

Altor and PCI Compliance

August 5, 2009 (Doc Rev A)

This document highlights the major PCI Data Security Standard (DSS) Requirements and explains how Altor can keep organizations in compliance.

This document is for informational purposes only. ALTOR MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Altor.

Altor may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Altor, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

© 2008 Altor Networks, Inc. All rights reserved.

You may not use any trademark or service mark appearing in this document without the prior written consent of the owner of the mark. "Altor", and the Altor logo are trademarks (or service marks, as applicable) of Altor.

All other trademarks and/or service marks identified or referenced are the property of their respective owners and subject to their usage requirements.

Table of Contents

PCI DSS Overview	4
PCI In a Virtual Environment	4
PCI DSS Key Requirements Supported By Altor	5
Build and Maintain a Secure Network	6
<i>PCI DSS Requirement 1</i>	6
<i>PCI DSS Requirement 2</i>	7
Maintain a Vulnerability Management Program	8
<i>PCI DSS Requirement 6</i>	8
Regularly Monitor and Test Networks	9
<i>PCI DSS Requirement 10</i>	9
<i>PCI DSS Requirement 11</i>	9
Maintain an Information Security Policy	10
<i>PCI DSS Requirement 12</i>	10

PCI DSS OVERVIEW

The Payment Card Industry Security Standards Council has established 12 Requirements for any business that stores, processes or transmits payment cardholder data. These requirements are summarized in the following table:

Table 1. PCI Data Security Standard (DSS) Requirements

Goals	PCI DSS Requirements – Validated by Self or Outside Assessment
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect cardholder data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored data4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update anti-virus software6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to cardholder data by business need-to-know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security

Compliance with PCI DSS also ensures compliance with several individual card standards:

- American Express (DSOP)
- Discover (DISC)
- MasterCard (SDP)
- Visa (AIS, CISP)

More information is available at the below locations:

https://www.pcisecuritystandards.org/pdfs/pciissc_getting_started_with_pciidss.pdf

http://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

PCI IN A VIRTUAL ENVIRONMENT

Organizations are deploying virtualization technologies because of the clear cost savings and operational efficiency gains. However, there are security risks when you virtualize, including: mixed Virtual Machine (VM) trust levels, dynamic VM migration, revision control and VM sprawl. Traditional security options (VLAN, legacy physical firewalls, etc.) aren't well suited to eliminate these risks regardless of whether they have been implemented to protect payment card systems or not.

The PCI requirements in place to ensure adequate system isolation and system monitoring of cardholder data are relevant whenever virtualization tools are being used.

When companies begin virtualizing systems they are creating an entirely new virtual network within their existing physical network. Virtual Machines are interconnected on this virtual network via virtual nics and virtual switches. Left in their default state, VMs are free to communicate with other members of the virtual network without a single packet having to leave the virtual network and thus be seen on the physical network. This means communication between virtual machines can completely bypass physical security products.

Securing up to the physical NIC on a virtualization host (ESX Server) does nothing to protect the virtual machines (VMs) which are running inside the host and communicating across the virtual network. This fact is the core issue in maintaining compliance when organizations decide to virtualize any portion of their payment card environment (and generally for meeting audit requirements as a secure organization).

Altor built a security solution for virtual environments and is uniquely positioned to provide the right type of dynamic, strong security measures needed for PCI compliance in virtual networks.

PCI DSS KEY REQUIREMENTS SUPPORTED BY ALTOR

The Altor solution easily helps IT departments achieve and prove compliance in several key areas. Altor includes three important modules for protecting networks: a Network Visibility Module, Firewall Module and an IDS Module. Using these three modules, Altor can be used to comply with four of the six high level PCI DSS Requirements:

High Level PCI DSS Goals Supported By Altor

- Build and Maintain a Secure Network
- Maintain a Vulnerability Management Program
- Regularly Monitor and Test Networks
- Maintain an Information Security Policy

The remainder of this document will highlight the exact requirements from the PCI DSS Specification (Version 1.2) which Altor helps satisfy.

