and that now the cost savings must come from other places.

“Supporting end users is a huge cost,” she says. “The idea of replacing laptops just for mobility’s sake is not appealing.”

At this point, however, servers are the main focus of most enterprise virtualization efforts; EMA’s numbers show that only 5 percent of enterprises have a desktop virtualization deployment.

The benefits of server virtualization are myriad, but the main attraction for most companies is the ability to use one physical server to host multiple instances of an operating system or several different operating systems. In this type of deployment, an application such as VMware ESX Server acts as the host OS on the server; administrators can then load several other operating systems on the same physical server. Each OS has its own dedicated set of hardware resources, including RAM, NICs, a CPU and a hypervisor.

This configuration gives administrators the ability to reduce the number of physical servers they deploy, while also keeping each instance isolated from all of the others on

“There are important security reasons for deploying thin clients. The biggest one probably is the close control of data on the endpoints.”

Patricia Bolton,
CTO, IBM Global
Services’ End User
Services Group

the same machine. That basic design is meant to increase security by preventing data from leaking between virtual machines or malware from jumping from one VM to another. A second type of server virtualization involves using an OS such as Solaris or Linux to act as the management layer and host other instances of the same OS.

“There is such a euphoria around this, and security is not at the forefront of people’s minds,” says Graham Lovelle, senior director of x64 systems at Sun. “Money savings are driving the interest in virtualization. But risks

do exist. It all starts with the robustness of the virtualization layer. VMware has proven to be enterprise-ready, but as you get any volume of software that goes up, people will write exploits against it. And those are potentially more insidious because they attack the layer that holds multiple operating systems. I do expect more attacks.”*

Dennis Fisher is executive editor of the TechTarget Security Media Group.

VMware has proven to be enterprise-ready, but as you get any volume of software that goes up, people will write exploits against it.

Security is a Virtual Reality

The same best practices that apply to a physical infrastructure apply to a virtual one as well. BY NEIL ROITER

Virtualization is changing the face of corporate IT, reducing the number of physical servers, saving space and cutting energy costs.

Its flexibility and ease of deployment enables companies to respond rapidly to new business initiatives and requirements. Gartner predicts more than 4 million virtual machines will be deployed by 2009.

Does this change the security environment? Yes and no.

“The baseline is that virtual infrastructure is quite similar to physical infrastructure in terms of security,” says Patrick Lin, VMware’s director of product management for data center platform products. “It doesn’t absolve you of following good security practices.”

Virtualization, in fact, improves security practices in some respects. It’s easy to create and deploy “gold” master server images, both for new deployments and for restoring compromised servers to a good state. It’s ideal for testing patches on multiple configurations without additional hardware or exposing production systems.

That also means security managers must remember that, as in a physical network, one compromised server can affect others. Each guest server must be protected.

“People sometimes assume that virtual machines are isolated from each other; the user interfaces of these tools seem to imply isolation,” says Ed Skoudis, founder of security consultancy Intelguardians.

“From a security perspective, generally, users in virtualized environments are still using the same tools in each guest that they are for physical servers, says Simon Crosby, CTO of Virtualization Citrix. “No one has gotten to the point in which the hypervisor offers security to multiple guests. That’s still coming.”

The shadow factor is the risk—mostly theoretical, at least for now—that the hypervisor itself can be exploited and controlled through some vulnerability and used to subvert the guest VMs.

“We advise people to assume the ability of an attacker to jump from guest to host to guest is a possibility, and to architect virtualization accordingly,” Skoudis says.

The biggest risk, perhaps, comes from the adage that complexity breeds insecurity.

IT security staff used to associating security practices with boxes and wired networks have to be alert to changes. Virtual servers are easily and transparently moved to maximize bandwidth and computing resources; dormant high-availability servers need up-to-date patches and configurations.

The danger is acute if business-critical, high-security VMs occupy the same physical box as less secure servers. Best practice requires

that enterprises group like servers from a security perspective.

It may be more complex than that. Maintaining—or even knowing—the correct configuration requirements may be problematic.

“There could be conflict when I change configurations and patch, given the complexity of SAN, virtualization software and the OS,” says Dennis Moreau, CTO of Configuresoft. “Best practices have focused on each layer in isolation, but what’s best for storage may not be for an application.”

This means thinking in terms of dynamic situations, in which one gold standard for a given OS or application doesn’t necessarily apply.

“IT has to connect dots across the components,” says Moreau. “How do virtual components impact each other?”

