



How Virtualization Affects PCI DSS

Part 1: Mapping PCI Requirements and Virtualization

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

Abstract

The PCI Data Security Standard¹ has been around for several years, but only recently has it become one of the major compliance requirements that many organizations are concerned about. Similarly, virtual infrastructures have come to be heavily depended on within many organizations. But within small pockets customers still seem hesitant to deploy virtualization – credit cardholder data environments are one of these pockets. As PCI compliance requirements become more and more strict and virtualization technology gains a stronger foothold in IT departments of organizations that also have to comply with PCI Data Security Standards, many questions are being raised: *“How will this technology affect my PCI compliance?”*; *“What new concerns need to be addressed to ensure continued PCI compliance?”*; *“Do these concerns really relate to the PCI Data Security Standard?”* and finally *“What exactly should I do address these concerns?”* This white paper series takes a pragmatic view at the different components of virtualization technologies and provides a perspective on how enterprises that are looking to deploy such technologies should think about their impact on PCI compliance initiatives. As these two major areas of IT focus inevitably intersect this series of whitepapers first present a mapping for the various and relevant PCI requirements and how these are impacted by virtualization. In the next paper we will discuss what we believe to be the top 5 concerns that must be addressed before a full-scale deployment of virtualization technologies is undertaken within a PCI environment.

Introduction

PCI Data Security Standard

Theft of credit/debit card information – also referred to as cardholder data (CHD) - is increasing with the steady rise in Internet shopping and e-commerce as well as the use of potentially risky technologies such as wireless networking. The PCI Data Security Standard (PCI DSS) was established by the major payment brands with a goal to limit the risk to cardholder data from such threats. The PCI DSS achieves this by specifying detailed people, process and technology related controls that must be implemented by all organizations dealing with cardholder data.

¹ <https://www.pcisecuritystandards.org/>

While all organizations dealing with cardholder data were always required to comply with the PCI DSS, the enforcement so far has been restricted to a handful of high-profile merchants and service providers. However, recent high-profile data thefts reported in the media² have resulted in stricter enforcement of the PCI DSS requirements, compelling many organizations to either demonstrate compliance or face various penalties including fines.

As most organizations turn towards virtualization to optimize resource utilization and operational efficiencies, they are faced with the reality that while the PCI Data Security Standard is very detailed and specific, to-date it does not acknowledge or accommodate some of the unique challenges faced by an organization that chooses to deploy hardware or software virtualization technology within its PCI environment. In fact, some PCI controls can be easily misinterpreted to mean that virtualization is incompatible with PCI DSS compliance. This is leading to confusion resulting in either failure to comply with the PCI DSS, or hesitation to deploy virtualization technology within PCI environments. The compelling benefits that virtualization has to offer make this latter choice not much of a solution.

Most PCI experts would tell you that the most important factor in achieving compliance is to clearly understand the intent behind each PCI DSS control. With this in mind, the first paper in our series maps out the various PCI controls and discusses how virtualization presents unique challenges to implementing these controls in your cardholder data environment (CDE). In the next whitepaper we will then aim to highlight the top five issues and concerns that PCI Qualified Security Assessors have about virtualization technology and propose solutions to demonstrate compliance while deploying virtualization technology within a PCI environment. The contents of this paper have been put together based on our experience of doing many PCI assessments as well as virtual 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 and 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

² <http://www.msnbc.msn.com/id/17853440/>

Mapping PCI Requirements

In the table below we present a description of the various PCI requirements as they relate to virtualization technology. When appropriate we cross reference our second whitepaper in the series which describes the top 5 issues in virtualized PCI environments.

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
1.1.3	Requirements for a firewall at each Internet connection and between any DMZ and the internal network zone.	<i>Discussed in "Top 5 Issues"; see Issue #2³</i> Certain virtualization technology provides organizations with the ability to implement virtual firewall technology. Organizations will need to ensure that the configuration and implementation of a virtual firewall provides the same level of protection as a physical separate firewall.
2.1	Always change vendor-supplied defaults before installing a system on the network.	As with any standard application or hardware organizations must not treat virtualization technology any differently and must change all default passwords on implementations. This includes passwords for the guests, the hosts, the virtual management utilities and any other related third party components used within the virtualization infrastructure.
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	Many organizations have developed secure build standards for tradition items of IT infrastructure such as operating systems and applications. Virtualization technology should not be treated any differently and each has their own security hardening requirements. Guidelines for the major virtualization platforms are listed at the end of this document.

³ Each of these references one of our Top 5 issues in the next whitepaper in this series.

