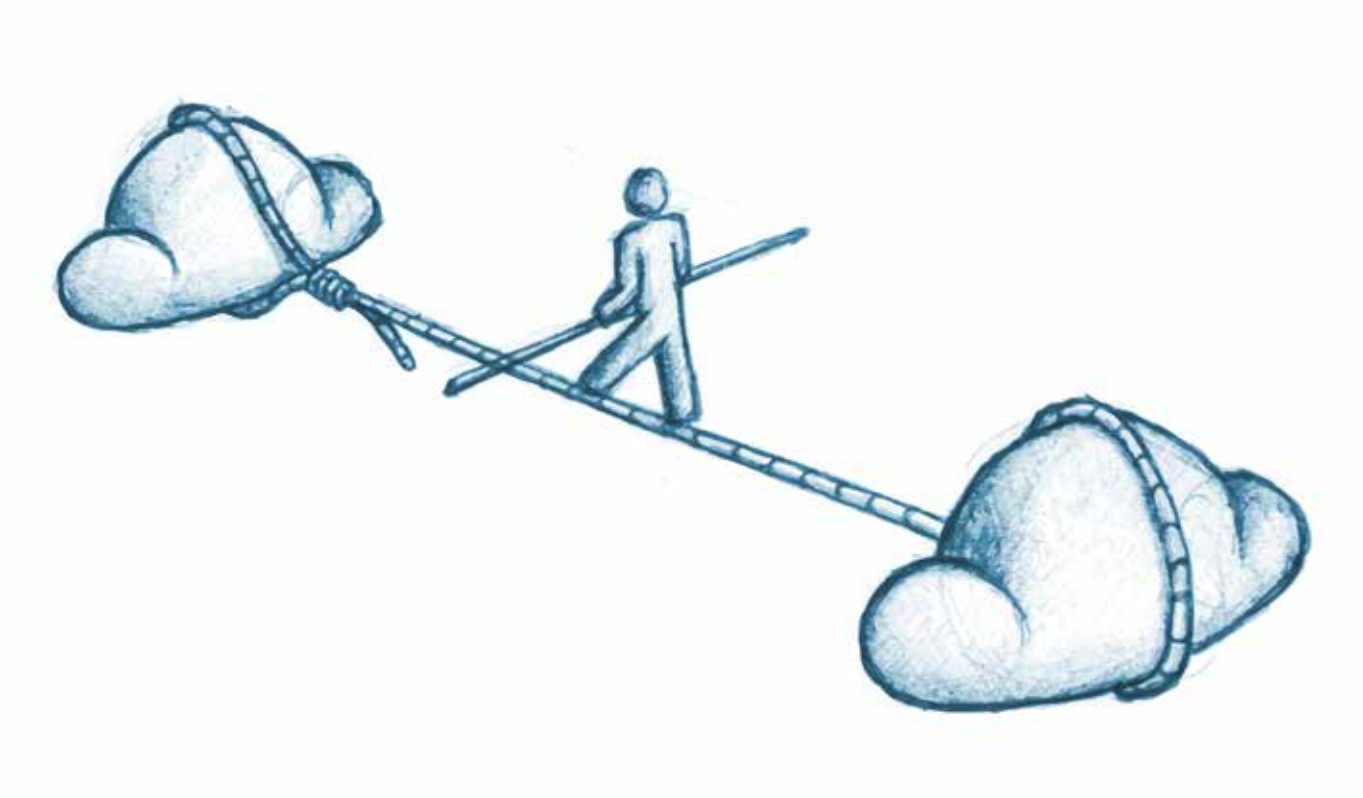
Bitdefender®

Evolve or Die: Security Adaptation in a Virtual World

Contents



Virtualization is ubiquitous

The use of x86 virtualization technology has been steadily growing since the early 2000's. In 2011, Veeam tracked virtualization adoption in the enterprise, finding that **39.4% of enterprise servers were virtual systems**, and that number likely continues to grow. In addition, **91.9% of enterprises had adopted some sort of virtualization technology**, indicating a huge shift toward virtualization overall.[1] According to a survey led by Cisco in 2013, the primary drivers of increased IT efficiency and cost savings lead the pack. The top benefit overall was **improved system scalability**, especially for new deployments.[2]

With these benefits comes a dark side, however. Virtualization technology implementation can easily lead to a lack of sound system inventory, incompatibilities with existing security technology, problems with file management and encryption, performance challenges with traditional antimalware solutions, and much more.

