

Retail



## PCI 1.2 Requirements Mapping for Aruba Networks' Endpoint Compliance System (ECS)

Jim Hietala  
CISSP, GSEC, GCFW Principal Analyst  
Compliance Research Group



# Contents

Introduction.....	1
<i>What is the Payment Card Industry Data Security Standard?</i>	
<i>Version 1.1</i>	
<i>Version 1.2</i>	
<i>High-Level Requirements</i>	
<i>The Costs of Non-Compliance</i>	
<i>How Aruba Networks ECS Helps Organizations Achieve Compliance with PCI DSS</i>	
Aruba Networks' ECS.....	3
<i>Identity Management</i>	
<i>Endpoint Compliance</i>	
<i>Usage Policy Enforcement</i>	
ECS PCI DSS Requirements Mapping.....	4
Summary.....	7
About Aruba Networks.....	8
About Compliance Research Group.....	8
Appendix A.....	9
<i>Summary of Significant Changes, PCI DSS 1.1 to 1.2</i>	
Appendix B.....	10
<i>The Payment Card Industry Data Security Standard</i>	
<i>Merchants</i>	
<i>Service Providers</i>	

## Introduction

Numerous high-profile security breaches in the retail and payment card processing industries drove the development of the Payment Card Industry Data Security Standard (PCI DSS), a mandatory standard that is having a significant impact upon all retailers and credit card processors. This paper describes the role played by Network Access Control solutions, and Aruba Networks' ECS, in helping to meet the requirements of PCI DSS, and to secure networks more effectively.

### ***What is the Payment Card Industry Data Security Standard?***

Requirements that were formerly part of the VISA CISP and Mastercard CDP programs in 2004 were incorporated into a new industry standard known as the Payment Card Industry Data Security Standard (PCI DSS 1.0). All major credit card issuers support this standard, which creates a set of common industry security requirements. Entities that store, process or transmit cardholder data must comply with the PCI DSS and it affects any organization in the credit card payment chain. These include not only the the payment card brands but acquiring banks, retail organizations, and service providers as well. Even healthcare organizations, colleges and universities must comply with PCI DSS if they accept credit cards for any product or service.

The impact of non-compliance with PCI DSS has been most glaringly apparent in the retail industry where recent security breaches have occurred at CardSystems, TJX, and Hannaford Brothers.

CardSystems, a leading processor of credit card transactions, suffered a breach of 40 million credit cards in 2005. As a result, Visa USA and American Express penalized CardSystems for failure to comply with their data-security standard, and the ensuing database breach, by terminating access to their respective networks. CardSystems was also hit with a class-action lawsuit for failing to alert victims to the breach in a timely manner. The ultimate impact to CardSystems of failing to comply with PCI DSS and failing to adequately secure their IT infrastructure was that they were forced out of business.

TJX, a large retail chain that includes the popular TJ Maxx, Marshalls, and Bob's Stores, experienced a security breach from May-December 2006. The breach involved millions of cardholder records and was not uncovered until December of 2006 after months of data theft. TJX was not in compliance with PCI DSS at the time of the breach. Among other clean-up costs, TJX has offered \$40.9 million to VISA Card issuers affected by the massive data loss.

Hannaford Brothers, a leading supermarket chain in the Northeastern U.S., experienced a major breach in spring of 2008. Although Hannaford was technically in compliance with PCI at the time of the breach, millions of cardholder records were stolen. The most recent major breach was experienced by Heartland Systems. This breach, which was disclosed in January, 2009, potentially exposed as many as 100 million credit cards, and has caused massive reissuance of credit and debit cards by over 220 financial institutions.

Retailers and other organizations that process credit card transactions are wise to consider not only what is required to comply with PCI DSS today, but other best practices and controls to prevent new security threats from breaching their networks in the future. The PCI Security Standards Council responds quickly by updating the PCI standard when security threats emerge and controls change—but vulnerabilities and threats are moving faster.