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
2.2.1	Implement only one primary function per server	<p><i>Discussed in "Top 5 Issues"; see Issue #1</i></p> <p>This requirement is a contentious issue for virtualization technology. It is definitely possible to use virtualization and still meet the intent of the requirement, but organizations will need to carefully consider how their whole infrastructure is architected in relation to this requirement. Further, only bare-metal or native virtualization must be considered for cardholder data environments.</p>
2.2.2	Disable all unnecessary and insecure services and protocols	<p>Each virtualization technology has specific recommended security administration settings. Ensure that the VI administrators in organizations follow these guidelines. In addition, virtualization technology may implement different services dependant on how the solution is configured and architected. Organizations should review the architecture in line with the services enabled. An example of this includes the use of the insecure VNC like protocol for remote connectivity to virtual machine consoles. Organizations should disable this protocol and use secure alternatives such as SSH.</p>
2.2.3	Configure system security parameters to prevent misuse.	<p>Each virtualization technology has specific security administration settings e.g. VMware has a security hardening document for the different versions of their virtual infrastructure. Ensure that the VM administrators in organizations follow these guidelines.</p>
2.2.4	Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	<p>Organizations should also consider disabling functionality that they are not using. This includes unnecessary functionality in the Service Console as well as convenience features such as cut and paste clipboard sharing.</p>

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
2.3	Encrypt all non-console administrative access. Use technologies such as SSH, VPN, or SSL/TLS for web based management and other non-console administrative access	<i>Discussed in "Top 5 Issues"; see Issue #2</i> Encryption of all non console access is of the utmost importance for virtualization technology. Organizations must understand that VM administrators have more concentrated power in their hands that traditional network and server administrators. It is therefore vital to not only use secure protocols such as SSL/TLS for connectivity to the hosts and virtual management servers but to also ensure that the SSL is correctly configured e.g. are SSL certificates being validated? Are self signed certificates in use?
3.1	Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for business, legal, and/or regulatory purposes, as documented in the data retention policy.	<i>Discussed in "Top 5 Issues"; see Issue #3</i> Organizations should ensure that they implement policies and processes to properly control cardholder data before the archiving and storage of virtual machine images.
3.5	Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse	<i>Discussed in "Top 5 Issues"; see Issue #3</i> Organizations should ensure that they implement policies and processes to properly control cryptographic keys before the archiving and storage of virtual machine images.
5.1	Deploy anti-virus software on all systems commonly affected by malicious software	Organizations will need to deploy AV not only on guest OS partitions but also on any console or management OS partition if it's Windows 2003 or UNIX.

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
6.1	Ensure that all system components and software have the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	<p><i>Discussed in "Top 5 Issues"; see Issue #5</i></p> <p>Like all commercial software virtualization technology will have security patches released. Organizations must ensure that they include the VM platform (guest virtual components such as VMware tools, host patches and virtual infrastructure management components) in existing patch management processes. It is also important to consider the patching of offline images, templates and snapshots.</p>
6.2	Establish a process to identify newly discovered security vulnerabilities	<p>Organizations must track vendor and public mailing lists for the various virtual infrastructure components to obtain prompt information as to the existence of security vulnerabilities in the software they have deployed. VMware provides a public subscription service for security alerts at http://www.vmware.com/security.</p>
6.3.2	Separate development/test and production environments	<p>Some organizations use virtual environments extensively for testing. Organizations need to make sure test images are segregated from production images.</p> <p>Dependant on an organizations risk profile they may also want to consider running separate environments on different physical hardware.</p>

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
6.3.5	Removal of test data and accounts before production systems become active	<p>This is especially relevant if virtual images are migrated from test environments to production environments.</p> <p>With virtualization, it is easy to copy a virtual machine directly from a pre-production environment directly into production. However, the best practice is not to do so, but rather to only use pristine virtual machine images or templates in production. These templates can be built to include the same operating system, patches, and applications for production as for pre-production. After this template has been thoroughly tested and approved, it can be used to deploy production systems.</p>
6.4	Follow change control procedures for all changes to system components	<p><i>Discussed in "Top 5 Issues"; see Issue #5</i></p> <p>Organizations need to ensure that their operational change control procedures cover the issues around VM environments. Change control is often treated loosely in virtual environments due to the ease with which changes can be made / undone in such environments. However, this is a bad practice since it can lead to unauthorized and potential catastrophic changes.</p>
7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	<p><i>Discussed in "Top 5 Issues"; see Issues #1, 2, & 5</i></p> <p>When assigning roles and responsibilities within the virtual environment ensure that these are assigned using the principle of least privilege. Also consider the</p>