PCI Standards Council Scope the problem (back in 2011)

In June, 2011, the Payment Card Industry (PCI) Standards Council released a long awaited information supplement to the latest Data Security Standard (DSS) titled "PCI DSS Virtualization Guidelines". This guide, collaboratively produced by a group of security and compliance professionals, provides guidance on how security and compliance teams, particularly PCI assessors, should go about evaluating virtual infrastructures that fall within the scope of payment card compliance requirements. Two key sections of the document stand out - one details virtualization risks, the second addresses control recommendations. Both are relevant to the end goal of data protection in virtual environments. Several of the risks discussed in the PCI document include:[3]

- **Vulnerabilities in the Physical Environment Applying in a Virtual Environment:** "Physical threats also apply to virtual implementations; the most securely configured, well-contained logical partitions will still need adequate physical controls for protection of the hardware"
- **Increased Complexity of Virtualized Systems and Networks:** The addition of new technology layers such as virtual networking and appliances, as well as the hypervisor itself, creates potential misconfiguration issues. These, possibly coupled with virtualization vulnerabilities, can lead to significant risk potential.
- **Mixing VMs of Different Trust Level:** The guidance implies that mixing different data classification levels on a single hypervisor could lead to data loss or exposure, which should also logically apply to the storage of VM images.
- **Lack of Separation of Duties:** Lack of proper role definition and privilege assignment could lead to privileged access being widely granted for far more than just the virtualization management console.
- **Dormant Virtual Machines:** "VMs that are not active (dormant or no longer used) could still house sensitive data such as authentication credentials, encryption keys, or critical configuration information."
- **VM Images and Snapshots:** "...if images aren't secured and protected from modification, an attacker may gain access and insert vulnerabilities or malicious code into the image. The compromised image could then be deployed throughout the environment, resulting in a rapid compromise of multiple hosts."

The PCI Council goes on to recommend the following measures that apply specifically to data protection:

- **Evaluate risks associated with virtual technologies:** Assess all virtualization components and processes for risk just like any other technology.
- **Restrict physical access:** Ensure physical access to VMs and virtualization platforms is restricted and carefully monitored.
- **Implement defense in depth:** Security controls should be considered and potentially applied at all layers of technology implementation, including physical systems, hypervisor software, host and VM platforms, applications, and storage.
- **Enforce least privilege and separation of duties**

1 http://www.veeam.com/news/veeam-launches-v-index-to-measure-virtualization-penetration-rate.html

2 http://ciscomcon.com/sw/swchannel/registration/internet/registration.cfm?SWAPPID=91&RegPageID=461862&SWTHEMEID=12949

3 https://www.pcisecuritystandards.org/documents/Rth87Wp/Virtualization_InfoSupp_v2.pdf

- **Harden virtual machines and other components:** Hardening and lockdown should include virtual network interfaces and storage areas, and integrity of any cryptographic key-management operations should be verified.

The release of this guidance demonstrates just how critical and widespread virtualization had become as early as 2011. It's worth noting that this is still the only formal compliance guidance released on virtualization security to date!

Major security challenges abound

Over the last several years, many security challenges have been encountered by security teams. The following sections outline some of these challenges, and how they're being addressed.

Inventory management efforts frustrated by VM sprawl

Security teams are struggling with the reality that data centers are now simply collections of files hosted by hypervisors and stored in a Storage Area Network (SAN) or other storage environment, rather than physical systems. This leads to the first issue; inventory management.

In the SANS 20 Critical Controls project, lack of inventory control for hardware and software are consistently the top two issues on the list.4 Virtualization technology facilitates much more rapid creation and propagation of live systems and applications since it requires only the creation of another collection of files, not new hardware. An administrator can create a virtual machine in seconds, and have it running in a production environment in minutes. This can easily lead to an abundance of systems that have little to no lifecycle controls applied.