“Security is not a problem perceived by customers; they’re focused on performance and achieving consolidation,” says Citrix’s Crosby. “The bad guys are not paying attention yet, but this will increase as the number of virtual machines increases.”*

Neil Roiter is *Information Security* senior technology editor.

Will Using Virtualization Software Put an Enterprise at Risk?

BY MICHAEL COBB

Question:

What are the security-related pitfalls of moving toward a virtualization environment and creating multiple-application systems on a single server?

Answer:

Although virtualization isn't a new concept, there is certainly a renewed interest in its use. A virtualized IT infrastructure can increase system availability and flexibility, and its more efficient use of resources can cut ownership costs. Dell Inc., for example, uses a server farm that runs virtualization software to provide more than 1,000 test and development environments on fewer than 100 physical servers. This greatly reduces the time spent setting up test environments.

One often cited benefit of virtualization is the technology's ability to simplify operations and consolidate the number of servers and machines in an organization. Your administrators, however, will need to learn how to configure and maintain a virtual IT environment. Not only is there a vast amount of terminology to understand, but most virtualization products also require additional hardware or software. This requires an understanding of the many choices of available hypervisors and hardware, and how each should be properly configured.

Once a virtual environment has been created, compliance and auditing must also evolve to handle the physical and virtual systems. This means finding a way to measure resource usage and cost allocations among applications across a shared infrastructure, because seri-

al numbers and physical locations are meaningless in the virtual world. Remember, if you can't measure what's on a virtual system, you can't obtain maximum benefit from it. Also, unless meticulous image cataloging is enforced, "image sprawl" and orphaned images can cause delays and overwhelm an IT staff. All this, not to mention the threat of possible rootkit hypervisors, adds to the burden of keeping virtualized systems secure.

Virtualization software can cause unpredictable errors, and the host is a potential single point of failure for all the instances that it hosts. Also, many software applications offer limited virtualization support. In the future, administrators will need to create an environment that preserves existing investments in such software licenses.

The other challenge over the long term will be to realize the benefits of licensing models that favor virtualization. To maximize savings, you will need a full understanding of contracts and vendor license options.

Despite all of these pitfalls, the benefits of virtualization make the technology well worth considering. With virtualization, IT administrators can consolidate their physical infrastructures, preserve their investments in existing operating systems and applications, and get more from their hardware investments. As virtual environments grow, there will also be additional benefits to business continuity and capacity management strategies.*

Michael Cobb, CISSP-ISSAP, is founder and managing director, Cobweb Applications Ltd., a consultancy that offers IT training and support in data security and analysis.

5 Virtualization Security Do's & Don'ts

BY THOMAS PTACEK

Virtualization changes the game for enterprise IT, but security doesn't have to be a barrier to implementation.

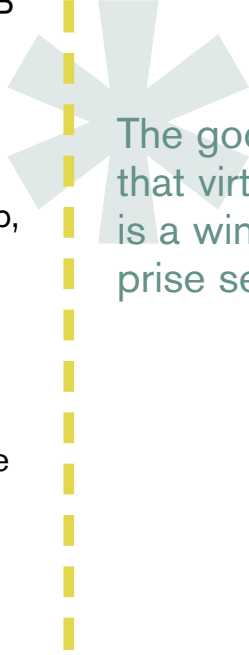
Five years from now, few enterprises will use “real” computers. Everything done with databases, Web applications or file shares will be intercepted and emulated by virtualization software, allowing one rack-mount server to act like 10.

Virtualization is inescapable; it's the most

important new force in enterprise IT since IP networks.

A security professional could be forgiven for feeling a lingering sense of dread about the implications of this trend. On internal networks, virtualization is redrawing the map, taking servers and applications that were once separated by hardware and network filtering and cramming them onto the same blade server. No change that far-reaching could come without security challenges, and the products we're using to make those changes aren't even 10 years old.

The good news is that virtualization is a win for enterprise security. Patching, staging, deployment and change management—



The good news is that virtualization is a win for enterprise security.

chronic headaches for IT security—get easier in virtualized data centers. The bad news is, before virtualization solves those problems for us, we've got challenges to overcome. In no particular order, here are five do's and don'ts for avoiding virtualization pitfalls.

1 DON'T LET YOUR ENTERPRISE SILO VIRTUALIZATION SECURITY

An enterprise typically has Windows administrators managing Windows security, Unix administrators for Unix security and storage administrators to keep the SAN locked down. Thinking that organization is also going to work for VMware ESX clusters is a fatal mistake.