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
7.2	Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	<p>significance of specific actions such as cloning a virtual machine when assigning these privileges and avoid handing out such sensitive permissions unless absolutely necessary for the business. Refer to the end of this document for pointers to guidelines on access controls.</p> <p>This is another reason why only bare-metal or native virtualization must be considered for cardholder data environments. Unlike hosted virtualization technologies, these provide much richer and fine grained authorization controls.</p>
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data	Create separate user IDs for all users accessing the virtual infrastructure platforms. In a virtualized environment access controls to the management console should be integrated with a directory service such as Active Directory
8.5	Ensure proper user authentication and password management for non-consumer users and administrators on all system components	Password complexity rules (length, character combo, expiry, history, etc) must be enforced on VM platform. Integration with a directory service such as Active Directory enables the use of existing centralized password management policies.
9.6	Physically secure all paper and electronic media that contain cardholder data	<p><i>Discussed in "Top 5 Issues"; see Issue #3</i></p> <p>Cardholder data may be present in virtual machine disk files. Organizations need to restrict access to these files and the ability to copy them to other media. They also need to keep track of all potential replicas of these files, such as snapshots, and destroy all copies when the virtual machine is no longer required.</p>
9.7	Maintain strict control over the internal or external distribution of any kind of media that contains cardholder data	

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
9.8	Ensure management approves any and all media containing cardholder data that is moved from a secured area (especially when media is distributed to individuals)	
9.9	Maintain strict control over the storage and accessibility of media that contains cardholder data	
9.10	Destroy media containing cardholder data when it is no longer needed for business or legal reasons	<p><i>Discussed in "Top 5 Issues"; see Issue #3</i></p> <p>Ensure that all VMs used for storing cardholder data are unregistered and deleted when no longer needed. This is especially true for snapshots or clones that have been created. In general, cloning or templating of virtual machines that already contain cardholder data must not be permitted as a best practice.</p>
10.2	Implement automated audit trails for all system components	<p><i>Discussed in "Top 5 Issues"; see Issue #4</i></p> <p>Ensure that audit trails are maintained for the virtual infrastructure components especially management utilities and the host. These audit trails must also be integrated with central log management facilities.</p>

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
10.3	Record at least the following audit trail entries for all system components for each event (User ID, Type of Event, Date and Time, Success/Failure indication, Origination of Event, Identity of affected system/data)	<p><i>Discussed in "Top 5 Issues"; see Issue #4</i></p> <p>Ensure the log levels are configured adequately to meet the PCI requirements. This applies to both the host the virtual infrastructure management components.</p> <p>VMware VI3 includes detailed logging of all events in a comprehensive events database. Local log files on servers also record events, providing a secondary record. Both of these should be used as sources for an audit trail.</p>
10.4	Synchronize all critical system clocks and times	Synchronize the guest with the host and the host to an NTP based time source that is used for other infrastructure components such as servers and network devices.
10.5	Secure audit trails so they cannot be altered	<p><i>Discussed in "Top 5 Issues"; see Issue #4</i></p> <p>Ensure all audit trails have strong access controls. Securing these is described in the vendor hardening guides as well as other sources such as the CIS baselines.</p> <p>Closely restrict access to any database where events are recorded, such as the Virtual Center database. Log files from individual ESX hosts can be sent to a secure remote syslog server, thus reducing the possibility of tampering.</p>

PCI DSS Requirement	PCI DSS Description	Virtualization Impact
10.6	Review logs for all system components at least daily	<i>Discussed in "Top 5 Issues"; see Issue #4</i> 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.
11.5	Deploy file-integrity monitoring software to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly	<i>Discussed in "Top 5 Issues"; see Issue #4</i> Configuration files 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.
12.1.1	Establish, publish, maintain and disseminate a security policy that addresses all PCI DSS requirements.	Ensure that all security policies have been extended to describe virtualization specific issues.
12.2	Develop daily operational security procedures that are consistent with requirements in this specification	Ensure that all security procedures have been extended to describe virtualization specific issues.
12.3	Develop usage policies for critical employee-facing technologies	Ensure that all usage policies have been extended to describe virtualization specific issues.

Conclusion

We have provided a cursory overview above of the PCI DSS controls and requirements and how these could be potentially affected by virtualizing your infrastructure. In the next paper in this series we will discuss the top 5 of these issues based on our experience having worked with companies in our capacity as a QSA as well as by leveraging our experience of performing virtual infrastructure security assessments.

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 aQSA 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. (NYSE: MFE), 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. For more information, visit www.foundstone.com.

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
"Application Virtualization"	Virtualization layer runs on top of traditional	VMware ThinApp

	operating system and intercepts application calls to specific operating system resources. The application believes it is fully installed on the operating system.	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.