Data archival and destruction are also critical stages of the data lifecycle. In virtual environments, this means tracking entire virtual machines and the data accessed and stored for use in virtual environments. Virtual machines stored in their entirety on backup tapes or other media cannot be safely stored if the backup media is not encrypted. Another archival scenario involves decommissioning entire virtual machines and "retiring" them. Without proper governance of the virtual environment and its assets, there is a very good chance **that sensitive data may still be present in VM disk or memory-related files**, and some of these may be left behind inadvertently if proper precautions aren't taken. In other words, it's not quite as simple as dumping a physical server into the shredder.

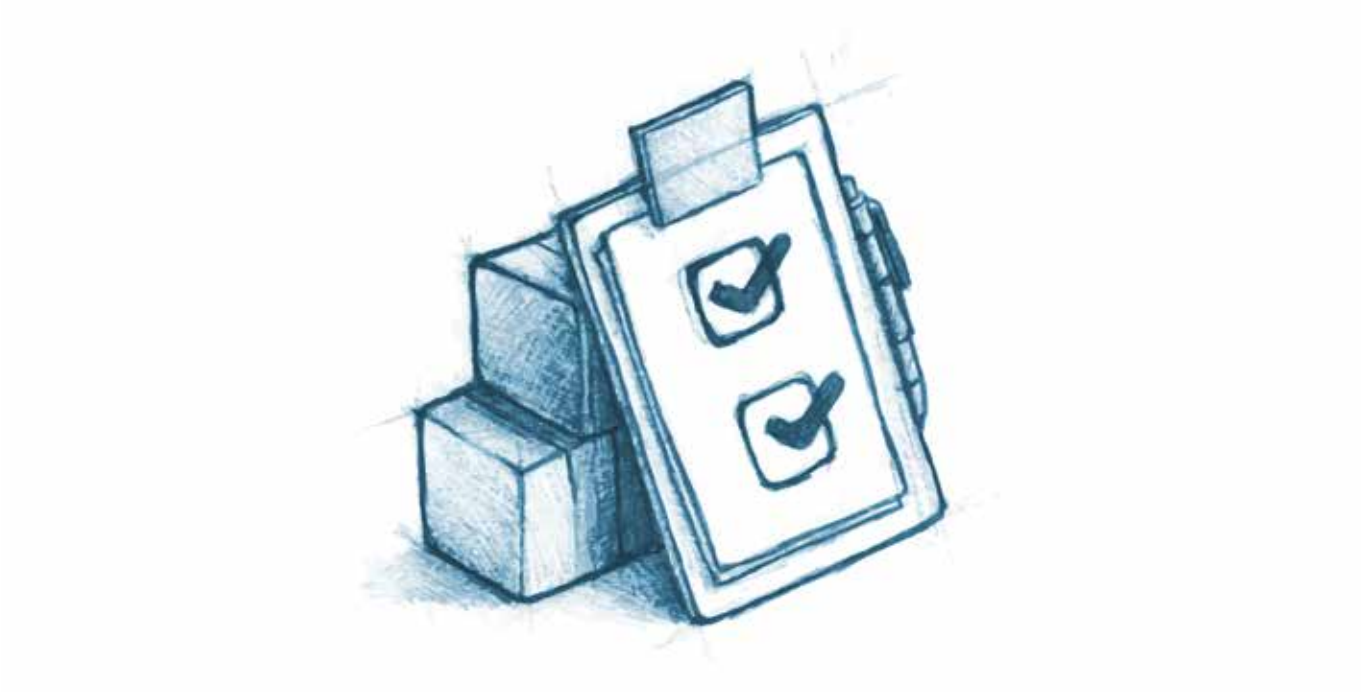
Since a virtual machine is simply a collection of files, they are an attractive target for attackers; stealing a machine is as easy as copying and pasting files.

