



How Virtualization Affects PCI DSS

Part 2: A Review of the Top 5 Issues

Authors:

William Hau

Vice President Professional Services
Foundstone Professional Services

Rudolph Araujo

Director
Foundstone Professional Services

Vivek Chudgar

Principal Consultant
Foundstone Professional Services

Roman Hustad

Principal Consultant
Foundstone Professional Services

Charu Chaubal

Technical Marketing Manager
VMware

Introduction

In the first paper of this series we mapped out the PCI requirements as they pertain to virtual infrastructure deployments and now aim to highlight what we believe to be the top five issues and concerns that PCI Qualified Security Assessors (QSA's) have about virtualization technology. For each of these we propose solutions that organizations can rely on to demonstrate compliance while deploying virtualization technology within their PCI environment. The contents of this paper have been put together based on our experience of doing many PCI assessments as well as virtualization infrastructure security reviews. However, it is important for the reader to understand that following the advice contained herein does not guarantee compliance. Ultimately you must work with your organization's acquirer and/or QSA to evaluate specific controls for compliance.

This paper assumes that readers are familiar with:

1. The twelve PCI DSS requirements and their sub-requirements
2. High-level security issues and concerns around information security
3. Key components of virtualization technology and general deployment scenarios

It is also important to note that while the concerns below are listed numerically, they are not ranked in any order, because the ranking depends on various aspects that in our experience are organization-specific and therefore not covered here.

Top 5 Concerns

Issue #1: Segregation of Systems

Requirement 2.2.1 states that you must "Implement only one primary function per server." This requirement is often misinterpreted to mean that virtualization is incompatible with PCI DSS compliance because by design, a hypervisor may have multiple virtual machines where each VM serves a different function. This interpretation can be refuted because the *intent* of the requirement has nothing to do with specific technologies, but is instead concerned with limiting the impact to cardholder data if a specific server function becomes vulnerable to attack. For example, a cardholder database server should not also be used for web surfing because this increases the number of attack vectors that can be used to compromise the system, and therefore increases the risk to the cardholder data. The PCI DSS itself demonstrates that the narrowest interpretation of requirement 2.2.1 is incorrect because it clearly allows shared hosting providers to host multiple customer environments on a single server in requirement 2.4 ("Shared hosting providers must protect each entity's hosted environment and cardholder data.") This is further clarified in Appendix A, which when examined makes it apparent that *appropriate controls* must be in place to mitigate the specific risks that come with shared hosting. Likewise, the use of virtualization technology is not a barrier to PCI DSS compliance as long as appropriate controls are in place to prevent one virtual system from increasing the risk to cardholder data on another virtual system.

So what are these appropriate controls and what are the risks that are introduced through virtualization, in relation to requirement 2.2.1? As you would expect the major concern is with inappropriate access to cardholder data through a compromise of guest-to-host or guest-to-guest isolation. For instance, a guest OS containing cardholder data might be compromised as a result of vulnerabilities existing in another guest OS running on the same hypervisor. While a hypervisor (or "host") should be explicitly designed to prevent such a compromise, it could be improperly configured during deployment such that the isolation between different virtual machine containers is not as strong as it could be. Examples of this include misconfiguring the virtual network to allow one VM to listen to all traffic on the host

A second risk related to requirement 2.2.1 and virtualization is the potential for direct compromise of the underlying host. To distinguish from the scenario presented above, consider the risk of a vulnerability in the hypervisor software itself. Exploiting such a vulnerability would provide an attacker with potential access to

all the guest machines, which represents a more dire situation. It is however critical to point out that known vulnerabilities in hypervisor software have been extremely rare. Of course the hypervisor is a PCI "system component" like any other, so the main controls to address this risk are already required by PCI DSS. Examples include prompt patching (6.1), restrictive access (7), proper user authentication (8.5), disabling unnecessary hypervisor services (2.2.2), and encryption of non-console administrative traffic (2.3). An example of restrictive access would be to limit all network-based remote access to the hypervisor, including all administrative access, to a small set of highly secure and trusted systems. This would typically involve the creation of a separate VLAN with strong access control mechanisms to host the management interface of the hypervisor (which is a separate IP address from those assigned to the guest OS). A best practice would be the implementation of stateful firewall rules to control access to this hypervisor-only VLAN and ensure that Guest OS network traffic is strictly prohibited.

