5 Steps to a More Secure Virtual Infrastructure

Sponsored by Dell and Intel®

Datamation®
Executive Brief

There are many reasons to virtualize your infrastructure — consolidation, cost savings and agility to name a few. Improved security is usually not a driver for virtualization because for a long time, security was thought to be an endemic downside. While security is hardly a selling point for the technology, it is not an inherent weak spot either. Taking proper actions will result in virtual server environment secure enough for even the most mission-critical applications and sensitive data.

That said, virtual servers have very real security needs. Understanding how those needs differ from their physical counterparts is critical. For starters, both physical and virtual servers must be secured against malware, viruses and intrusion. But many organizations think primarily at the physical level and neglect to protect their virtual servers and hypervisors from the same woes.

Fortunately, as enterprises have gone from dipping a toe in the virtual waters to swimming with the sharks, IT organizations have heeded the advice of analyst firms and security experts before an oft-predicted major data breach related to virtualization has occurred. This focus on security has also coincided with the migration of data and applications of increased business importance to virtual servers.

In addition, as virtualization has become more commonplace, IT vendors all along the stack from processors to CPUs to firmware to operating systems and hypervisors, and all the way up to applications, have taken the technology into account. Security is a key part of these adaptations, which include firewalls, virus protection and high availability.

In the case of Dell's 12G PowerEdge servers, featuring the Intel® Xeon® Processor E5 Family, security begins at the processor level with Intel® Trusted Execution Technology (Intel TXT). Intel TXT provides hardware-based resistance to malicious software attacks that could occur before the virtual machine boots.

These efforts to bolster security are well received. An Infonetics Research Survey[1] of 105 North American companies in mid-2011 forecasted breakout spending in 2012, with respondent companies expecting to spend an average of 51 percent more on security for virtualized environments in 2012 than they did in 2010.

Still, security is not something to be complacent about. Just as you would not rely on the vendors you work with to spearhead your security efforts, so too must you lead the effort to keep your virtual infrastructure secure. If your virtual environment is not secure, the physical host they reside on will not be secure. One poorly secured virtual instance introduces a vulnerability that can impact your entire network.

As hyperbolic as that sounds, this is the heart of what differentiates a physical server security from virtual server security. ServerWatch, a website in the IT Business Edge Network,

cites four key reasons[2] why virtualized servers tend to be less secure than the physical machines they replace:

- Security considerations are not taken into account from the very beginning in many server virtualization projects
- All the virtualized workloads have the potential to be compromised by a single compromise of the virtualization layer
- Virtualized workloads that have different trust levels are often consolidated onto a single physical host without sufficient separation
- Many organizations lack adequate controls for administrative access to the hypervisor/virtual machine monitor layer and to administrative tools
- Fortunately, all of these reasons can be remedied. These five key steps will explain how.

1. Understand the Strengths and Weaknesses of a Virtual Infrastructure

Security is not a zero sum game, and a virtualized infrastructure does have some security advantages over an unvirtualized one. Understanding the fundamentals of these differences and planning your deployment accordingly will go a long way.

For starters, a virtualized environment is likely to have less hardware. This means less actual equipment to keep track of and fewer physical servers and networking elements to secure from outside threats. It also means fewer systems to worry about going down.

"Security is not a zero sum game, and a virtualized infrastructure does have some security advantages over an unvirtualized one. "

However, using virtualization to consolidate hardware means many more eggs in far fewer baskets, so it is all the more important that these systems be reliable. When a box goes down, it is not just one application that must fails, but multiple applications. Similarly, it is not just a single entry point on the network to be protected but multiple.

Each virtual server is a potential entry point on the network. From there, the attacker can mount an attack and take control of the hypervisor. This is referred to as *"VM escape."* Alternately, the hacker can move on from the virtual server of entry and compromise other virtual servers running on the same hardware. This is referred to as *"VM hopping."*

There is also the possibility of *"VM Theft,"* the ability to steal a virtual machine file electronically, and then mount it and run it elsewhere. This is the virtual equivalent of stealing a physical server — without having to enter an actual data center and remove a piece of computing equipment.

Hypervisor: The Achilles Heel of the Data Center

There is also the danger of the hypervisor being attacked directly. Hypervisors are a huge potential security weak spot, as they run at the most privileged ring level on a processor. This makes it difficult, if not impossible, for an OS running on the hypervisor to detect an attack such as *"hyperjacking,"* in which a hypervisor is subverted or a rogue hypervisor inserted. From there, a hacker can use his control of the hypervisor to control any virtual machine running on the physical server.