For example, in VMware environments, a virtual machine (here called "VM") contains a number of specific files:

- VM.vmx: VM config file
- VM.vmdk: Virtual disk config file
- VM-flat.vmdk: Actual VM hard disk
- VM.nvram: VM's BIOS file
- VM*.log: VM log files
- VM.vswp: The VM Swap file
- VM.vmsn/vmsd: VM snapshot metadata
- VM0000001-delta.vmdk: Real-time snapshot write file
- VM-***.vmss: Suspended VM memory data

Not all of these exist at any given time; it depends on the state of the VM. All of these files are important, but **some, if unprotected, can contain sensitive data**. For example, the VM swap file (vswp) and VM suspension file (vmss) might contain passwords, crypto keys, or sensitive application data. An attacker could access and steal this data while these files are in storage. From a configuration standpoint, the .vmx file is the most critical, and a number of specific settings within this file can help to secure the VM, with controls ranging from logging parameters to interaction with the hypervisor system. These same file types exist in all major virtualization environments, including Citrix, Microsoft, KVM, and others.

4 http://www.sans.org/critical-security-controls



Currently, most organizations are struggling with **inventory management** for all assets, not just virtual machines and applications. However, new tools from the leading virtualization vendors (VMware, Microsoft, Citrix, etc.) and 3rd-party solutions focused on VM lifecycle management can help to some degree. Most VM sprawl scenarios are due to poor processes and lack of attention to lifecycle and security policies. For example, when a developer needs a new system for testing, there should be monitoring and restrictions limiting how long the VM can run before expiring. Making the creation of VMs a heavily automated process is, at most, only half of the struggle – and also something that exacerbates gaps in lifecycle and asset management controls.

Classification and encryption of mobile VMs

As organizations look to enhance their virtualization implementations by moving to a private or hybrid cloud, securing the mobility of virtual machines within the cloud must be addressed. Several key points to consider include:

- **Clear-text data in transit:** Using vMotion and similar VM migration techniques, a migration operation exposes VM memory in-transit, potentially allowing application data or file data to be accessed by anyone monitoring the network over which this data traverses.

- **Multi-tenancy:** VMs of differing classification levels hosted on the same hypervisor can potentially lead to sensitive data exposure if classification of systems is not enforced during data and VM migration. Many organizations do a poor job of data classification, and complex cloud environments could easily have numerous VM migration operations occurring simultaneously. For example, a VM hosting payment card data processing applications could be migrated to a hypervisor hosting much less sensitive systems, opening up a new avenue of exposure.

- **Data-at-rest security:** Data at rest generally means data that has been written to disk. Since a Virtual Machine is simply a collection of files, the entire VM can, and often should, be encrypted on disk if possible. The running VM image is not the only place where sensitive data can be stored. Snapshots, backup images, and memory images of suspended VMs can also contain information that should be protected.

To solve these security problems, many in the security community are looking for new security mechanisms where security policy and enforcement stays with the virtual machine as it travels.

To be effective, security policies need to be created and applied within a virtualization solution and be recognized by each hypervisor hosting the virtual machine as the virtual machine travels.

With encryption services, keys are generally involved. Keeping keys secret, from an attacker or from a cloud provider's administrators, adds a dimension that must be considered. There are numerous options emerging to help manage cloud encryption and security. New solutions from Hytrust, Ciphercloud, CloudLink, SafeNet, and even key management services from Porticor and others can help to simplify encryption both within the data center and when moving out into public cloud providers.

Amazon is one example of a cloud provider that is embracing the move to **customer-managed encryption**. They allow customers to manage their own keys to storage mounted in EC2 instances, dedicated S3 buckets, and even offer a dedicated encryption storage platform.

More virtualization vendors (and cloud providers) like VMware and Microsoft now recommend using encryption tools within VMs to secure data in private and public cloud environments. One of the big concerns operations teams have had with this approach is the potential impact on virtualization operations that encryption and decryption processes may cause.

