WHITE PAPER – June 2011

5 Mistakes Auditing Virtual Environments (You don’t Want to Make)

Payment Card Industry (PCI) Qualified Security Assessors (QSA) increasingly are asked to verify whether a virtual environment is in compliance with the Data Security Standard (DSS) 2.0. Virtual systems, in other words, have to be assessed to determine their adequacy for protection of a cardholder data environment (CDE) – Ability to protect systems that store, process or transmit payment card data, especially sensitive authentication data.

This paper provides guidance on how to avoid five of the most common errors when virtual environments are assessed for PCI DSS 2.0 compliance.
Contents

Mistake #1 Scope 3
Mistake #2 Data Access 4
Mistake #3 Unique ID 5
Mistake #4 Incomplete Access Monitoring and Tracking 6
Mistake #5 Vendor Defaults and Hardening 8
Mistake #1 Scope
(PCI DSS v2.0 Executive Summary)

The PCI DSS has twelve requirements; but there also is a requirement before the twelve considered so essential it has become known as Requirement 0. The following text from PCI DSS 2.0 makes the requirement clear:

*The first step of a PCI DSS assessment is to accurately determine the scope of the review. At least annually and prior to the annual assessment, the assessed entity should confirm the accuracy of their PCI DSS scope by identifying all locations and flows of cardholder data and ensuring they are included in the PCI DSS scope.*

An assessed entity has to provide an accurate scope but the auditor has to review the entity’s scope statement(s) for completeness as well as accuracy. Segmentation is not a requirement of PCI DSS but it influences the scope for an assessment. The auditor has to carefully review controls and how they are used to validate segmentation; otherwise they will fail to review all areas that require assessment.

PCI DSS Assessors and other auditors who review a segmentation control for effectiveness and scope may not realize the capabilities of a virtual environment. A virtual environment introduces powerful software automation tools to handle many layers of resource management. Once the virtual environment is operational it can be more easily modified than a traditional IT environment. This ease of modification required more diligence for these changes in the evaluation necessary for true segmentation.

The time and physical access that used to be required to modify a data center, for example, is replaced by an application with just menus to select from. Systems are deployed or modified easily and challenge the accuracy of scope efforts – migration of an entire system or adding/removing connections may take no more than a click of a button. An unrelated area of the network may quickly become directly involved in payment card storage, processing or transmission.

The diagram to the right shows how audit of a virtual machine with multiple disks can involve a much broader environment than with a traditional machine. The audit scope may be not only what is seen in this picture but virtual disks and files more accessible from management systems outside this diagram or an array not illustrated (where they could migrate). Does the present state of a virtual environment represent the total scope of likely cardholder data environment configurations?
Mistake #2 Data Access
(PCI DSS v2.0 Requirement 7)

Access to system components, as defined by the PCI DSS Requirement 7, must be restricted to only the individuals whose job requires access. The intent of the Role Based Access Control (RBAC) requirement is clear – the less access to data the lower the risk of its unauthorized disclosure. Only those who need access to fulfill their job should be granted access and the system they use must be capable of documenting and controlling their access as well as denying access to all others.

A mistake commonly made is to treat a virtual environment as similar enough, and even equal, to traditional IT environment controls. There are notable differences, however, as illustrated in the figure below. Virtual machines, their related data and networks, can exist within a software environment that may require unique, non-traditional or even proprietary controls.

It is not unusual for an environment to require the introduction of controls separate and distinct for its network and system devices.

An assessor often will find different access control procedures and policies for different platforms in the CDE; RBAC in a Windows environment may be managed distinctly from a UNIX environment. This is despite significant overlap and similarities between systems. The virtual systems have the same issue. They apply the generic concepts of Users, Groups, Roles, and Permissions to a separate layer and interface.

The need for a separate control approach for virtual systems is highlighted by the test procedure for PCI DSS Requirement 7.1.4.

*Confirm that access controls are implemented via an automated access control system*
This confirmation test leads directly into PCI DSS Requirement 7.2, which calls for the establishment of a system that can enforce a “default deny” policy and prevent unauthorized access.

Although virtual environments provide their own access controls to address RBAC (a user can be defined locally by VMware vCenter or with LDAP, for example) they also have to meet the requirement for an automation system. Automation has to cover the guest system (e.g. Linux and Windows) as well as the host (e.g. VMware ESX/ESXi) controls. The key is to establish that controls are in place including audit trails for least privilege, assignment by job class and function, and documentation of approvals.