### ***Version 1.1***

These constant reactions and updates make PCI DSS a constantly evolving standard. In September of 2006 the PCI Security Standards Council issued version 1.1, which updated the original PCI Data Security Standard. Version 1.1 added new controls to protect stored cardholder data, strengthen wireless network and application security, and other areas. The concept of compensating controls also was introduced.

### ***Version 1.2***

Responding to an increase in application vulnerabilities to cross-site scripting, SQL injection and other threats, PCI DSS version 1.2 was introduced in October, 2008. This white paper reflects Version 1.2 of the PCI DSS, which introduced the following significant changes:

- New language regarding all forms of malicious software, versus just anti-virus, was added to requirement 5
- New application security controls and test requirements were added to requirement 6
- Major expansion of access control requirements were added to requirement 7, which has important implications for network access control technology

## **High-Level Requirements**

PCI DSS version 1.2 continues the established organization of the standard, with 12 high-level requirements grouped into six objectives. Each high-level requirement consists of numerous additional specific requirements. The table below summarizes the 12 high-level requirements:

Objectives	Requirements
Build and Maintain a Secure Network	<b>1: Install and maintain a firewall configuration to protect cardholder data</b> <b>2: Do not use vendor-supplied defaults for system passwords and other security parameters</b>
Protect Cardholder Data	3: Protect stored cardholder data 4: Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	<b>5: Use and regularly update anti-virus software</b> <b>6: Develop and maintain secure systems and applications</b>
Implement Strong Access Control Measures	<b>7: Restrict access to cardholder data by business need-to-know</b> <b>8: Assign a unique ID to each person with computer access</b> 9: Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<b>10: Track and monitor all access to network resources and cardholder data</b> <b>11: Regularly test security systems and processes</b>
Maintain an Information Security Policy	<b>12: Maintain a policy that addresses information security</b>

*Note: Requirements addressed by Aruba Networks' ECS highlighted in bold.*

Nine of the requirements can be addressed by network access control (NAC) technology. The three remaining requirements relate to administrative or physical controls where NAC is not applicable.

## **The Costs of Non-Compliance**

PCI DSS compliance is enforced by the individual payment card brands. Each card-brand promotion program requires compliance to protect the brand's image and reputation. For example, VISA's PCI Compliance Acceleration Program, announced in December, 2006, provides incentives for acquiring financial institutions to demonstrate compliance, and levies significant fines for non-compliance. Acquiring banks may be subject to fines of \$5,000-\$25,000 per month for each of their Level 1 and Level 2 merchants who are not in compliance. In 2006 alone, VISA levied millions of dollars in fines.

Fines from the payment card brands may be the least of the problems faced by organizations with security breaches, however. Non-compliance can damage the company's own brand or image, and cause significant financial liabilities. Public awareness of security breaches from embarrassing publicity often has a negative impact on business and decreases goodwill.

Companies from service providers to retailers also risk losing customers if they are not compliant. PCI DSS requires merchants to do business only with service providers that adhere to the standard and these merchants could be forced to switch service providers if their database is compromised. In extreme circumstances, merchants that don't comply with PCI could lose the ability to process cardholder data altogether.

## **How Aruba Networks' ECS Helps Organizations Achieve Compliance with PCI DSS**

The PCI DSS requires organizations in the payment processing chain to secure both their networks and the systems on which cardholder data is processed or stored. NAC secures internal networks by ensuring the health and identity of the devices connected to them. NAC solutions address network access and control issues that cannot be countered by legacy firewalls and host-based identity and access management solutions.

Aruba Networks NAC solutions help organizations to secure and control access to networks. Aruba Networks ECS enables PCI DSS compliance by automating enforcement of strict access control policies to ensure that devices attaching to networks meet specific security requirements. Aruba Networks' ECS address 9 of the 12 PCI requirements. The three remaining requirements relate to administrative or physical controls where NAC is not applicable.

ECS is an out-of-band solution that leverages an organization's existing network infrastructure to enforce security policies. Leading analysts characterize out-of-band NAC implementations as the most secure, most scalable, most flexible, and most cost-effective solutions for automating network access control.