Build and Maintain a Secure Network

PCI DSS Requirement 1

“Install and maintain a firewall configuration to protect cardholder data”

PCI DSS Requirements	How Altor Enables Compliance
<p>1.1 Establish firewall and router configuration standards</p> <p>1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure</p>	<p>Altor is installed within the virtual infrastructure and stores all network communication (either vm-to-vm or vm-to-physical) in a database.</p> <p>Reports can be generated showing all network activity (protocols, ports, etc.) in use on every VM over any given time period. As new VMs are created Altor see’s them automatically and can report on that activity.</p> <p>With this information you can properly document all known services/protocols in operation and justify their usage.</p>
<p>1.2 Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment</p> <p>1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.</p> <p>1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.</p>	<p>Altor has a rich history of building successful security solutions. We’ve created a hierarchy of firewall policies which allow administrators to easily secure VMs.</p> <p>All VMs are required to conform to the Global Policy with high level and low level rules. Next there are Group Policies (for example Web Servers) and finally the ability to create a policy for an individual VM.</p> <p>All data in or out of the virtual environment can be tightly controlled (the rule editor is simply defined into ‘inbound and outbound’ sections). It doesn’t matter if the remote network is wireless or internet connected traffic must pass through the Altor firewall before reaching the actual VM.</p>
<p>1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.</p> <p>1.3.1 Implement a DMZ to limit inbound and outbound traffic to only protocols that are necessary for the cardholder data environment.</p> <p>1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.</p> <p>1.3.3 Do not allow any direct routes inbound or outbound for traffic between the Internet and the cardholder data environment.</p> <p>1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.</p> <p>1.3.5 Restrict outbound traffic from the cardholder data environment to the Internet such that outbound traffic can only access IP addresses within the DMZ.</p> <p>1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only “established” connections are allowed into the network.)</p> <p>1.3.7 Place the database in an internal network zone, segregated from the DMZ.</p>	<p>In addition to the granular policy editing described above there are some other key elements which allow Altor to build any incarnation of firewall policy needed for the protection of payment card resources.</p> <ol style="list-style-type: none"> 1. Altor does security based on IP address as well as the unique VMID/UUID which is associated with a VM when it’s created in VirtualCenter 2. Altor does all security policy enforcement in the kernel of the hypervisor therefore individual policies can be created on a per-vm basis without use of TCP RSTs or large zones/groups of VMs (VLANs, etc.) 3. Altor can write policy for VM-to-VM communication or VM-to-Physical communication (either by host or by subnet definition)

PCI DSS Requirement 2

“Do not use vendor-supplied defaults for system passwords and other security parameters”

PCI DSS Requirements	How Altor Enables Compliance
<p>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.</p> <p>2.2.2 Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device’s specified function).</p> <p>2.2.3 Configure system security parameters to prevent misuse.</p> <p>2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.</p>	<p>Altor is able to produce network connection reports which clearly show the protocols in use by every VM on the network where payment systems are connected. You can determine if unnecessary web servers are running or file servers are functioning or any other applications are being used and shouldn’t be.</p> <p>In addition, you can automatically disconnect systems which are inappropriately connected to secure networks like the ‘vmsafe’ communication network.</p> <p>You can monitor for things like VMware VMCI on VMs which can lead to security issues.</p>
<p>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.</p>	<p>Altor uses encryption for all system communication and requires encrypted authentication to access the Altor Management Center application (all passwords are force changed during install).</p> <p>Altor can monitor, alert and/or stop the use of non-encrypted protocols on the network (telnet or ftp instead of ssh or scp/sftp).</p>

Maintain a Vulnerability Management Program

PCI DSS Requirement 6

“Develop and maintain secure systems and applications”

