

A Practical Guide to Securing your Virtual Environment

John Reeman - CTO and Founder
VM Informer

www.vminformer.com

Executive Summary

Today we live in a dynamic world, everything around us is changing in terms of how we communicate, socialize and conduct business. The mobile phone I carry in my pocket today has more computing power than the first computer I learnt to program on at university and that was little more than a decade ago.

Virtualization is just one of the exciting new technologies that has been growing at a phenomenal rate over the last five years and is set to revolutionize the platforms we run our business on and how we conduct business now and in the future. Virtualization is one of those technologies that subtly creeps up on organizations slowly building its momentum that in the next 3-5 years there is no doubt in my mind that it will be a ubiquitous part of everything that we do.

Cloud Computing whether you believe in it or not is just another technology area that will utilize virtualization as a core component of its overall architecture. Organizations who are considering cloud computing in whatever form that might take now or in the future must seriously look at how they protect their assets and data. The boundaries that were once easy to define for organizations have been slowly eroding over the last decade and with the advent of the dynamic world that virtualization technology and cloud computing brings this has never been more true.

This document is about imparting knowledge and providing organizations or individuals with practical steps that can be taken when making the journey into the world of virtualization a much safer one.

The main focus of this document is about security and although virtualization itself is not inherently insecure there are like with anything pitfalls to avoid as well as myths to overcome.

Where do you start?

A Journey has to start somewhere. Typically virtualization starts because the organization wants to drive down costs, or adopt a stronger environmental approach. The business and perhaps external consultants start to tell you about this wonderful new technology called virtualization. The CEO of your organization then informs you that virtualization is a key strategic goal for the business and insists that it needs to be adopted within the next 6 months. At which point you put the phone down and perhaps panic!

However this story starts eventually virtualization in some form or another starts to creep into the organization. It may be low key at first, you deploy the technology in a development environment and then slowly over time migrate over to your production environment or you go for the big bang approach because the business demands it.

You may decide to start consolidating your server infrastructure from physical to virtual at first and this is typically the case. Some organizations are now starting to look at virtualizing their desktop infrastructure as well. The more adventurous are even doing this at the same time or before they virtualize all of their servers. Neither approach is right or wrong and every organization is different but prior experience has shown that security is very often given insufficient consideration in the planning and design phases.

It's often that not until virtualization projects are fully under way or even completed that someone may raise a hand and ask "what about security?". That's the moment when everyone shrugs their shoulders and looks at each other searching for an answer. Should you be surprised? Well not really, security and I generalize when I say this "is always the last thing organizations think about" and anyway the virtualization salesman said it was more secure and offered greater redundancy.

Such an important and strategic technological change that virtualization brings must embrace security at it's core. The consequences of not doing so will come back to haunt organizations for many years to come and could be potentially disastrous, or at least expensive to rectify.

Should your organization be concerned?

Obviously every organization should be concerned about IT Security whether the infrastructure be physical or virtual. The virtual environment however brings new challenges because of its dynamic nature and therefore security should be given more focus than it might perhaps have had in a physical environment.

Virtualization is not less secure it's just more dynamic, it has multi layers of management and its networking arguably is more secure, however the intricacies of virtualized networks are less understood. You also have an environment that at first glance has no definable boundaries, virtual machines can be moved from host to host depending on resource requirements and the shift of control and responsibility for which is now under the remit of completely different teams of people.

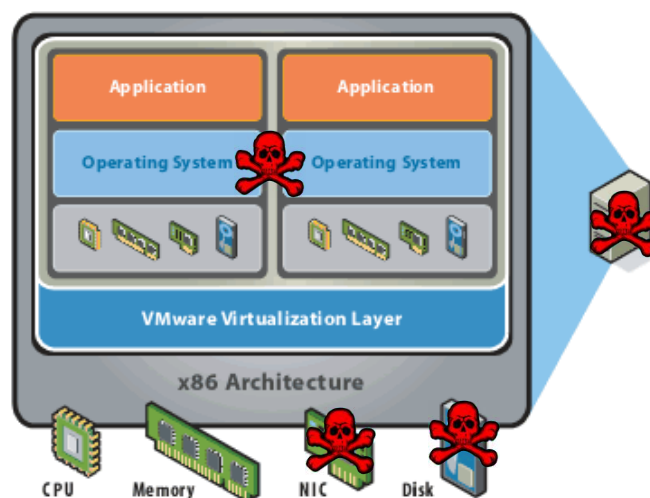
A team or perhaps an individual that does not have the necessary technical skills, be they network, security or storage now has the administration rights over this new ubiquitous environment and the potential to jeopardize the business at large.