“The organizational impact of virtualization is profound,” says Christofer Hoff, chief security architect at Unisys and an expert on virtualization security. “A lot of companies are getting caught flat-footed” by virtualization security, he says, and networking teams are throwing up deployment roadblocks. So long as it's only the VMware admins left holding the ball on security, nobody else has any skin in the game. What you're left with is a fragmented, half-deployed architecture

where security is an afterthought.

Think back to the 1990s, when enterprise switching and VLANs emerged. Lack of cooperation and a poor game plan for security left us where we are today with open, uncontrolled networks where one hacked help desk computer can threaten mainframes and storage networks. don't let that happen again.

Virtualization gives enterprises a second chance to get the IT security playbook right. Server admins should have a plan for staging, deploying and patching virtual machines. Network admins should have a plan for keeping access rules tight and consistent around physical servers and between guest operating systems. And security teams should have policies in place to audit configuration and deployment.

2 DO PRACTICE SEGMENTATION ON YOUR PHYSICAL VM SERVERS

Some guest hosts are going to handle sensitive data, such as credit cards or protected health information. Others won't. don't let these two types of VMs share the same hardware.

“The organizational impact of virtualization is profound.”

Christofer Hoff,
chief security architect,
Unisys

For proof of why segmentation is critical, ask Tavis Ormandy. Last summer, Ormandy published an in-depth study of virtualization security with a report documenting “iofuzz,” a tool that uncovered vulnerabilities in practically every virtual machine hypervisor he tested. When it comes to virtualization, “x86 is tough to get right,” he says. For Ormandy, the idea that developers will have an easier time writing secure hypervisors than secure operating system kernels is a tough sell. Ouch; it took more than a decade to lock down Windows.

What does a hypervisor vulnerability mean? Just this: someone with access to any one of your VMs can “jailbreak” into the host and compromise the rest of them. Isn't that a good enough reason to keep sensitive VMs on separate hardware from testing VMs?

And jailbreaking vulnerabilities aren't the end of the problem. Consider all the network security mechanisms you've put in place to guard your data centers. Or, don't, because when it comes to traffic running on “virtual switches” between guest hosts on the same hardware, none of it matters. “Trying to replicate high-availability network security given today's virtual switching introduces really nasty performance and availability issues,”

GLOSSARY

Virtualization Lexicon

Here's a cheat sheet to help navigate virtualization.

VIRTUALIZATION • Technology that enables a single computer to run multiple operating systems simultaneously, each behaving as if it had sole access to the underlying hardware.

GUEST (aka VM) • A virtual machine. Run Windows Server 2003 “under” VMware and you have created a “guest” virtual machine.

HOST (aka HYPERVISOR) • The software that enables the virtual machines to run, or, alternately, the operating system instance on which that software runs. VMware Server is a hypervisor that runs on a Windows XP host operating system; VMware ESX is a hypervisor and its host operating system.

MIGRATION • A virtualization feature that allows a running guest to be transferred from one physical server to another, without necessarily halting the virtual machine.

SNAPSHOT • A virtualization feature that allows “versions” of a guest system, hard drive contents and all, to be stored and later recovered.

VIRTUAL SWITCH • The software inside a hypervisor that emulates a network, allowing guests to communicate between themselves (“inter-VM”) and with the outside world.*

—THOMAS PTACEK

says Hoff.

What should you do? The answer is technically simple but organizationally difficult. Enterprises need to figure out what their security domains are, gaining a sense of

what their most sensitive data is. Then, machines that handle that data need to be kept on isolated hardware, whether it's efficient to do so or not.

DON'T IGNORE THE RISKS OF VIRTUALIZATION ADD-ON SERVICES

Aside from the issues associated with network security and virtual machines, companies need to think through virtual machine migration. Migration features like VMware's "VMotion," which allows a VM to hop from one hardware platform to another without downtime, are one of the ideas that get enterprises interested in virtualization in the first place. But they can play havoc with security.

Many IT teams are relying on virtual machines as "virtual security appliances," through which all traffic in and out of application VMs must be routed. That can be a problem, explains Hoff. Those VMs "don't take well to being "vmotioned," because the things that protect them don't move with the VM."