One control to address this concern is to physically separate the hosting of VMs in the cardholder data environment (CDE) and those that are outside the cardholder data environment as shown in Figure 1.

Enforcing this control means it would not be possible for someone to compromise guest-to-host isolation of a non-CDE VM and then directly leverage the access into a compromise of a VM with cardholder data.

Alternatively, your organization may have a valid reason why VMs from the cardholder data environment must be deployed on the same hypervisor as VMs that are outside the CDE. A critical aspect of this configuration would be to put different classifications of VMs on different virtual networks. This can be accomplished either by using different virtual switches, as illustrated in Figure 2, or by using a single virtual switch with different VLANs.

Similarly, the datastores used to house the virtual machines would also be separated. This approach relies upon both the strength of isolation of the underlying virtualization layer as well as the correct configuration of it. Since the PCI Council offers no guidance on this

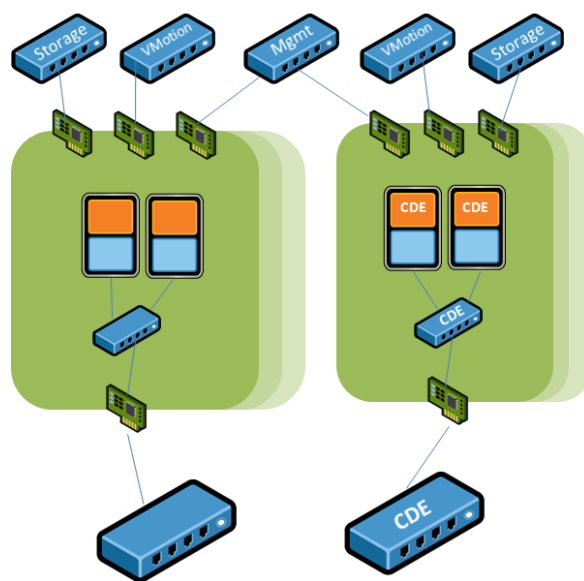


Figure 1: Physical Separation of the Cardholder Data Environment (CDE)

thus far, the compliance judgment as to whether CDE and non-CDE VMs can exist on the same physical host will need to be made on a case-by-case basis by a PCI QSA and/or the acquirer. They would need to

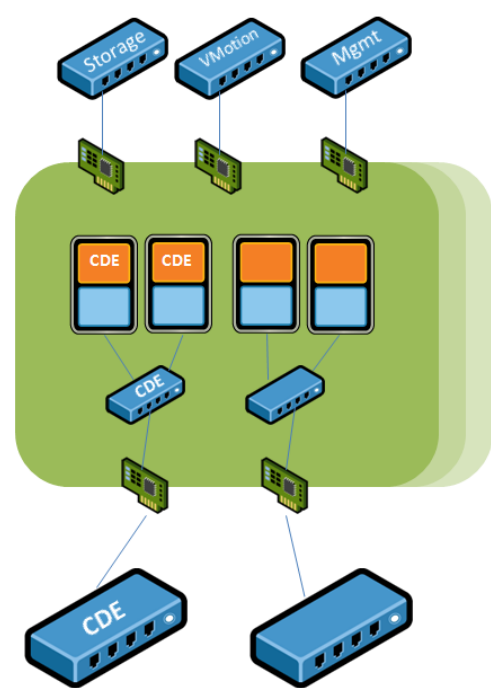


Figure 2: Logical Separation of the Cardholder Data Environment (CDE)

determine whether the configuration meets the requirement directly or should be treated as a compensating control. The PCI risk assessment results (requirement 12.1.2) will likely be a significant factor in this determination.

Another specific risk is that some virtualization platforms break guest-to-host or guest-to-guest isolation intentionally to allow optional features such as drag-and-drop, clipboard sharing and the like. Disabling such features should be an absolute requirement to adequately reduce the risk of a break in isolation. And finally, hypervisor configuration standards should incorporate the detailed security checklists provided by your virtualization software provider to ensure a thorough lockdown (see Appendix for links). In general, bare-metal virtualization is preferred over hosted virtualization technologies for virtualization of servers in the CDE. The former make much stronger guarantees of isolation and come in a default lockdown state. Additionally, this restriction should apply both to production as well as staging or test environments.