Security needs to be at the top of your agenda when planning and designing your new virtual infrastructure.

The risks

The virtual environment is made up of a number of components that interact with each other. Each of these layers have associated risks which are outlined below:-

| | |
|------------------------------|---|
| Host to Guest compromise | The virtualization vendor host platform gets compromised and therefore the Virtual Machines that it supports (guests) can now be compromised. Such compromises could be anything from a simple misconfiguration to a 'root-kit' that circumvents the security controls of the host. |
| Guest to Host compromise | The Virtual Machine (Guest) becomes compromised which in turn, potentially compromises the security integrity of the host platform. |
| Guest to Guest infection | In much the same way as physical machines can be compromised through malware, viruses and alike so can virtual machines be compromised and then spread to all other machine types. |
| External to Host compromise | The Host platform becomes compromised through an external source. This could be through a management tier, through API's or as simple as failing to security harden the host itself. |
| External to Guest compromise | Systems outside of the virtual environment are able to compromise the security of the virtual machines and again this could happen for a variety of reasons. |



Practical Steps to Securing a VMware Infrastructure

Design and Architecture

It is a cliché, but when you buy a house the first thing anyone says to you is “Location, Location, Location”. When you design your Virtual Infrastructure or indeed any infrastructure, you should be thinking “Design, Design, Design”. Get it right from day one and those fundamental building blocks will serve you well.

What is good design? Is it “Best Practices” or just a copy of your current physical infrastructure as a virtual one? Have you simply taken the latest network design documents from your chosen virtualization platform vendor and diligently applied them?

The answer to all of those questions and many others is, not surprisingly it depends on what you have and want! You always need to look at your specific business requirements and then incorporate them as much as possible into your design. A best practice guideline is just that ‘a best practice’. It doesn’t mean that it is right or even appropriate for you. Gather as much information as you can particularly about your current physical infrastructure as it stands today. Whatever problems or issues you have in your current environment will only manifest themselves again in your virtual one possibly with far reaching consequences. So you do need to go through a thorough capacity planning exercise, as it may well be that not all of your physical servers, applications and specific network requirements can be met by virtualization today.

In this process stage it is important that you involve all parties, network teams, server teams, security teams as well as key business stake holders. Those people who don’t understand virtualization should be given an overview of how it works, and what it means so that they can be better informed and more willing to help rather than putting barriers in place.

In your overall design think about the functions and the importance of the servers you are virtualizing and where the data is being stored. It is important that you segregate machines and networks appropriately and isolate your management networks. This can be achieved within the virtualization technology itself augmented by more traditional physical methods like firewalls as required.

Host Platform

Your host platform is the work horse of your entire virtualization environment; it contains all of the networking, storage and virtual machine configuration settings and ultimately data that is potentially the life blood of your business.

Security of your host platform is therefore paramount, protect it as much as possible. It is critical that you reduce its attack surface and try and eliminate as many threats as you can.

Do not treat the host virtualization platform as you would any other general purpose operating system - it is fundamentally different. It has to be patched by the virtualization

vendor and not with normal OS Vendor patches. Avoid the common mistake of introducing security weaknesses by installing management agents that you may well install to manage physical systems but are entirely unsuitable for a virtualization host.

Lock down the configuration of this environment and work on the principle of least privilege. Monitor and record all access sessions to and from the host and make sure that all logs are stored in a remote repository such as a centralized log management solution.

If administrators do require access make sure they have individual user accounts and ensure that if they are elevating privileges to perform more sensitive operations that they are accountable and that all sessions are logged.

Virtual Machines

Treat the security of Virtual Machines in much the same way you would your physical machines. Deploy Anti-Virus, Anti-Spyware, Host Firewalls and IDS where appropriate.

There will also be virtualization vendor specific controls that can be utilized to improve the security of your virtual machines. For example disable copy and paste functions between the virtual machine and remote machines or the host itself in order to protect sensitive data. You should disable unnecessary device drivers like USB devices and as required lock down the guest so that only those users with privileged access can make changes.