It gets trickier. Last year, a research team at the University of Michigan published a

report at USENIX demonstrating attacks against migration in VMware and Xen, the two most popular platforms. Their modus operandi: rewriting virtual machines on the fly as they crossed the network. By the time they landed at their destination server, operating systems that had been secure just moments before were backdoored.

Don't overlook backup, either. Checkpointing and snapshotting capabilities (see "*Virtualization Lexicon*," p. 14) in virtualization software are giving rise to a cottage industry of special-purpose products that promise to streamline backup storage for systems like VMware ESX. There is no more sensitive function in IT than backup and disaster recovery, which handle vast quantities of protected information. Be sure your backup vendor understands that.

How does a company know if its VMware backups are safe? It should ask its vendor if a third party has tested the security of its product, and if so, what did the tester find? Vendors that skip this step invite disaster. Network backup products want the keys to log in to all your virtualization servers; if they have bugs, attackers can steal those keys and with them every virtualized host in your enterprise. *Caveat emptor.*

Aside from the issues associated with network security and virtual machines, companies need to think through virtual machine migration.

DO CONSIDER VIRTUALIZATION SECURITY PRODUCTS CAREFULLY AND CRITICALLY

The virtualization security product market is an emerging industry to keep a watchful eye on. "It's a splashy area of security," says Marty Roesch, CTO of network security vendor Sourcefire and creator of the Snort intrusion detection project. "People are asking us what we can do." But he questions whether that's the right battle for enterprises to fight.

Roesch asks why the intra-VM traffic, running between guest operating systems on the same hardware, is "so much more important than the traffic at the switching and access layer."

For years, enterprises have struggled to get security policies right on the internal network. Perhaps zealous efforts to get security deployed in every virtual switch shouldn't take priority over solving security on real networks.

"I have to ask if it's better to deploy security in 200 server blades, or whether your threat is coming from outside in. How is it better to have sensors watching each blade individually, as opposed to watching one at the uplink?" Roesch says.

Because it's cheaper, counters Aaron

Bawcom, vice president of engineering at Reflex Security, a virtual network security company. "We've seen customers with hundreds of locations, each with multiple point-of-sale systems rolled up into a few servers handling the IT infrastructure for that location. Have you looked at the cost of deploying just a firewall at a thousand sites?" The cost of deployments like these is so high, he says, companies are simply paying the fines from credit card industry audit violations rather than re-architecting the network.

Rather than deploying hardware to every branch, Bawcom wants enterprises to consider exploiting virtualization to consolidate servers at branch offices. Once you're managing just a single physical server and three virtualized guests, you can implement network security simply by adding it to the virtual switch. "With hardware appliances, there's a barrier of ROI that you can't get past. When you virtualize security, you can deploy more of it for less cost and more value," he says.

One area in which Roesch and Bawcom agree is security monitoring. "Network visibility thrives when you deploy it as virtual appliances at the hypervisor level," says Roesch, "because when you have tools to

"I have to ask if it's better to deploy security in 200 server blades, or whether your threat is coming from outside in. How is it better to have sensors watching each blade individually, as opposed to watching one at the uplink?"

Marty Roesch,
CTO, Sourcefire and
creator of the Snort
intrusion detection project

distill it for you, the more information you can get, the better.” For Bawcom, virtualization also creates new opportunities for management, allowing enterprises to get a top-down map view of their systems and to go back in time to see what’s changing.

None of these benefits are free, however. “Virtualization doesn’t reduce security costs,” argues Hoff. “You’re still deploying the same agents everywhere; same intrusion prevention, same antivirus.” The implication is that the flexibility of virtualized environments can also be their undoing. “Virtual security appliances are being asked to screen every single traffic flow. Just when you think you’ve got the memory and CPU constraints for that worked out, 10 more VMs get migrated to that server. It’s very difficult to forecast how much throughput you’re going to need,” he says.

There’s an elephant in this virtual security room. Far and away the most popular provider of enterprise virtualization is VMware, and VMware has not been standing still on security. VMware is in position to make virtualization security a feature instead of a product, but for now, the company is giving mixed signals. Its recently announced VMsafe initiative promises to make VMware

hypervisors more accessible to third-party vendors. But last year, it purchased Determina, an up-and-coming host security company. VMware now finds itself supporting a top-caliber security research team staffed with researchers such as Alex Sotirov and Oded Horovitz, both famous vulnerability hunters, neither of whom is just sitting around doing nothing.