## **ECS**

ECS™ provides a comprehensive NAC solution that actively enforces network usage policies. As employees, contractors, partners, customers and others access network resources via wired, VPN and wireless access, ECS automatically ensures that users and devices are authorized to gain access and that they meet specific security policy requirements. ECS's identity management, endpoint compliance and usage policy enforcement capabilities help organizations to enforce specific access policies through role-based access to network resources. It protects against unauthorized users and non-compliant devices.

### ***Identity Management***

With employees and others using a range of devices to access network resources from diverse locations, effective network security for organizations must start with a robust identity management process. ECS requires all users and devices to be registered and authenticated before permitting access to the network.

Role-based access functionality ensures that users are allowed access only to specific network resources depending on the type of service they are authorized to use. The result is tight control over network access and a consistent, real-time view of the users and devices that are accessing network resources.

### ***Endpoint Compliance***

ECS ensures that all devices accessing the network meet required security standards by performing registry-based scans on endpoint devices prior to allowing network access. It can also perform port-based vulnerability scans using the open-source Nessus application.

ECS places devices that fail to meet specified security standards into a secure 'quarantine' state that prevents access to network resources. From this quarantine state, it gives legitimate users the ability to remediate any policy violations in order to regain network access.

ECS's endpoint compliance features monitor things like operating system types and patch levels, anti-virus / anti-spyware application types and definition version levels, the presence of required applications such as firewalls or prohibited applications such as peer-to-peer communications. In addition, customizable registry scans detect a range of other endpoint compliance criteria.

### ***Usage Policy Enforcement***

ECS applies role-based identity information and endpoint compliance criteria to enforce user-specific network access policies at the network edge – which is the point where endpoint devices physically attach to the network.

Usage policy enforcement actions include a wide range of configurable actions, such as blocking network access completely, limiting network access to only specific resources (such as for remediation), and alerting network administration and/or security personnel of policy violations.

ECS also interfaces with third-party solutions such as IDS, IPS, and Firewalls to gather additional information for enforcing access control policies. The result is network-wide control over access to network resources and automated enforcement of specified network usage policies.

## ECS PCI DSS Requirements Mapping

This section identifies the 9 specific PCI DSS requirements that ECS addresses. Requirements not addressed by ECS relate to administrative and physical controls and are excluded from the mapping below.

### Build and Maintain a Secure Network

<b>1.0</b>	<b>Install and maintain a firewall configuration to protect cardholder data</b>	
	<i>Firewalls are computer devices that control computer traffic allowed between a company's network (internal) and untrusted networks (external), as well as traffic into and out of more sensitive areas within a company's internal trusted network. The cardholder data environment is an example of a more sensitive area within the trusted network of a company.</i>	
	<i>A firewall examines all network traffic and blocks those transmissions that do not meet the specified security criteria. All systems must be protected from unauthorized access from untrusted networks, whether entering the system via the Internet as e-commerce, employees' Internet access through desktop browsers, employees' e-mail access, dedicated connections such as business to business connections, via wireless networks, or via other sources. Often, seemingly insignificant paths to and from untrusted networks can provide unprotected pathways into key systems. Firewalls are a key protection mechanism for any computer network.</i>	
	<b>Requirement</b>	<b>Relevant ECS Functionality</b>
1.2	Build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment.	ECS segregates user access to network facilities based upon identity and role-based policies. This capability can restrict access to the cardholder data network to only authorized users and devices.
1.3	Prohibit direct public access between the Internet and any system component in the cardholder data environment.	While not a firewall per se, ECS can restrict user and device access to the cardholder network, using a seven-point authentication match, VLANs, and role-based access control. ECS provides positive authentication and access control for all network users and devices, including those accessing the internal network from wireless network segments.
1.4	Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	ECS can enforce this important PCI requirement across all systems, including mobile and employee-owned computers. Systems attempting to access the network without personal firewall software that is both installed and operational can be denied access, quarantined, and forced to remediate the condition before being granted access.
<b>2.0</b>	<b>Do not use vendor-supplied defaults for system passwords and other security parameters</b>	
	<i>Malicious individuals (external and internal to a company) often use vendor default passwords and other vendor default settings to compromise systems. These passwords and settings are well known by hacker communities and are easily determined via public information.</i>	
	<b>Requirement</b>	<b>Relevant ECS Functionality</b>
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.	ECS helps to enforce configuration standards by identifying devices with security posture issues. ECS examines the device security configuration, anti-virus and anti-spyware signature files, and vulnerability status before granting network access to the device.  Devices found to not conform to the organization's security policy can be quarantined or automatically remediated.
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.	ECS utilizes SSL encryption between management workstations and all ECS appliances. SSH and/or SNMPv3 communication is supported between ECS appliances and network infrastructure devices