Malware has long been virtualization aware

While malware originally didn't hesitate to infect VMs (Windows is Windows, as it were), things have become more nuanced. One of the more disturbing trends to occur since 2006 is the onset of VM-aware malware. These strains of bots, worms, rootkits, and others are capable of leveraging a number of techniques, both simple and complex, to determine whether they're running on a physical or virtual host. When the malware detects that it's within a virtual environment, it may refuse to run, or will behave differently than it would on a physical host.

Consider a piece of malware that targets end-user operating systems. Most end-users are not running their systems in virtual environments. On the other hand, most security companies run end-user operating systems in virtualized environments for the same reason that any enterprise leverages virtualization.

By acting benign, or not acting at all, malware authors hope to evade virtualization-powered automated analysis or honeypots (systems deployed such that they appear normal, but are actually heavily-monitored to better understand infection techniques).

The performance cost of antimalware

Aside from new **virtualization-focused threats**, simply implementing antimalware has been incredibly problematic in virtual environments.

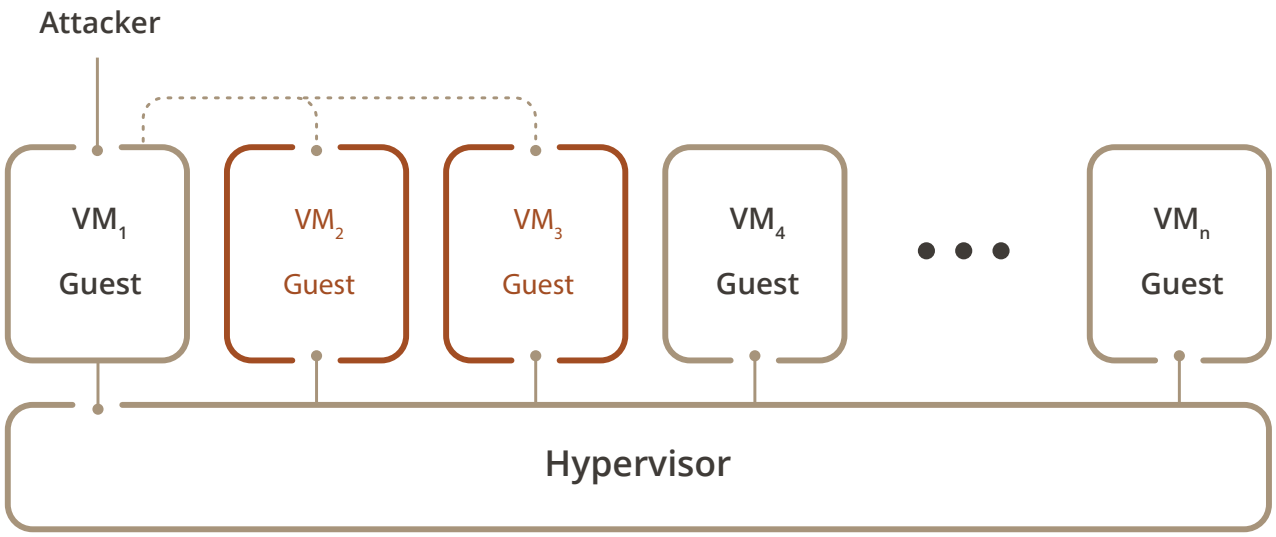
Administrators have been reluctant to install traditional antimalware tools within virtual computing environments due to fears that the required overhead will be too great. With a full antimalware agent, each virtual machine takes-up more CPU and memory than expected. This effect is multiplied as more virtual machines run on a host. While virtualization centralizes and deduplicates many of the resources used by virtual machines via the shared resources model, traditional antimalware duplicates resource consumption within each and every virtual machine.

This becomes especially **important when moving to hybrid and public clouds**. Having a more lightweight and flexible security agent can prevent major cost overruns that result from resource utilization, and licensing miss-match, in a cloud provider environment. Organizations should strive to understand if security tools can effectively operate in public cloud environments.

VM threat detection and intrusion monitoring, lack of visibility and control

There are many new types of threats within the virtual environment. Some threats are operational in nature, such as resource consumption and availability challenges or exposure of sensitive data via unencrypted channels.