One other scenario to consider is hosting providers that offer virtual machines for all or part of a customer's CDE. Customers who make use of these services must themselves configure the virtual machines to be PCI compliant, and furthermore must manage the relationship with the hosting provider in accordance with PCI DSS requirement 12.8. Shared hosting providers involved in such a relationship must comply with the full PCI DSS on their own, including requirement 2.4 and Appendix A. All the advice presented in this whitepaper applies to such providers, who should also consider a third-party virtual infrastructure security assessment.

Issue #2: Segregation of Networks

An important aspect of network segregation is the isolation of all management / control networks. These are defined as the networks on which administrative (i.e. not production) interfaces are situated. Since the easiest way to compromise a system is simply to configure it to bypass security measures, it is critical that these administrative interfaces are protected by multiple layers. For VMware VI3, make sure that the network which has the service console and Virtual Center is isolated from other networks especially the guest network and other user networks. It should be firewalled and accessible only to authorized administrators. You should use a VPN or other access control methods to restrict access to this network. The same is true for any other non-production networks, e.g. those used for IP-based storage, VMotion, and other auxiliary services such as DNS, AD, and system monitoring. An option for enabling usage of management clients is to create "jump boxes" within the management network on which the management clients run. Access to these jump boxes is limited, e.g. by firewalls, only to remote display protocols, so that interaction with outside networks is as minimal as possible.

To aid with the separation of networks and host isolation, ESX 3.5 for instance, includes a firewall that protects the Service Console management interface. This provides an important layer of defense, and should be utilized appropriately. The only ports that should be open are those which are needed by essential services running in the Service Console. These services themselves should be kept to a minimum; you should avoid running any additional agents in the Service Console unless they are deemed required by your IT policies.

The firewall included with ESX does not provide any protection for virtual machines or virtual networks. For the virtual machines, you need to use a separate firewall, either physical or virtual. A physical firewall can be used to block traffic between physical switches that are connected to individual virtual switches. Since there is no mechanism for two virtual switches on the same host to exchange packets, they are isolated from each other. In this case, the only way that virtual machines on two virtual switches can share information is via the external (physical) network. Alternatively, a virtual firewall, which consists of a special-purpose virtual machine that bridges two or more virtual networks, can be employed to mediate traffic between two virtual switches. In this case, the inherent isolation between virtual switches is deliberately broken via this virtual firewall. You need to ensure that it is configured properly to avoid letting too much (or too little) network traffic through.

A frequently asked question is whether a virtual firewall can be used as a control to meet requirement 1.1.3, which states there must be a "firewall at each Internet connection and between any DMZ and the internal network zone." It is important to note that the PCI DSS is not prescriptive with certain technologies; instead it is prescriptive for certain functions that the technology must provide. Hardware firewalls are not mentioned specifically anywhere in the standard, but there are a number of clarifying statements in requirement 1 as to which functions a firewall must provide and how they must be configured. Specifically, the standard states that "a firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria." Internet-facing firewalls must additionally support configuration of a DMZ (1.3.1), restriction of outbound traffic (1.3.3 & 1.3.5), stateful packet inspection (1.3.6), and a form of IP masquerading such as NAT and PAT (1.3.8). If a virtual firewall can perform these functions and is configured correctly to meet the other sub-requirements of requirement 1, then it should be considered PCI DSS compliant.

Finally, another avenue for inappropriate access to cardholder data worth discussing is the misconfiguration of virtual networks. Without adequate controls or oversight, it is possible to place VMs in the cardholder data environment (CDE) on the same subnet as VMs outside the CDE, thus bypassing all intended network security barriers. This is especially critical when CDE and non-CDE VMs are combined on the same host. The main controls to address this risk are as follows:

- Restrict all privileges which allow arbitrary virtual machine network assignment. For example, in VMware VI3, do not allow direct virtual machine creation or reconfiguration by anyone except the most trusted administrators, but instead only allow virtual machine deployment via virtual machine templates, which embeds the network assignment in its specification. Furthermore, all such changes and deployments must be made after following change control procedures that have been documented and enforced
- Monitor virtual networks in the CDE for any virtual machine assignment, so that any unauthorized virtual machine on a network can be immediately detected and responded to.