Ultimately, enterprises need to apply a healthy dose of skepticism when it comes to virtualization security products. Ormandy puts it simply: “People still believe that virtualization can be a security silver bullet, which does not reflect current reality.” Virtualization security products can offer opportunities for more widespread network security coverage, but those opportunities should be clear, compelling and immediate before an enterprise acts on them.

DON'T LET VIRTUALIZED MALWARE KEEP YOU UP AT NIGHT

Here’s something that isn’t clear, compelling and immediate: the threat of virtualized malware. What’s virtualized malware? It is Trojan horse rootkit software that

Just when you think you’ve got the memory and CPU constraints for that worked out, 10 more VMs get migrated to that server. It’s very difficult to forecast how much throughput you’re going to need.”

Christofer Hoff,
chief security architect,
Unisys

exploits hypervisor technology to hide itself “above” the infected operating system. The grim promise of virtualized malware is rootkits and botnets that are undetectable.

Anyone who follows security carefully has probably heard about virtualized rootkits. As a news story, it writes itself: virtualization is hot, and security attacks always make good reading. But how much of a problem are virtualized rootkits in the real world? Not much at all; they're essentially never seen in the wild.

So why aren't we seeing a new wave of malware taking advantage of virtualization capabilities? Researchers developing proof-of-concept rootkits might argue it's because we're not looking for them, or able to find them with our current tools. But that might not be the case.

Last year, this writer worked with Nate Lawson from Root Labs and Peter Ferrie from Symantec to develop techniques for detecting virtualized rootkits. We found so many ways to do it that we doubt the pursuit of “undetectable” virtualized rootkits is a good strategy. The team's key finding was that virtualization does a great job of hiding itself from applications that aren't looking for it, and that's enough to keep the lights

IMPLEMENTATION

Insurance Policy

Esurance makes security a priority as it steps into the world of virtualization.

When Esurance embarked on virtualization, it undertook the project like any other: securely.

“Security is part of our DNA at Esurance,” says Marjorie Hutchings, director of Internet operations at the San Francisco-based online insurance company. “No matter what we implement, security is at the forefront of each project.”

Esurance, whose television ads feature Erin, a pink-haired cartoon crime fighter, deployed VMware in its pre-production environment and more recently virtualized its enterprise directory services. In implementing virtualization, the company adopted the same types of security measures it has in its physical infrastructure, Hutchings says.

That includes antivirus software, strict administrative controls, and monitoring for any kind of configuration changes to guard against misconfigurations. Virtualization makes it easy to enforce a hardened server build, she says.

The company also isolates the management network in the virtualized infrastructure, and keeps virtual machines with sensitive data separate from others.

“We make sure to pay extreme attention to securing the virtual drive image as well as the virtual machine template,” Hutchings adds.

Virtualization allows the fast-growing insurance firm to bring up additional development environments quickly, easily and properly configured while saving on hardware. The technology also helps the company with its green initiative, Hutchings says: “Virtualization allows us to save power and energy and reduces our carbon footprint.”

Esurance, which has more than a half million policyholders in 28 states, hopes to expand its use of virtualization into its production environment, possibly next year.*

—MARCIA SAVAGE

on and the hard drives spinning. But when you look closely, illicit hypervisors leave tell-tale signs that are extraordinarily hard to conceal.

It's not all good news. The rootkit threat is very real; it's just more likely to bite at the application layer. There are only a few virtualization platforms for a rootkit to hide in; we can audit those. But there are tens of thou-

sands of applications, each with hiding places for backdoors and rootkits. Without a doubt, enterprises will need to remain vigilant in the era of virtualization.*

Thomas Ptacek is a founder and principal at consultancy Matasano Security.

The rootkit threat is very real; it's just more likely to bite at the application layer.

How to Build Security into a Virtualized Server Environment

BY THOMAS PTACEK

Tactics for thwarting attacks against virtual machines.

Virtual machines are to today's enterprises what VLAN switching was in the '90s: a transformative technology that simplifies IT, so compelling that it promises to become ubiquitous in a short period of time.

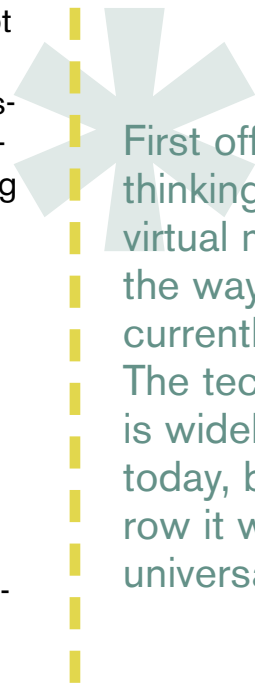
Unfortunately, there's no such thing as a free lunch. Enterprise security teams largely ignored the security implications of VLANs. Today, as a result, penetration-testing teams can often break into a receptionist's desktop

computer, for example, and get a clean shot at mainframes and storage networks.