### Maintain a Vulnerability Management Program

<b>5.0</b>	<b>Use and regularly update anti-virus software or programs</b>	
	<i>Malicious software, commonly referred to as "malware"—including viruses, worms, and Trojans—enters the network during many business-approved activities including employees' e-mail and use of the Internet, mobile computers, and storage devices, resulting in the exploitation of system vulnerabilities. Anti-virus software must be used on all systems commonly affected by malware to protect those systems from current and evolving malicious software threats.</i>	
	<b>Requirement</b>	<b>Relevant ECS Functionality</b>
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers)	ECS enforces the presence of AV software on all network-attached systems, and it further ensures that the signature files and the AV executable are current, according to the policy established by the organization. Devices found to not conform to the defined security policy can be quarantined or automatically remediated.
5.1.1	Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	ECS greatly enhances the organization's ability to respond to this PCI provision by allowing active, policy-based reaction to the security posture of the device that is trying to access the network.
5.2	Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	ECS ensures that AV software is running, active, has current signature files, and is capable of creating audit event logs.

<b>6.0 Develop and maintain secure systems and applications</b>	
<p><i>Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed by vendor-provided security patches, which must be installed by the entities that manage the systems. All critical systems must have the most recently released, appropriate software patches to protect against exploitation and compromise of cardholder data by malicious individuals and malicious software.</i></p> <p><i>Note: Appropriate software patches are those patches that have been evaluated and tested sufficiently to determine that the patches do not conflict with existing security configurations. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques.</i></p>	
Requirement	Relevant ECS Functionality
<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>Note: An organization may consider applying a risk-based approach to prioritize their patch installations. For example, by prioritizing critical infrastructure (for example, public-facing devices and systems, databases) higher than less-critical internal devices, to ensure high-priority systems and devices are addressed within one month, and addressing less-critical devices and systems within three months.</p>	ECS queries the device security posture for all systems on the network before allowing access. Patch levels can be enforced, and a variety of actions can be undertaken when it is determined that a system does not conform to policy, including quarantine and proactive remediation.
6.3.2	Separate development/test, and production environments
	ECS uses VLANs and role-based access control to segregate user access, and can provide an effective mechanism to separate the development, test, and production environments within an organization.

**Implement Strong Access Control Measures**

<b>7.0 Restrict access to cardholder data by business need to know</b>	
<p><i>To ensure critical data can only be accessed by authorized personnel, systems and processes must be in place to limit access based on need to know and according to job responsibilities.</i></p> <p><i>"Need to know" is when access rights are granted to only the least amount of data and privileges needed to perform a job.</i></p>	
Requirement	Relevant ECS Functionality
7.1	Limit access to computing resources and cardholder information only to those individuals whose job requires such access.
7.1.1	Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities
7.1.2	Assignment of privileges is based on individual personnel's job classification and function
7.1.4	Implementation of an automated access control system
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. This access control system must include the following:
7.2.1	Coverage of all system components
7.2.2	Assignment of privileges to individuals based on job classification and function
7.2.3	Default "deny-all" setting