This possibility became even more real in May 2012 when VMware revealed[3] that confidential source code for its ESX hypervisor had been leaked and was posted to a code sharing site. (The 300MB of hypervisor source code were from 2003.) This left many wondering if the code contained in

the leak was still current, and therefore cause for concern, or obsolete and thus nothing to worry about.

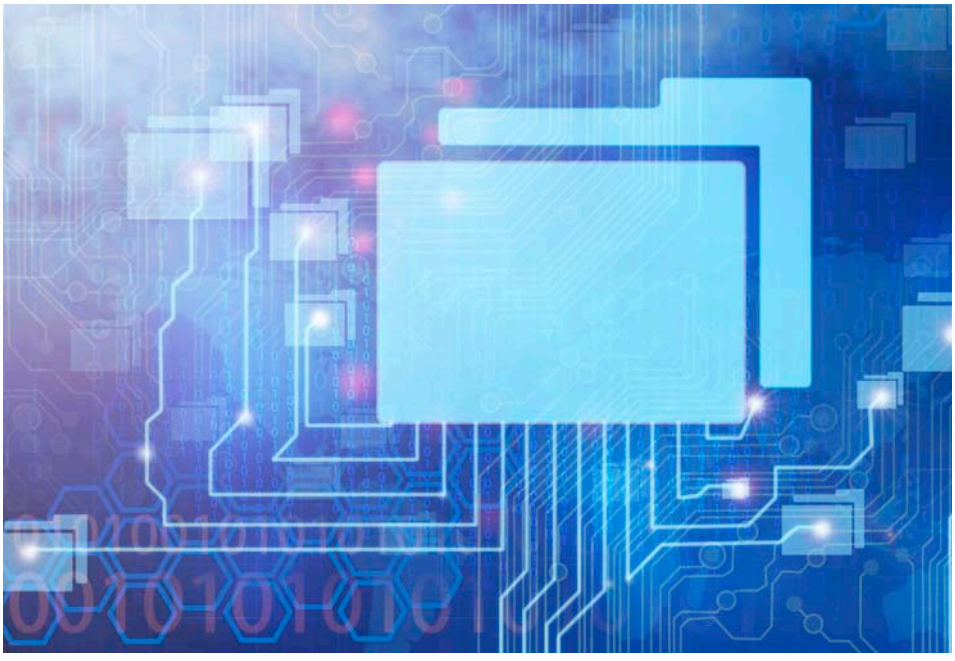
Whatever an enterprise's level of concern, this should be treated as a wakeup call. If your hypervisor layer is not patched to minimize vulnerabilities, and locked down to prevent exploits, you are exposing your entire network to a potential hack. Dell has found a variety of ways to protect the hypervisor. In addition to building in protection at the processor level in its 12G PowerEdge servers, featuring the Intel® Xeon® Processor E5 Family, Dell has taken steps toward mitigating potential downtime caused by hypervisor vulnerability by running redundant hypervisors on mirrored dual-secure digital cards.

One thing is clear about virtual server security, however. Each virtual server, whether guest or host, should get the same level of protection afforded to the physical server. This does not mean the security should be the same mechanics as that of the physical server — and do not get so busy securing your virtual servers that you forget to secure the boxes in which they sit — rather, it means that each virtual server should receive the well thought out protection historically given to the box in which it sits.

Although many of the conventional security offerings are not equipped to catch virtual server traffic that does not leave the physical server, this is changing. A variety of offerings have sprung up in the past few years that address the security needs to virtual servers. In addition, the hypervisor vendors have begun to address these issues within their offerings.

2. Security Starts at the Processor Level

Just as a chain is only as strong as its weakest link, a virtual server can't be any more secure than the box itself. Securing your virtual server starts with the physical hardware, and the reliability of the box is a big part of this. Security therefore begins at the processor level.



The major processor vendors have designed their most recent generation of processors with virtualization in mind. Intel® Trusted Execution Technology (TXT), for example, integrates with Intel® Active Management Technology and Intel® Virtualization Technology.

Intel®TXT delivers an isolated execution environment and associated sections of memory where operations can be conducted on sensitive data such that they are invisible to the rest of the system. It offers a sealed portion of storage where sensitive data, such as encryption keys, can be kept. This shields the data so it is not compromised in a malicious code attack. Intel® TXT also features attestation mechanisms to ensure the code is in fact executing in this protected environment and has correctly invoked Intel® TXT.

Together, these components help ensure the Intel® Xeon® Processor E5 Family is optimized for a virtual environment. This enables Dell's 12G PowerEdge servers to better facilitate software-level virtualization, minimizing the performance bottleneck and leading to greater uptime and reliability.