How can the industry avoid the same mistakes with virtualization? By tracking virtualization technology as it evolves, and thinking like an attacker. In this tip, we'll cover ways to proactively build security into a virtual server environment.

SERVER VIRTUALIZATION REQUIRES NEW THINKING

First off, stop thinking about virtual machines the way they're currently used. The technology is widely deployed today, but tomorrow it will be universal. New applications simply aren't going to be deployed on physical hardware; soon nearly all appli-



First off, stop thinking about virtual machines the way they're currently used. The technology is widely deployed today, but tomorrow it will be universal.

cation servers will be managed from a virtualization console.

Look at that architecture the way an attacker would: Virtualization controls every application in the enterprise. Therefore, virtualization infrastructure is the most valuable target on the network. It's the first thing they're going to go after.

USING POLICY AND TECHNOLOGY

Next, remember an iron law of IT security: no matter what policies and controls are in place, some machines will be compromised. Plan for it.

Before virtual machines, those compromised systems gave attackers access to the internal network. With virtual machines, not only do they get access to the network, but also any attached virtualization infrastructure, putting all virtualized systems—and the data they contain—at risk.

The most important challenge in virtualization security is to prevent that access from being a “game-over” threat that surrenders every other virtual machine in the enterprise. How can that be accomplished? Here are some tactics:

- **Segment virtual machines by the information they handle.** Yes, high-security

virtual machines will manage credit card numbers, medical information and other data of the highest importance. But there will still be plenty of virtual machines designated for quality assurance and systems testing where the administrator password is “password”. Count on it. don't make the same mistake we made with VLANs: have a policy, spelled out up front, that those two types of virtual machines can never share the same hardware. However unrealistic it may sound today, assume that if an attacker can run code on one VM, they can run code on every other VM on the same machine.

- **Watch out for cryptography.** Enterprises use it in more places than you may think, like to power Active Directory servers, to secure SSL connections, and to generate session cookies on Web applications. Virtualization does an imperfect job of protecting cryptographic secrets, because of timing artifacts hidden in the underlying hardware. don't deploy financial applications on virtualized shared hosting.

- **Create standard locked-down images.** Host security matters more under virtualization, because virtual machines that share hardware can often talk to each other

Look at that architecture the way an attacker would: Virtualization controls every application in the enterprise.

directly. Your whole organization should use exactly one baseline Windows server installation, or exactly one Linux build. That build should be locked down tight; in other words, hardened and configured with a minimum footprint and maximum security controls.

- **Secure storage, migration and back-up.** Virtual machines are often stored on storage area network (SAN) technology like iSCSI, migrated over standard TCP/IP networks, and backed up using FTP. What's key to remember about all of this is if an attacker

can see and change those virtual machine bits in transit or at rest, he or she can easily rewrite the virtual machine, negating your security entirely. Control access to virtual machine storage as tightly as you do access to your domain Administrator passwords and SSH keys.*

Thomas Ptacek boasts more 10 years of product development and security research experience prior to founding consultancy Matasano Security.

Your whole organization should use exactly one baseline Windows server installation, or exactly one Linux build.

Preparing for Virtualization Security Unknowns

BY MIKE ROTHMAN

Virtualization changes the definition of servers and data centers. As a result, securing virtualized environments will be a challenge.

Virtualization is all the rage in the data center world, and for good reason. With the typical server running at less than 40% utilization, virtualization can make more effective use of technology resources and lead to substantial cost savings. Given the expansion of EMC Corp.'s VMware subsidiary and a number of other virtualization platforms, the technology is clearly in rapid growth mode.

Per usual, security is an afterthought,

which is a huge problem. Virtualization changes the definition of servers and data centers. As opposed to physically distinct servers connected over a network (that can presumably be secured or monitored), a virtual environment is an isolated, self-contained “data center in a box,” and when all the process-to-process communications that have happened over a network in the past are instead happening inside a single IT enclosure, there’s no doubt that security ramifications will be significant.