Issue #3: Protection of Virtual Media

PCI DSS Requirements 9.6 – 9.10 pertain to media which might contain cardholder data. Just like in a non-virtualized environment, it is important to ensure that any databases that store such data are strongly access controlled, encrypted and protected as appropriate. These requirements cover both protection of this information in production but also on backup and archival devices. None of this is unique or different in virtualization systems. However, with virtualization, it is important to bear in mind that virtual machines themselves are ultimately files stored on a file system or on backup tapes. These files are used to maintain everything from the virtual hard disks to the RAM for the virtual machines and their BIOS settings. As one would expect unfettered access to these key files would allow for information disclosure (potentially credit card information in our context) as well as unauthorized modifications to the CDE itself.

It is therefore critical from a data protection perspective that these be protected and that access to them be controlled. This can be done through traditional access control mechanisms including the segregation of SAN devices and their management networks. Further, a number of virtualization technologies support the use of encrypted artifacts such as virtual hard disks. Organizations must consider deploying such technologies especially when using hosted virtualization platforms. Finally, it is also important to consider the security of backups of virtual machines themselves. Again such backup media must be protected through encryption and access control as appropriate. This applies not just for the virtual hard disks but also for the RAM and the virtual management components. With the ability to construct snapshots and clones this problem can quickly expand to a large number of virtual machines. Hence, policies must be set in place to ensure minimal VM sprawl. For instance, creation of templates, clones and snapshots from VMs containing cardholder data may be disallowed entirely.

Issue #4: Logging and Auditing

PCI DSS requirement 10.2 mandates that an organization must "implement automated audit trails for all system components." As with access control, the software tools provided by virtualization vendors are generally adequate to meet this requirement, but the audit configuration, management, and ongoing log monitoring of the virtualized environment, if incorrectly implemented, can be a significant burden in an operational environment without serving the intended purpose. Auditing and logging can consume noticeable computational resources such as CPU cycles, memory, disk space and network bandwidth. However, many organizations fail to make provisions for these computational overheads while designing the virtualization infrastructure. Instead, auditing/logging is turned on as an afterthought once the virtualization infrastructure goes live. Often organizations that adopt such a casual approach to auditing/logging eventually find that their virtualization architecture is unable to effectively handle the computational overheads of this critical security and compliance function. They are faced with the tough and mostly expensive choice of retrofitting more capacity into their existing virtualization architecture or turning off logging/auditing and then dealing with the risk of not meeting the PCI requirements. An ideal solution to avoid such a situation would be to determine upfront the auditing/logging settings necessary for PCI compliance and configure the test environment per these settings. This will ensure that any additional resource requirements related to auditing/logging are clearly identified during the capacity planning phase and the virtualized infrastructure deployed in production is able to meet the related PCI requirements without causing performance issues or bottlenecks.

A related issue that arises with the use of virtualization in the cardholder data environment is the challenge of forensic examination, which is one of the main reasons for keeping audit trails in the first place. For example, when a virtual machine is compromised should the host system be quarantined as well? Another issue arises with the seizure of evidence: if a crime is committed on a virtual machine, law enforcement investigators may very well confiscate the entire host and all the other VMs on that host. Your organization should already have an incident response plan per PCI DSS requirement 12.9, but may not have considered these issues that are unique to the virtualized environment.

Most bare-metal virtualization vendors provide centralized management capabilities that allow remote administration of hypervisors using mature administrative interfaces that in turn depend on production-grade relational databases as the backend data repository to store the hypervisor configuration settings and

administrative privileges. To ensure compliance with auditing and logging requirements of the PCI DSS, controls must be put in place that turn on logging on these databases as well as any other logging capabilities provided by the hypervisor vendor. Additional controls that can be considered are hosting these central management systems on their own dedicated infrastructure and segmenting them from the rest of the network. Further, most virtualization providers also support the ability to write logs to a remote, hardened log server. This is a capability that should be invested in to help in achieving compliance with the PCI DSS. Unfortunately however, there is not a single standard for such remote logging. Most providers however do support technologies such as SNMP and WMI which in turn allow for these components to be integrated with existing log management solutions that you might already have deployed within your environment. As an example, the table below provides a non-exhaustive list of some of the events that can be logged and monitored in a VMware based virtual environment:

System	Source
ESX	Log file found in Service Console: VMware-specific events: /var/log/vmware/hostd.log System events: /var/log/messages
ESXi	Log file available via standard interface (VI CLI, PowerShell, VI API) VMware-specific and system events: 'messages'
Virtual Center	Events table (exposed via VI API or specially-created DB View)

VMware VI3 includes detailed logging of all events that occur through Virtual Center in a comprehensive events database. Local log files on ESX also have entries for all events on that host. These serve as a secondary record of events which occur through Virtual Center, as well as the only audit log for actions initiated directly on the ESX host (i.e., not through Virtual Center). Both of these should be used as sources for an audit trail. The table above for instance, shows a list of sources for event records in a VMware Infrastructure 3 deployment while the table below shows examples of the types of events that can and should be tracked.

Event Category	Example Events
Authentication & Authorization	<ul style="list-style-type: none"> • Successful login: who and when • Unsuccessful login: who, when, frequency of attempts • Access Controls: user/group granted a new role, new role created, existing role modified

Networking	<ul style="list-style-type: none">• VM added to a monitored network (portgroup)• VM network assignment changed (to different portgroup)• VM bridging two networks
Datastore	<ul style="list-style-type: none">• VM added to monitored datastore• Storage VMotion of monitored VM

Log files from individual ESX hosts can be sent to a secure remote syslog server, thus reducing the possibility of tampering. Add virtualization logs to the existing log management tools and process so as to ensure that these are audited on a regular basis just like other logs within your environment. In order to prevent tampering with audit records, closely restrict access to any database where events are recorded, such as the Virtual Center database. Configuration files for both ESX and Virtual Center can be collected and monitored on a regular basis and monitored for unauthorized changes. Tools are available from various vendors which provide file-integrity monitoring capabilities, and should be used whenever appropriate.

Issue #5: Asset & Change Control

The relative ease with which a virtual machine can be deployed, copied, stored, and transmitted is both a blessing and a curse. PCI DSS requirements that were straightforward in a physical environment, such as patching (6.1) and change control (6.4), may require additional processes and/or technology to ensure compliance in the virtual environment. For example, when an old or new VM is "turned on" in the cardholder data environment, it must comply with the PCI DSS immediately. The organization must therefore tightly control deployment of VMs and should perform manual audits of running VMs to ensure that "rogues" are not deployed outside the change control process. With regard to patching, VM template images may quickly become out of date so the use of products that can perform offline patching and anti-virus updates is essential. Features such as "snapshot" are quick and handy but a "rollback" may return a machine to an unpatched and non-compliant state and therefore the ability to execute such functions must be tightly controlled. This can typically be achieved through the fine grained access control definitions provided within your virtual management components. Another concern is the access control of virtual machine image files, especially those containing cardholder data. If someone can manage to copy a virtual machine image, they can simply wait until a new privilege escalation vulnerability is announced for the platform and then boot it up, elevate privilege, and steal the cardholder data. Again, virtual management software packages can be used to provide audit controls around the storage and deployment of images and these controls should be enabled. As mentioned above, it is also vital to protect all media that contains virtual machine artifacts. Several solutions exist for monitoring and remediating offline VMs and templates for operating system patches and updates. VMware Update Manager is one such a solution, enabling administrators to create baselines which define minimum patch levels for the operating system and critical applications. It can then monitor both online and offline virtual machines as well as templates for compliance with these baselines. Administrators can then use it to keep those images up to date. VMware Update Manager also provides a comprehensive way to keep the ESX host software itself monitored and up to date. Similarly, McAfee's TOPS for Virtualization suite also allows for performing scanning and updates of offline VMs from an anti-virus and anti-malware perspective.

Conclusion

Achieving PCI compliance in a virtualized environment is very much attainable. It simply requires you to understand the intent of each of the requirements and how these are impacted by virtualization (see the earlier whitepaper in this series). As you go through this process you will quickly find, in most organizations, that each of the compliance challenges presented by virtualization can be mitigated or worked around in a reasonable and practical manner.