Another of the most oft-discussed security issues with virtualization platforms is the notion of "VM Escape", where code runs within a VM and is able to "break out" onto the underlying hypervisor host.



This is a security professional's worst nightmare - trust zones are violated, access controls are circumvented, privileges are likely rendered useless, and the confidentiality and integrity of hypervisor hosts become suspect.

Most security professionals today believe that VM escape can happen. Since 2006, several tools have been released and discussed at conferences that allow data transfer between virtual machines, as well as virtual machines and the underlying host.

In **December 2005**, Tim Shelton reported a buffer overflow in the NAT networking capability of VMware Workstation, Player, ACE, and GSX Server. This vulnerability allowed an attacker to send malformed FTP commands from the guest to the host over the NAT networking channel, causing code execution on the underlying host.

Most of the VM escape flaws reported to date have been related to some sort of directory traversal attack. The first of these was reported by iDefense in **April 2007**, and described an issue with the Shared Folders functionality in VMware Workstation. Due to a problem with the way Workstation interpreted file names, a malicious user could write files from inside a Guest to the underlying host with the privileges of the user running VMware Workstation on the host. Intelguardians (now InGuardians) built on this research in their presentation on VM security issues during the SANSFIRE 2007 conference in Washington, DC. In **February of 2008**, researchers at Core Security (the company that makes the Core IMPACT penetration testing tools) released a flaw in certain versions of VMware Workstation, ACE, and Player that allows an attacker to locally or remotely exploit the Shared Folders functionality and read or write to any area of the underlying host OS.

The reason that these are not classified as a true "VM escape" is that code must be running on both the VM and the host for the tools to function properly. A true "VM escape" will be independent of code running on the host, allowing a purely guest-focused attack to break out of the VM and start running on the host. True escapes seem to be manifesting today, however. The exploit development team at VUPEN has successfully created two highly-publicized escape scenarios, one for the **Xen CVE-2012-0217**[5] flaw, and another in **mid-2014** for **VirtualBox**[6]. These allow full privileged access to host resources from within a VM running in the environment, as long as the attacker has user/process access to the VM.

In a paper published in **November of 2012**, researchers demonstrated a viable "side-channel" attack against VMs running on the same hypervisor platform.7 In the attack, one VM floods the local hardware cache, causing the target VM to have to overwrite some of this data with its own. Based on the data written, as well as the manner in which it is written, attackers can discern a variety of details about the target VM, including crypto keys in use for isolation and other encryption functions.

Access to VMs should be carefully controlled, both through the **assignment of roles and privileges for access and interaction**, as well as monitoring and auditing on storage infrastructure where VMs are located. This will depend on the type of storage you have in place, as well as monitoring capabilities with tools like log management and Security Information and Event Management (SIEM) platforms. The types of activities and actions organizations should pay attention to include:

5 http://www.vupen.com/blog/20120904.Advanced_Exploitation_of_Xen_Sysret_VM_Escape_CVE-2012-0217.php

6 http://www.vupen.com/blog/20140725.Advanced_Exploitation_VirtualBox_VM_Escape.php

7 http://phys.org/news/2012-11-vm-rude-awakening-virtualization.html

- Which users are accessing virtual machine files
- Where these users are coming from
- What type of access is employed, ranging from virtualization management console access to remote file share access using domain credentials
- When the access and/or actions took place

Generally, traditional network security tools are not instrumented for virtualization and are unable to monitor VM-VM or VM-Host communications. Many have been worried that VM to VM traffic could be carrying attacks and malware, with little or no chance of detecting it internally within the virtual infrastructure. For some time, this was actually the case, and the virtual network was viewed as somewhat of a "black box".

Fortunately, new tools have emerged, and intrusion detection can most definitely be accomplished by using one of several well-known methods today. VMware introduced the VMsafe (now NSX) API program that provides instrumentation to allow security monitoring vendors to properly allow their products to monitor traffic without deploying agents everywhere. In addition, the introduction of SPAN ports in Virtual Distributed Switches have allowed traditional, unaltered IDS and IPS solutions to be virtualized and used as-is with virtual switches from Microsoft, VMware, and Open vSwitch used by Citrix. Netflow support on virtual switches has also greatly increased the visibility into the network traffic within the virtual infrastructure, allowing network and security teams to more effectively build network behavioral baselines of traffic patterns in the virtual environment.