Consider the level of security that you enforce on virtual machines according to how critical they are and also where they are deployed on the network. For example you may have a number of servers running critical applications that are deployed in your DMZ network and these clearly require a more stringent security regime than other less critical servers that are deployed on your internal network.

Make sure that you mandate the use of traditional management methods for virtual machines such as RDP or SMS, rather than solely using the virtualization management layer tools. These tools tend to add overhead and can provide less accountability and operationally can be dangerous if used by inexperienced virtualization administrators.

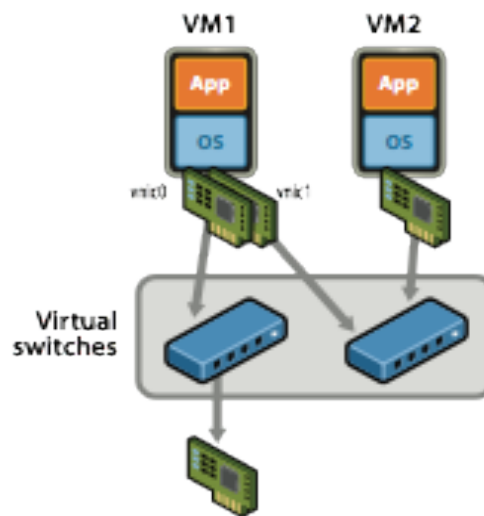
Network Considerations

Isolate your networks where possible according to function. If appropriate separate your production network traffic from your Management network traffic.

This can be achieved using VLAN's, separate virtual network switches and concepts such as Private VLANs (PVLANS) provided by platform vendors such as VMware through its vNetwork Distributed Switch (vDS) technology.

You can use PVLANS to isolate virtual machines even if they are on the same subnet, which as well as providing security benefits also gives you further flexibility and control.

Of course, you can continue to use more traditional methods like routing all traffic out through a single virtual machine on to the physical network, through a firewall and then back into the virtual environment. There are pro's and cons with all approaches if you use traditional methods then you will have the cost of doubling up on networking kit as well as security controls like firewall's.



Virtualization platform vendors have security controls built into the virtual switch fabric, things like protection against MAC address spoofing and forged transmits can all be enabled so make use of these features where appropriate.

Don't mix environments, sounds obvious but if you are planning on virtualizing your desktop as well as your server environment make sure they are completely isolated from each other. Unfortunately, in my experience this is a surprisingly common occurrence!

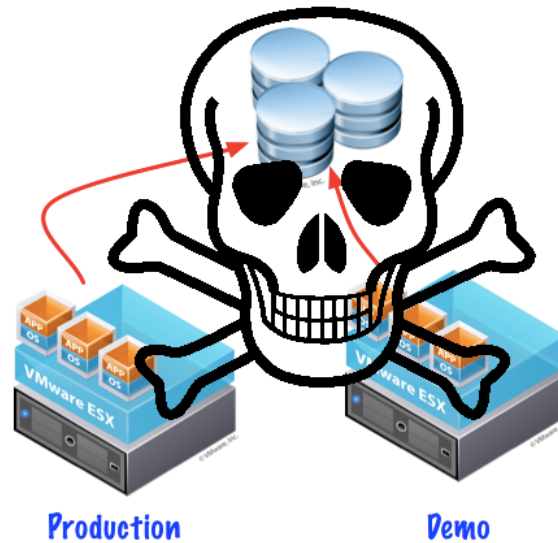
Traditional network teams often argue that inter VM traffic cannot be secured as it cannot be seen. This is a complete myth and can be counter argued by asking those same network teams how they currently secure servers attached to the same switch fabric in a physical environment today? The answer is that typically they don't. Except when the physical machine is in a DMZ and protected by an IPS of some kind but on a LAN most organizations provide full access between machines and networks.

Storage Considerations

Irrespective of your chosen storage platform you must think about the underlying storage requirements for each of your virtual machines and make data security a fundamental part of the design. Consider the business function that each virtual machine performs and try to segregate the data accordingly.

For example you may have a single VMware ESX host that combines both production and non-production virtual machines which can if designed correctly be separated on the underlying storage fabric.