Legacy access control systems and those provided by virtualization vendors typically do not provide sufficient assurance at this level of control, let alone automation. VMware vSphere, for example, has controls that account for access to resources such as the network and data stores. This is not sufficient for a QSA or other auditor to verify whether a virtual image can be moved to a cluster that does not comply with PCI DSS 2.0 requirements. While an administrator can be in charge of one or more clusters or one or more physical servers, the assessor has to verify which clusters adhere to compliance requirements and audit the controls within the administrator’s interface (e.g. VMware vSphere).

New capabilities mean new areas to assess for granularity and control. The setup, configuration, monitoring and auditing within the virtual environment increases time required to assess compliance. An entity may try to reuse groups and permissions from their existing environments, omitting to include details that are specific to the unique access and management steps for virtual machines.

Important audit questions to ask are:

- Is every access by a role (i.e. admin) recorded?
- How are duties segregated in the virtual environment?
- Are all clusters in scope or can migration be controlled?

A QSA can avoid mistakes on Requirement 7 by looking for evidence of strong authentication and granular RBAC with clear labels for all levels of access within products such as VMware’s ESX/ESXi, vCenter, VM console, and virtual network products such as the Cisco Nexus 1000V.

**Mistake #3 Unique ID**

*(PCI DSS v2.0 Requirement 8)*

The virtual environment introduces new layers to identity management in the cardholder data environment (CDE). It adds both remote and local accounts to be reviewed in addition to accounts that already would exist in a traditional IT environment.

Assessors must not make the mistake of underestimating the importance of the non-unique accounts such as root on VMware ESX (Linux) or administrator on VMware Virtual Center (Microsoft Windows). Extra caution is necessary to ensure controls are present to manage the virtual environment.
First, the virtual environment non-unique IDs bring with them different risks. A host in the virtual environment has a super user account, as with any multi-user system. Unlike the traditional IT environment, however, this account has authority over guest data, communication between guests and communication with external networks.

Guest systems are exposed to a non-unique super user account on a host infrastructure in new and different ways than if they were in a traditional IT environment. The generic administrative identities of VMware vCenter and ESX/ESXi, for example, can affect remote access as well as access to system components and cardholder data. PCI DSS Requirement 8.2 means that every action by a user account on a host that communicates with the Internet must be tied to a unique identity and two-factor authentication. The virtual environment also must be able to achieve the more granular controls under PCI DSS Requirement 8.5 such as idle session timeout after 15 minutes and restricted/authenticated database access.

Second, the guest systems also easily can be migrated to a new host as illustrated below, exposing them to non-unique super user accounts on systems different from where they might be audited for compliance.

A system with cardholder data is at risk of being quickly and easily moved into an environment that is not PCI DSS compliant. Auditors must confirm that the virtual environment detects and prevents this movement as well as provisioning that would enable a virtual machine with a default non-unique account.

It is critical for an auditor to confirm specific procedures and controls are in place to prevent a new virtual machine from being deployed with a generic account like root, a default password, and a service running that enables remote connections (i.e. SSH).

The host systems for virtual machines may be intended to operate as a secure appliance or to be an independent infrastructure isolated from the virtual machine. However, this must be verified by an auditor by examining controls most likely designed specifically for a virtual environment. The virtual environment should be assessed for the capability to put all non-unique credentials in a “vault” – access to any and all generic accounts should be restricted to make their use far less likely and also constantly monitored for abuse.

**Mistake #4 Incomplete Access Monitoring and Tracking**

(PCI DSS v2.0 Requirement 10)

PCI DSS Requirement 10.2 states that all system components must have automated audit trails. Virtual environment infrastructure products can provide capabilities to achieve some of what is required. They have log output for user and system events. An auditor would be mistaken to consider them sufficient on their own.
The operating systems have proven to require separate and distinct access monitoring and tracking controls. Likewise the virtual environment software layer that is introduced as a host to the operating systems requires functionality beyond what it included by default. The ability to configure, manage and monitor the logs has to be carefully implemented or it can add significant burden to operations without achieving the compliance requirements.

Audit of a system that performs monitoring and tracking can become complicated without the presence of controls and tools dedicated to log management. Virtual environments may offer the ability to create a network for web applications and log all connections, but they add additional layers of information to access monitoring. The diagram shows a firewall in front of a three-tier application, which illustrates the need to audit the web segment, application segment, and database segment to account for separation within a virtual environment.