How our policies, processes, and technology will need to change to adapt

Virtualization and private clouds touch every part of the IT infrastructure - traditional server OS, applications and databases, storage, networking, as well as the desktop. Changing how those components interrelate can't help but change the policies that govern those relationships, as well as the processes used to manage the environment.

The lack of ability to track approved and unapproved changes over time is amplified in a virtual infrastructure. As virtual machines are continually provisioned and moved around the infrastructure, the diversity among the machines begins to grow, especially after going through patch cycles and interaction with end users. Over time, the virtual machine that was originally provisioned from an approved secure build drifts to a different state than the template. This drift introduces risk to the organization from a security exposure standpoint, while it also becomes harder to diagnose system failures. When you consider change control issues in combination with the next challenge, chain of custody, many organizations will have a problem demonstrating awareness and change management to auditors.

Organizations generally exhibit an inability to prove chain of custody over virtual machines as they change lifecycle stages from development to testing, and to production. Ideally, IT should be able to implement workflow and processes that track each VM and prove that the VM that was approved in one stage maintains integrity in the next stage. When organizations fail to provide this lifecycle management there is the risk of unapproved changes, or even worse, the inclusion of test data and mechanisms like debug logs and default accounts in the production version of the VM.

One overlooked area of security for a virtualization infrastructure is **isolation and access control related to the management network** that connects administrators to management servers and the management servers to the hypervisor platforms. This management network must be isolated, if at all possible (likely a significant shift in network architecture and management). Creating a carefully isolated management network will have a significant impact on the daily processes administrators use to access and control the environment. This model may also provide opportunities to implement more security "choke points" into the network with access controls and auditing in place.

Another key security principle to enact for virtualized infrastructure is **separation of duties**. In many organizations, virtualization is managed by existing Windows or other systems administrators. Although this may be convenient, there are numerous aspects to properly managing and administrating a virtualization environment that should ideally be left to the appropriate teams.

Most virtualization platforms allow for reasonably **granular role creation** and **privilege allocatio**n. Many administration teams will use a built-in Administrator role (or its equivalent), and assign most users to roles that allow access to virtual machines (VMs) for specific use-cases. Many privileges can be assigned, including explicit access to defined storage areas hosting virtual machine files, which can help to control unauthorized access to data. Proper planning, often a significant effort, is critical to ensure that user roles and data access privileges are appropriate for the organization.

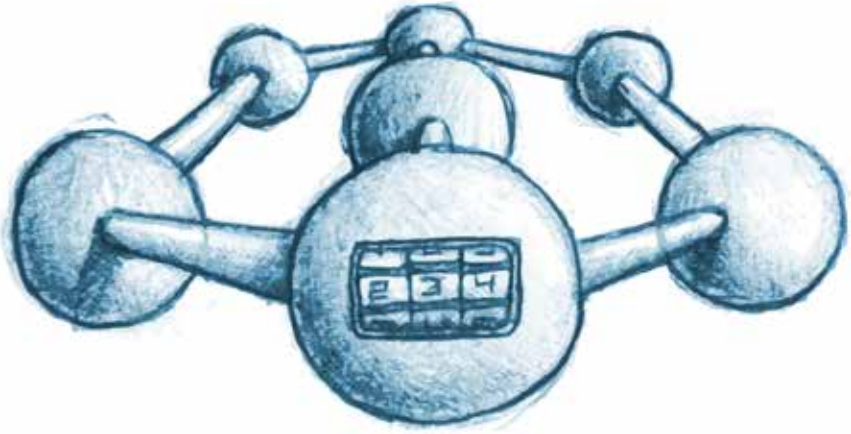
Lack of separation of duties is often coupled with excessive privilege use. Virtualization administrators are often granted full rights to all objects and components within the environment, which could easily lead to devastating results if a virtualization admin became a legitimate insider threat (benign or malicious). To properly get a handle on insider threats and misuse of systems and data in virtual environments, organizations should:

- **Define virtualization roles and privileges that align with the types of IT operations activities you would see performed in a physical environment.** Storage team members should be allowed to manage storage, network team members should be allowed to manage virtual networking components, etc. Virtualization team members should be allowed to configure and manage only the virtualization components (hypervisors, backup and redundancy tools, and resource pools across clusters) as needed. Another option is the use of privileged user management (PUM) tools to help control access rights by privileged users.