PCI DSS Requirements	How Altor Enables Compliance
<p>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>	<p>Altor has two types of patches/updates.</p> <ol style="list-style-type: none"> 1. Altor Application fixes 2. Altor signature feed for malicious traffic monitoring (IDS) <p>In both cases, the Altor application will notify an administrator that a patch needs to be applied. The patches for signature updates can also be applied without administrator intervention.</p>
<p>6.3 Develop software applications in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices, and incorporate information security throughout the software development life cycle.</p> <p>6.3.2 Separate development/test and production environments</p>	<p>VMware environments will often have both a test/dev cluster(s) as well as a production cluster(s). Because Altor is installed in the kernel of each individual ESX/ESXi host it is easy to create security policies which completely isolate the traffic in each environment.</p>
<p>6.5 Develop all web applications (internal and external, and including web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes</p> <p>6.5.1 Cross-site scripting (XSS)</p> <p>6.5.2 Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.</p> <p>6.5.3 Malicious file execution</p> <p>6.5.4 Insecure direct object references</p> <p>6.5.5 Cross-site request forgery (CSRF)</p> <p>6.5.6 Information leakage and improper error handling</p>	<p>Altor has an IDS engine which is incorporated into the virtual infrastructure. The IDS engine is signature based and a portion of the signatures come from the Sourcefire VRT professional feed the foundation of which has more than 3.7 million users and is the most widely distributed intrusion technology in the world. Altor also adds custom signatures and expertise to this feed giving users world class protection.</p> <p>The IDS signature rules detect XSS, injection flaws, malicious file extensions, insecure direct object references and other malicious or inappropriate traffic.</p> <p>In addition since Altor monitors all connection flows, it can be used to spot information leakage between systems (i.e. VM1 communicating 10GB of traffic to VM2 unexpectedly).</p>
<p>6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by <i>either</i> of the following methods:</p> <ul style="list-style-type: none"> ✍ Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes ✍ Installing a web-application firewall in front of public-facing web applications 	<p>Altor has an advanced firewall and a combination of web based IDS signatures which allows organizations to fulfill the general requirement to protect web applications.</p>

Regularly Monitor and Test Networks

PCI DSS Requirement 10

“Track and monitor all access to network resources and cardholder data”

PCI DSS Requirements	How Altor Enables Compliance
<p>10.2 Implement automated audit trails for all system components to reconstruct the following events:</p> <p>10.2.1 All individual accesses to cardholder data 10.2.7 Creation and deletion of system-level objects</p>	<p>Controlling access to cardholder data is not just done by user based authentication. Access can also be controlled by implementing network based control (firewall blocking of access from system to system). Altor can show all access between systems and control access at the lowest level possible (i.e. system to system).</p> <p>Because Altor is tightly integrated into VMware VirtualCenter we are able to see the creation and deletion of VMs and adjust security policy accordingly. In addition, it's possible to see manipulation of security policies or events in the Altor application via system monitoring options.</p>
<p>10.4 Synchronize all critical system clocks and times.</p> <p>10.4.b Verify that internal servers are not all receiving time signals from external sources.</p>	<p>Altor can monitor all NTP traffic in the environment and block payment card systems from using unauthorized NTP systems.</p>
<p>10.5 Secure audit trails so they cannot be altered.</p> <p>10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.</p>	<p>Externally facing systems in the virtual environment can have logging turned on for their activities. Altor allows secure storage of these logs in a local database or can be configured to send logs via syslog to a central log collector.</p>

PCI DSS Requirement 11

“Regularly test security systems and processes”

PCI DSS Requirements	How Altor Enables Compliance
<p>11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).</p>	<p>Altor doesn't have an explicit scanning engine (such as Qualys). However, it's more likely you'll be able to pass compliance if you are aware of new VMs being created and/or deleted and have some history on what those systems have done over time. Since Altor sees (and stores) information related to every VM (regardless of their state in VMware) this information can be used to remain compliant.</p>
<p>11.4 Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines up-to-date.</p>	<p>Altor's IDS engine and updating mechanism fully satisfies this requirement</p>

Maintain an Information Security Policy

PCI DSS Requirement 12

“Maintain a policy that addresses information security for employees and contractors”

PCI DSS Requirements	How Altor Enables Compliance
<p>12.5 Assign to an individual or team the following information security management responsibilities:</p> <p>12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.</p> <p>12.5.5 Monitor and control all access to data</p>	<p>Altor has a reporting module which can be used to keep the security individual (or team) aware of exactly what is happening on the virtual network. The IDS and security alerts can show exactly what types of alerts are being triggered (High, Medium, Low, etc.).</p> <p>The reports can be set to automatically generate at predetermined intervals.</p>
<p>12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.</p> <p>12.9.5 Include alerts from intrusion-detection, intrusion-prevention, and file-integrity monitoring systems.</p>	<p>IDS reports can be easily created and even filtered for payment card systems only. Alerts for various activities include SMTP and SNMP.</p>