There will be logs for the deployment and configuration of the three VMs, the host system, as well as the firewall to deploy and configure the networks. There also will be logs for communication between the segments and the virtual machines. The misconfiguration of any of these elements should be detected by access monitoring and tracking.

Virtualization introduces a greater ability for administrators to duplicate and deploy systems with these multiple tiers. Access monitoring must provide evidence of uniqueness and the capability to ensure separation. An auditor must test, for example, whether a client IP address will be logged consistently across numerous instances of a similar or even identical architecture. There can be multiple firewall deployments within a host yet the access management of each must be uniquely tracked and monitored with a centralized system.

Operational logs also have to be able to support the granularity necessary to identify the exact objects that are modified by administrators and users (e.g. the zone has to indicate web, app or db). Success and failure operations for objects also have to be logged and tied to individual unique identities.

An administrator that configures a new virtual web application setup, in other words, should be traced in the logs to a unique individual and their actions tied to the various and numerous objects deployed, configured and accessed. If logs indicate only that a single process from a generic account created a complex new network with multiple hosts, then the virtual environment does not provide the level of detailed access monitoring and tracking necessary for PCI DSS 2.0 compliance under Requirement 10.
Mistake #5 Vendor Defaults and Hardening (PCI DSS v2.0 Requirement 2)

PCI DSS 2.0 Requirement 2.1 states that systems cannot be installed on a network until vendor defaults have been changed.

Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.

A virtual machine easily can be duplicated and deployed using vendor-supplied defaults. Controls to prevent this in a traditional IT environment, such as scanning the network for new systems, become less effective in a virtual environment. An auditor may easily fail to notice defaults as an entity has to manage virtual machines from within the virtual environment itself.

Applications used to build, configure and deploy the virtual systems provide the ideal place to extend scans for vendor defaults. The ease of hiding virtual machines from legacy assessment tools means the legacy tools are typically insufficient on their own; for example, they are unable to see services running on virtual interfaces on a virtual network. The deployment of a virtualization-aware scanner or access monitoring system would address this audit failure.

PCI DSS 2.0 Requirement 2.2 states that system components must use standard configurations that address security.

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.

Audit tests to meet this requirement are not only that configurations be “consistent with industry-accepted hardening” and kept up-to-date but also that the configurations are “applied when new systems are configured”. Auditors must take special precaution to test this in virtual environments because of the low barrier to configuration of new systems.

A virtual machine deployed for the first time will have to be secured before it is launched in order to comply with Requirement 2.2. Systems that already are deployed also must be assessed and updated to meet a configuration standard. Given that deployment in a virtual environment can be just a button click or two, an auditor might assume that it always is easy to make changes to a configuration. This is not always the case, however.
VMware vCenter Server has a Host Profiles feature, for example, which can capture a "gold image" configuration of an ESX host and then configure other hosts. The Host Profile can be created from an operational host and used to check for compliance but it cannot be applied unless the host is set to Maintenance Mode; virtual machines on the host have to be migrated to another host or powered down while a configuration is updated.

The traditional IT environment typically has maintenance windows and the virtual environment may adopt the same approach to get around this Maintenance Mode outage. Other solutions may also be available. An auditor should test procedures and policy to determine whether an outage requirement prevents the timely update of configurations. Hardening a virtual environment should be approached in a manner that minimizes downtime yet allows for monthly updates.
K3DES, headquartered in Houston, TX, is a consulting firm focused on the security of electronic payments systems – debit, credit, and stored value cards. The firm is a Payment Card Industry (PCI) Qualified Security Assessor (QSA) and provides computer and network security assessments, network vulnerability scanning, application penetration testing, application code reviews, cryptographic and security consulting, cryptographic training, forensic assessments and fraud analysis for the electronic payments industry. Information about K3DES can be found at http://www.k3des.com.

HyTrust®, headquartered in Mountain View, CA, is the leader in policy management and access control for virtual infrastructure. HyTrust delivers enterprise-class controls for access, accountability, and visibility in the virtual environment. The Company is backed by top tier investors Granite Ventures, Cisco Systems (Nasdaq: CSCO), Trident Capital, and Epic Ventures; its partners include VMware; Symantec (Nasdaq: SYMC); Citrix (Nasdaq: CTXS); RSA (NYSE: EMC) and Intel Corporation (Nasdaq: INTC). Information about HyTrust can be found at http://www.hytrust.com.