The fact is that no one knows how much virtualization is going to upend the 15 years of work the industry has invested to build defenses for systems and applications. In order to grasp the situation, it’s important to understand that security functions are different in a virtualized world.

To again be clear, it’s impossible to say



The fact is that no one knows how much virtualization is going to upend the 15 years of work the industry has invested to build defenses for systems and applications.

exactly what the most significant virtualization security challenges will be, but here are some key points to consider.

- **Network defenses are moot.** Most network defenses are predicated on seeing traffic, comparing either packets or behaviors to what it knows to be malicious, and then taking action. If the traffic can't be seen, a network-based approach to work within the virtualized server must be implemented. In other words, monitoring inter-process communications within the virtual machines or between a virtual infrastructure that spans multiple physical machines.

The definition of the “network” in a virtualized world is significantly different, and requires different defenses. Blue Lane Technologies Inc. and Reflex Security Inc. are two of the vendors already working to solve the problem, whatever the problem turns out to be.

- **Hypervisors are great (to attack).** Everyone talks about how insecure the OS is. Yes, all of the OSes are insecure, but to add a bit more complexity (what's a bit more complexity between friends), it means layering a whole mess of potentially insecure

OSes on top of what is potentially another unsure OS—the hypervisor.

For those of you not familiar with virtualization terminology, the hypervisor is the software abstraction layer between the bare metal and the operating system instances that run on top of it. This is software, and as is the case with most software we all know it is pretty much vulnerable. The question is how vulnerable? The stakes are high; if the underlying hypervisor is compromised, it's possible to own all of the virtual machines that run on top of it.

If the hypervisor turns out to be vulnerable, a good analogy would be building a skyscraper on a foundation of quicksand. You don't need to be a structural engineer to figure out how that works out.

- **Configuration management on steroids.** When five, 10 or 100 virtual devices are on each physical server, a lot of strain is placed on the existing configuration management infrastructure. Patching 5,000 virtual images running different OSes is near impossible. Today's configuration management offerings must evolve to factor in the scalability (and efficiency) needed to operate in a virtualized world.

When five, 10 or 100 virtual devices are on each physical server, a lot of strain is placed on the existing configuration management infrastructure.

- **Business continuity is challenging.**

Many organizations run stand-by servers and replication technology, just in case. For mission-critical applications it's the right thing to do since downtime is quantifiably expensive. But if these critical applications are running in a virtual space, your business continuity plans need to evolve to factor that in.

In the category of “what’s old is now new again,” this is a solved problem. Solved by the mainframe operating systems of days gone by. Just because we’ve seen the problem before and can pick out an analogy, it doesn’t mean the problem is close to being solved in this new reality.

- **Software business models must change.** Lots of software, especially management software, is priced per managed device, but in a virtual world, what is a managed device? Does every created virtual image need to be paid for? Is a credit issued

when the image is removed? I don’t have those answers, but I can tell you the pricing status quo is not sufficient.

We’ll see new software pricing models emerge as a result of virtualization.

There may very well be early answers to some of these issues. I know there are a lot of smart folks figuring them out and bringing new products to market to solve problems.

But until the key issues are outlined, it’s important to work with the data center folks in your organization to figure out what the virtualization security plan should be for your environment. The road to virtualization will be fun—the “I am feeling a bit woozy and about to puke because I just got off of a roller coaster” type of fun.*

Mike Rothman is president and principal analyst of Security Incite, an industry analyst firm in Atlanta, and the author of *The Pragmatic CSO: 12 Steps to Being a Security Master*.

Until the key issues are outlined, it’s important to work with the data center folks in your organization to figure out what the virtualization security plan should be for your environment.

Sourcefire

The Impact of Virtualization on Network Security

What Works in Intrusion Detection and Prevention

Case Study: How Weill Cornell Medical College Gained Network Visibility with IDS/IPS

Technology Brief: Improving Network Security with Adaptive IPS

Third Brigade

Practical Tips for Unlocking Virtualization and Cloud Computing Cost Savings

Virtualization Security: A Coordinated Approach for Intrusion Detection And Prevention

Case Study: Protecting a VMware(r) Virtualized Data Center with Host Intrusion Defense

Tripwire

Forrester Research: Server Virtualization Security: 90% Process, 10% Technology

Update security practices and protect your organization's system.

Seven Practical Steps to Mitigate Virtualization Security Risks

7 practical steps that IT organizations to mitigate the security challenges of virtualization.