About The Authors

William (Bill) Hau, Vice President, Foundstone Professional Services

As vice president, Bill is responsible for running and growing the Foundstone Professional Services consulting business. Bill also has extensive experience in Information Security across all industry sectors from Managing Security for Global organizations through to performing technical assessments for Fortune 500 and government clients. Bill is a PCI Qualified Security Assessor and holds the standard information security professional certifications as well as a MSC in Information Security. He has presented to many audiences on the matter of Information Security and proactively contributed to the startup of the Open Web Application Security Project (OWASP) project.

Rudolph Araujo, Director, Foundstone Professional Services

Rudolph is responsible for creating and delivering the virtualization, threat modeling and security code review service lines. He is also responsible for content creation and training delivery for Foundstone's Building Secure Software and Writing Secure Code – ASP.NET and C++ classes. Rudolph's code review experience is varied and includes among others custom operating system kernels, hardware virtualization layers, device drivers and user-mode standalone, client / server and web applications. Rudolph also helped create the industry's first virtual infrastructure security assessment and has delivered this across a wide variety of clients and industries. He is a columnist and speaker at events such as Microsoft TechEd and SD-West.

Vivek Chudgar, Principal Consultant, Foundstone Professional Services

Vivek is a PCI Qualified Security Assessor and responsible for developing and managing the risk and compliance management service lines, including PCI Compliance. Vivek has extensive knowledge and experience in strategic consulting services such as information security program development and budgeting, risk assessments, governance reviews, PCI and HIPAA compliance assessments, ISO 27001 policy development and compliance reviews. Vivek also routinely delivers tactical consulting services such as firewall and network architecture reviews, database security audits, Windows AD security audits, and penetration testing. He also helped create the industry's first virtual infrastructure policy assessment and has delivered this across a wide variety of clients and industries. Vivek is a frequent speaker on security topics including PCI at events for groups interested in security.

Roman Hustad, Principal Consultant, Foundstone Professional Services

Roman is a PCI Qualified Security Assessor and is responsible for secure software development life cycle design and implementation, security code review, software architecture and design reviews, and threat modeling for Fortune 500 and government clients. He is the Lead Instructor for the Foundstone course *Writing Secure Code - Java* and also created the free computer-based training *PCI DSS Compliance for Developers*. Roman has over 15 years of IT experience and has been on both sides of the PCI compliance issue – as a QSA and as a payment application developer.

Charu Chaubal, Technical Marketing Manager, VMware

Charu Chaubal is a Senior Architect in Technical Marketing at VMware, where he is chartered with enabling customer adoption and driving key partnerships for datacenter virtualization. His areas of expertise include virtualization security, compliance and infrastructure management, and he has been responsible for defining and delivering VMware's prescriptive guidance on security hardening and operations. Previously, he worked at Sun Microsystems, where he had over 7 years experience with designing and developing distributed resource management and grid infrastructure software solutions. He holds several patents in the fields of datacenter automation and numerical price optimization. Charu received a Bachelor of Science in Engineering from the University of Pennsylvania, and a Ph.D. from the University of California at Santa Barbara, where he studied theoretical models of complex fluids.

About Foundstone Professional Services

Foundstone® Professional Services, a division of McAfee Inc., offers expert services and education to help organizations continuously and measurably protect their most important assets from the most critical threats. Through a strategic approach to security, Foundstone identifies and implements the right balance of technology, people, and process to manage digital risk and leverage security investments more effectively. The company's professional services team consists of recognized security experts and authors with broad security experience with multinational corporations, the public sector, and the US military.

About VMware

VMware (NYSE: VMW) is the global leader in virtualization solutions from the desktop to the data center. Customers of all sizes rely on VMware to reduce capital and operating expenses, ensure business continuity, strengthen security and go green. With 2007 revenues of \$1.33 billion, more than 120,000 customers and more than 20,000 partners, VMware is one of the fastest-growing public software companies. Headquartered in Palo Alto, California, VMware is majority-owned by EMC Corporation (NYSE: EMC). For more information, visit www.vmware.com.