- **Enforce a strong authentication and access control.** If a separate management network has been established, require all access to management tools and systems to originate from a gateway or "jump box". Some organizations are also using password generation tools and access token mechanisms (sometimes called "password vaults") to provide short-term randomized passwords. This can help lock down authentication requirements, and also provide a solid audit trail for security teams to track.

- **Disable local access to both hypervisors and virtual machines.** Instead, require the use of a directory services environment like LDAP or Active Directory to centrally control users, groups, and access rights to systems wherever possible.

Finally, don't assume it won't happen. In July 2010, Jason Cornish, a member of the pharmaceutical firm Shionogi's IT operations team, deleted 88 virtual systems by illicitly accessing a hidden VMware vSphere client he had installed before leaving the company. He was caught, but not before causing approximately $800,000 in damages.[8]



Key areas of virtualization security

There are many different types of security concerns in virtual environments, primarily focused on virtual machines and their overall security. As a recap, here are some of the key areas to focus on, with some insights from the author based on many years consulting in large organizations:

- **Inventory management remains a huge issue.** Virtual machine sprawl continues to be a difficult problem to curb. Based on experience, 75% or more of large enterprises with virtualization technology in place do not have accurate inventory of virtual machines throughout the environment.

8 http://www.darkreading.com/vulnerabilities-and-threats/virtualization-security-your-biggest-risk-is-disgruntled-insider/d/d-id/1099988?

- **Encryption for virtual environments is still difficult to implement,** ranging from certificate management to encrypted virtual machine files. Most organizations are still using traditional encryption tools and key management systems that do not always work well in virtual machines, especially those that are propagated to public cloud environments.

- **OS-based security, especially antimalware tools,** can cripple virtual environments. 90% of organizations are still using traditional antivirus agents in virtual machine environments, which can consume significant amounts of resources. With newer types of tools available that reduce resource consumption, the time is now for organizations to revisit how they're protecting virtual machines from malware and other threats

- **Monitoring within a virtual environment is still proving to be a challenge.** Half of organizations using virtualization technology are not adequately logging events within the hypervisor and other components, and in many cases network monitoring is not on-par with traditional physical network monitoring and intrusion detection.

- **50-75% of organizations today are not designating roles within their virtual and cloud environments to properly implement separation of duties.** The vast majority are still using generic "administrator" roles that have far too many privileges, and not enough time is spent creating additional roles that minimize privilege and permissions. A virtualization administrator can undertake malicious actions within the virtual environment without properly segmented management networks, stringent authentication and access control methods, a robust audit trail, and limited privilege allocation.

As the **use of virtualization technology continues to grow**, so will the **need for proper security controls** - managed by **security** and **operations teams**. The risks discussed in the PCI Council's 2011 supplement are all still very real, and will likely remain as applicable in the foreseeable future. The good news is we have the tools and the knowledge to start improving security in the virtual environment, and the state of virtual security will continue to improve over time.

Bitdefender delivers security technology in more than 100 countries through a cutting-edge network of value-added alliances, distributors and reseller partners. Since 2001, Bitdefender has consistently produced market-leading technologies for businesses and consumers and is one of the top security providers in virtualization and cloud technologies. Bitdefender has matched its award-winning technologies with sales alliances and partnerships and has strengthened its global market position through strategic alliances with some of the world's leading virtualization and cloud technology providers.

FOR MORE INFORMATION VISIT: enterprise.bitdefender.com

BD-Business-May.14.2015-TK#: 70583