If you handle any credit or charge card information you will more than likely be subject to the Payment Card Industry Standard (PCI) where there is a storage control requirement. If you are subject to other compliance regulations you will always need to prove that you are keeping satisfactory records of access to data.



Think about whether you are going to use thick provisioning or thin provisioning and what impact that will have. Don't rely on snapshots in the virtualization environment as a replacement for backup. Snapshots are a temporary measure to test a configuration not to be used as a general purpose backup process.

Consider the sensitivity of the data on your virtualized platform? Should it be encrypted? (note the PCI comment above). If it should be encrypted - is it appropriate to the environment? Finally and it seems obvious but where are backups stored for the virtualized platform? Often it is forgotten that these backups are not simply machines they contain sensitive data and should be secured with adequate access controls and encrypted if necessary. In order to safeguard the integrity and availability of the backups they should be kept separate from the virtual infrastructure and not stored on any virtual machines.

Assessment and Monitoring

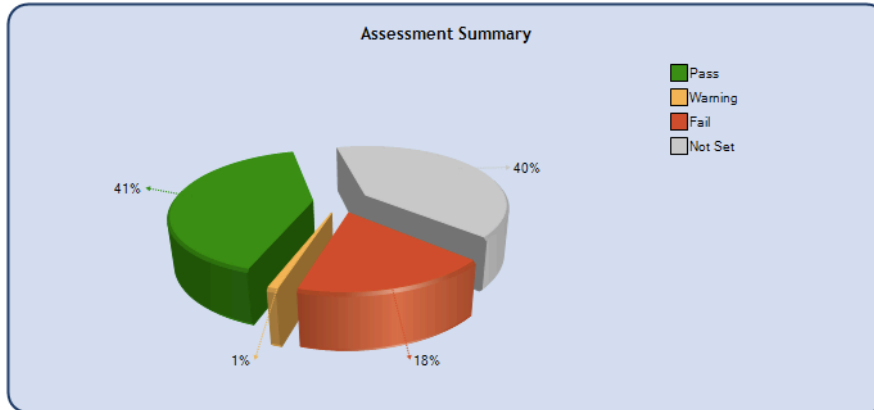
The virtual environment is a dynamic one, maybe some are less dynamic than others but none the less it is more dynamic than a physical one. Therefore the need for continual assessment and monitoring of that environment is paramount in order to maintain its efficiency, availability and security. This should become second nature and part of your organizations best practice to assess and monitor on a regular basis to maintain efficient operation. If you have compliance drivers you have no choice you have to audit regularly.

Make sure you are aware of all of the network ports that are enabled in your virtual network, particularly concerning management. VMware for example provides a firewall at the host level to restrict access and by default blocks all incoming and outgoing connections or at least that is what you would think. In reality, at the time of writing, this default firewall policy blocks everything apart from management connections of which there are quite a few. Some of these connections may not be required, and others should be locked down to specific networks or individuals.

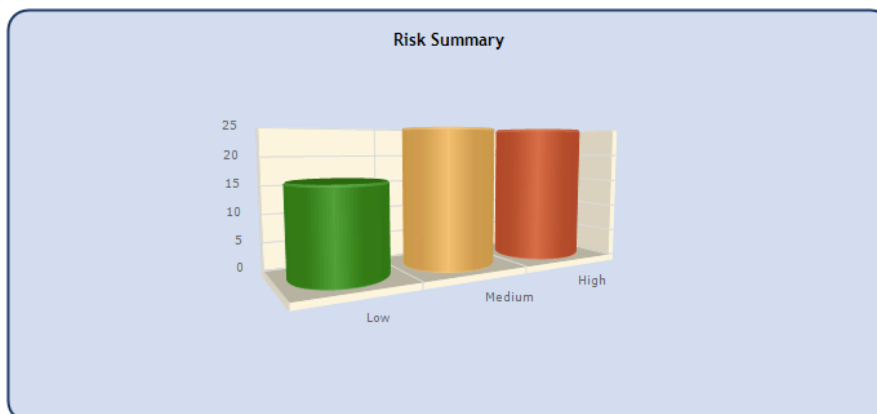
Whatever tools you do use for monitoring, you should use a combination that cover general health as well as security of your virtualized platform. Make sure they adequately perform the following functions:-

| | |
|----------------------|---|
| Complete Assessment | Look at the entire virtual environment and report back on all components, from the virtual machines, host platforms and management tiers. |
| Rapid Identification | Rapidly identify key security issue within the entire virtual infrastructure. |
| Classify | Having identified your key security issues classify these according to risk. e.g. High, Medium, Low |
| Business Context | Provide business context for your virtual machines by applying asset tags with meaningful names, e.g. production or development. |
| Report | Report on all findings in a clear and concise way for both Management, Security and Operation support teams to investigate. |
| Remediate | Provide feedback and remediation information that can be fed into an organizations change control management system. |