Glossary

Term	Explanation	Example Products
"Platform Virtualization"	A layer of abstraction between the operating system and the hardware that allows for the emulation of hardware resources. Contrast this term with "resource virtualization" and "application virtualization."	N/A
"Hypervisor"	Also called a Virtual Machine Monitor (VMM), a hypervisor is the software that controls the actual virtualization of hardware.	N/A
"Native Hypervisor" / "Bare metal virtualization"	The hypervisor runs directly on the hardware.	VMware ESX Microsoft Hyper-V Xen Parallels Server
"Hosted Hypervisor"	The hypervisor runs as an application on top of a traditional operating system.	VMware Server VMware Workstation Microsoft Virtual Server Microsoft Virtual PC Parallels Workstation
"Full Virtualization"	The hypervisor emulates the full instruction set of the underlying hardware. This may or may not make use of virtualization-specific hardware features (i.e. "hardware assisted virtualization").	VMware products Parallels products
"Paravirtualization"	The hypervisor emulates a subset of the processor instruction set. The guest operating system must be ported to make some "system calls" directly to the hypervisor.	Xen
"Desktop Virtualization"	Each desktop connects to a virtual machine that is remotely hosted on a server.	VMware VDI Citrix XenDesktop Parallels VDI
"Resource Virtualization"	An abstraction of certain system resources such as storage (SAN/RAID), networking (VLAN), and memory.	N/A
"Operating System Virtualization"	Partitioning and isolation of user spaces is accomplished by intercepting system calls.	Parallels Virtuozzo chroot
"API Virtualization"	User-level library calls are replaced with calls to a compatibility layer that translates the virtualized system calls into native system calls.	Wine

Term	Explanation	Example Products
"Application Virtualization"	Virtualization layer runs on top of traditional operating system and intercepts application calls to specific operating system resources. The application believes it is fully installed on the operating system.	VMware ThinApp Microsoft App-V

Appendix: List of Vendor Documentation for Secure Configuration

Document	Link
VMware Infrastructure 3.5 Security Hardening	http://www.vmware.com/vmtn/resources/726
Managing VMware Virtual Center Roles and Permissions	http://www.vmware.com/vmtn/resources/826
ESX STIG (Secure Technology Implementation Guide)	http://iase.disa.mil/stigs/stig/esx_server_stig_v1r1_final.pdf
CIS (Center for Internet Security) Benchmark	http://www.cisecurity.org/bench_vm.html
DMZ Virtualization with VMware Infrastructure	http://www.vmware.com/vmtn/resources/1052
VI:ops Virtualization Security Community	http://viops.vmware.com/home/community/security
Hyper-V How To: Harden Your VM Security	http://blogs.technet.com/tonyso/archive/2008/09/23/hyper-v-how-to-harden-your-vm-security.aspx
Securing Xen	http://wiki.xensource.com/xenwiki/SecuringXen

Appendix: References and Further Information

Document	Link
Virtualization and Risk - Key Security Considerations for your Enterprise Architecture (Whitepaper)	http://www.foundstone.com/us/resources/whitepapers/VirtualizationWP_Foundstone_FINAL.pdf
Putting Security Into Your Virtual World (Webcast)	http://www.foundstone.com/us/resources/webcasts/virtualization_and_risk_webcast.zip
Top 10 PCI Concerns (Webcast)	http://www.brighttalk.com/webcasts/1202/play
PCI for Developers (3 hour computer based training module)	http://www.foundstone.com/us/cbt-pci-for-developers.asp
Security Design of the VMware Infrastructure 3 Architecture (Whitepaper)	http://www.vmware.com/resources/techresources/727
McAfee Virtualization Portal	http://www.mcafee.com/virtualization

Disclaimer

Although McAfee makes all reasonable efforts to maintain the accuracy of the contents of this document, it relies on third parties for much of the information provided and does not accept any liability for information that is found to be incomplete, inaccurate or out of date. McAfee reserves the right to change product or service specifications or data at any point.

The information contained in this document is only for general information, and is not intended to provide any advice, make any offer or in any other way result in the creation of a legally enforceable relationship between McAfee and yourself. You should place no reliance on such information for investment purposes or otherwise, and McAfee excludes all liability for loss or damage, whether financial or otherwise (to the fullest extent permitted by law) ensuing from your use of this information.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security.

<http://www.mcafee.com>.

McAfee, Foundstone and/or other noted McAfee related products contained herein are registered trademarks or trademarks of McAfee, Inc., and/or its affiliates in the US and/or other countries. McAfee Red in connection with security is distinctive of McAfee brand products. Any other non-McAfee related products, registered and/or unregistered trademarks contained herein is only by reference and are the sole property of their respective owners. © 2009 McAfee, Inc. All rights reserved.