"Reducing virtual machine sprawl and its security consequences boils down to adopting the management practices that worked in the physical world. "

Reliability is a key tenet of security. A server that constantly crashes does not offer the business continuity that organizations require for data and applications access. It introduces greater risk for data to be hacked into, and it can result in damages and loss of the data, impacting the credibility of the business as a whole.

Today's CPUs are designed for to be virtualized. In some cases this involves the actual hardware, in other cases, systems vendors partner with the virtualization vendors and an optimized version of the virtualization technology is installed natively, sometimes on the bare metal server. This results in better performance as well as enhanced security.

In addition to securing your virtual servers, it is also important to ensure that your network is secure. Endpoints should be firewalled to protect the network from intrusion, viruses and malware. In addition, any data or virtual machines (and with that applications contained on them), traveling over the network should be encrypted.

3. Choose Software Carefully and Keep It Current and Secure

Whether you're evaluating firmware, a hypervisor, a firewall, an application or other software, be sure that its security limitations are acceptable for your organization.

Firewalls have undergone major changes in recent years. Many now go beyond packet and stateful filtering. Newer generation firewalls routinely include application layer filtering, perform deep packet inspection, and offer integrated intrusion protection systems. These capabilities can all help protect servers running virtual instances of critical applications against attacks. As with any IT equipment (and regardless of whether the firewall is software- or hardware-based), you need to be diligent with updates and applying patches. If you are not, a hacker might exploit the vulnerability the patch is intended to secure. And this would put your systems at risk.

Similarly, new patches and updates to all applications and hypervisors must be applied as soon as they are released. The challenge in a highly virtualized environment is to ensure all virtual instances of a vulnerable application are patched.

Because it is so easy to create and deploy virtual machines, there are often virtual instances created for test or other purposes that simply are not ever taken down. Over time, these unattended virtual machines may be left out of the normal patch process. Again, this could open your company up to risk if a hacker were to exploit the vulnerability of an abandoned virtual machine.

4. Keep a Close Eye on Your Virtual Servers

Some of virtualization's virtues — agility and flexibility, for example — can double as management vices, particularly when it comes to managing easily created virtual machines as they move through their life cycles.

Rapid growth of virtual machines can lead to a condition known as "virtual sprawl," in which lapses in the basic care of multiplying, unaccounted-for virtual instances can present major problems to a company.

Reducing virtual machine sprawl and its security consequences boils

down to adopting the management practices that worked in the physical world. You might begin by standardizing on well-planned golden images of certain applications' virtual instances. Conduct careful inventories to ensure all virtual machines are known. And adhere to timely patching regimes.

Just as with physical servers, virtual instances must be deployed and configured systematically to ensure security and reliability. And you should create master images where software can be installed and validated once.

Over time, it is likely that you will end up with many clones as virtual machine images are deployed, customized and updated. This adds to the management chores needed to secure your systems. The reason: The greater the variety of virtual machine images that must be updated, the more difficult and time-consuming the task. This is where having a current, easily accessible and comprehensive inventory of virtual machine images becomes critical. After all, software needs to be inventoried before it can be maintained and patched.

5. Follow Sound Practices and Policies

Finally, the human element of security must be addressed.

To begin, use the best practices from the physical world. Have policies in place that ensure virtual servers are configured correctly and set up securely. Set levels of access and management control so only authorized users can create, deploy, change or patch a virtual machine.

Be sure physical servers are secure. Use common sense. Grant data center access only to authorized staff. Control access with passkeys or some other form of protection. Lock racks with servers and storage devices that handle mission critical applications and data. Grant administrator level access to physical and virtual elements only to those who need it. And monitor for suspicious activities.

Develop guidelines and rules for virtual machine creation and deployment. Ensure the rules and policies are enforceable using systems and security management tools.

Bring It All Together

Securing a virtual infrastructure requires additional work over securing a physical server. Many of the issues, potential problems, management challenges and vulnerabilities are the same. As such, comparable approaches to those used with physical servers must be employed to ensure that your virtual assets are not compromised or your organization will be exposed to risk. Dell's 12G PowerEdge servers, featuring the Intel® Xeon® Processor E5 Family, go a long way toward meeting this challenge. ■

---

[1] http://www.infonetics.com/pr/2011/Virtualized-Infrastructure-Security-Survey-Highlights.asp

[2] http://www.serverwatch.com/trends/article.php/3895846/3-Ways-to-Secure-Your-Virtualized-Data-Center.htm

[3] http://www.eweek.com/c/a/Security/VMware-Code-Leak-Highlights-Security-Concerns-Around-Virtualization-739352/