Assessment summary of the complete virtual environment



Classification of key security risks



Step by Step remediation guidance

| | |
|--|--|
| Rule Name: Disable copy and paste operations between guest os and remote console | |
| Description It is possible in a default configuration to copy and paste data between the Guest VM and Remote Console. This could potentially open a security risk in allowing sensitive data to pass from the guest to an external host. If this behaviour is not required then it should be turned off. | |
| Entity: isolation.tools.copy.disable isolation.tools.paste.disable isolation.tools.setGUIOptions.enable | Recommended Values: Disable Copy : TRUE Disable Paste: TRUE GUI Options: FALSE |
| Risk Level: High | |
| Remediation: 1. Login to the VC or ESX Host using the VI client 2. Select the specific VM you want to change the setting for 3. Edit the Machine settings 4. Select options then advanced 5. Then select general and then click the button configuration parameters 6. Enter the entity information and value as specified above. | |

Management and Operations

Virtualization platforms can be managed in a multitude of different ways. If not controlled and monitored these management paths can compromise security.

The virtualization vendors provide many tools to access and manage their platform architectures. VMware for example, have a management tier called vCenter or Virtual Center, this stores all of the configuration data about the virtual environment as well performing the day to day tasks like powering off and on virtual machines. These management tiers are typically accessed through client 32 applications as well as web interfaces and API's. Control is typically through user/password authentication mechanisms. In practice these may not be robust enough authentication mechanisms for your infrastructure, as often passwords are too weak or left at default settings.

Manage and control this environment according to the needs and requirements of the business. As with most security systems work on the principle of least privilege. VMware for example links into Microsoft Active Directory for its authentication process. The default account setup allows the Administrator group access - which may not be appropriate in anything but the smallest organizations, so check your entitlement carefully.

Management infrastructures that are not isolated could potentially leave themselves open to risk through man in the middle attacks, brute force password attacks, SQL injection and Cross Site Scripting Attacks (XSS) and the like.

Monolithic Security Controls

Many of the traditional security vendors are starting to port their particular technologies to the virtual environment but they are still along way off from seamlessly integrating these at the hypervisor level.

I would refer to these as first generation technology offerings. Security technology that simply takes a physical version of what exists today and turns it into a virtual machine should be carefully examined. Others will tell you that you will experience bottlenecks and contention for resources as this 'new' virtual security machine not only tries to protect your other virtual machines but also simultaneously competes for the same resources that your critical business assets require to run!

Consider whether you currently secure your servers or desktops in the physical network from each other, and if not do you wish to behave differently in a virtual network.

Security at the hypervisor level that incorporates aspects like anti-virus, firewalls and IDS/IPS will come. Such technologies are still being developed and at the time of writing in my opinion are generally not robust enough to deploy in a production environment. That doesn't mean without it that virtual environments are not secure, it all comes down to trust and confidence in the technology. Again at the time of writing it is worth noting that there are still no known security breaches of the hypervisor that exist in the wild today.

Conclusion

Today Virtualization security has no silver bullet, and the virtualization platform vendors are still maturing. The next 12-18 months will be an interesting and challenging time for both vendors and customers alike as we see more wider adoption of virtualization technologies as well as convergence in this space.

Many of the topics brought up may seem obvious. In my experience, and perhaps yours, it is often the obvious that is too readily overlooked and in a dynamic environment there is no room for complacency or ignorance as this is a place you or your organization cannot afford to be.

I hope that this document has given you something to think about in your journey to securing your virtual infrastructure. Hopefully it will have imparted some knowledge, points to revisit, and triggered a thought process to take back to your business. You will be better prepared and informed when asked the question “what about security” in your virtual environment.

If you would like to find out more then please come and visit us at www.vminformer.com where you can find further articles relating to virtualization security and download our free community edition assessment tool.