**PCI Requirements Mapping for Aruba Networks' Endpoint Compliance System(ECS)**

<b>8.0 Assign a unique ID to each person with computer access</b>		
<i>Assigning a unique identification (ID) to each person with access ensures that each individual is uniquely accountable for his or her actions. When such accountability is in place, actions taken on critical data and systems are performed by, and can be traced to, known and authorized users.</i>		
Requirement		Relevant ECS Functionality
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	ECS employs a seven point identity match including user name, user role, device name, MAC address, IP address, network access point, and time. The system also supports 802.1x, LDAP, and RADIUS authentication.
8.2	In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users:  <ul style="list-style-type: none"> <li>• Password or passphrase</li> <li>• Two-factor authentication (for example, token devices, smart cards, biometrics, or public keys)</li> </ul>	
8.3	Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Use technologies such as remote authentication and dial-in service (RADIUS); terminal access controller access control system (TACACS) with tokens; or VPN (based on SSL/TLS or IPSEC) with individual certificates.	
8.5.4	Immediately revoke access for any terminated users	
8.5.6	Enable accounts used by vendors for remote maintenance only during the time period needed	ECS can apply roles with limited network access privileges, including time restrictions.
8.5.16	Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users	The role-based access policies implemented within ECS can authenticate all access to certain network segments, and can additionally determine based upon policies and roles which users are even permitted to connect to the database or LAN segment containing cardholder data.

**Regularly Monitor and Test Networks**

<b>10.0 Track and monitor all access to network resources and cardholder data</b>		
<i>Logging mechanisms and the ability to track user activities are critical in preventing, detecting, or minimizing the impact of a data compromise. The presence of logs in all environments allows thorough tracking, alerting, and analysis when something does go wrong. Determining the cause of a compromise is very difficult without system activity logs.</i>		
Requirement		Relevant ECS Functionality
10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	ECS provides critical audit trails for all internal network access, showing what devices and users are connecting to what network resources throughout the internal network, and further showing any invalid access attempts for wired, wireless, and VPN network connections.
10.2	Implement automated audit trails for all system components to reconstruct the following events:	
10.2.1	All individual user accesses to cardholder data	ECS restricts and secures access to audit trails on the ECS platform. Log data can be archived for long term storage, and standards-based data export facilities are supported to allow log data to be exported to external systems for detailed forensic analysis and/or reporting.
10.2.3	Access to all audit trails	
10.2.4	Invalid logical access attempts	
10.2.5	Use of identification and authentication mechanisms	
10.3	Record at least the following audit trail entries for all system components for each event:	
10.3.1	User identification	
10.3.2	Type of event	
10.3.3	Date and time	
10.3.4	Success or failure indication	
10.3.5	Origination of event	
10.3.6	Identity or name of affected data, system component, or resource	
10.5	Secure audit trails so they cannot be altered.	
10.5.1	Limit viewing of audit trails to those with a job-related need.	
10.5.2	Protect audit trail files from unauthorized modifications.	

<b>11.0</b>	<b>Regularly test security systems and processes</b>	
	<i>Vulnerabilities are being discovered continually by malicious individuals and researchers, and being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security controls continue to reflect a changing environment.</i>	
	Requirement	Relevant ECS Functionality
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).  Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by Payment Card Industry Security Standards Council (PCI SSC). Scans conducted after network changes may be performed by the company's internal staff.	ECS does not replace quarterly scans by Qualified Data Security scanning firms certified by the PCI Security Standards Council. The ECS agent significantly augments this, however, by scanning devices attempting to connect to the network much more frequently, and quarantining devices or remediating issues as they arise.
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.	While ECS is not itself an intrusion detection or prevention system, it integrates with third-party IDS/IPS systems. It can take their alarms and alerts as inputs for automated security policy decision making, and then enforce policy at the edge of the network.

**Maintain an Information Security Policy**

<b>12.0</b>	<b>Maintain a policy that addresses information security for employees and contractors</b>	
	<i>A strong security policy sets the security tone for the whole company and informs employees what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it. For the purposes of this requirement, "employees" refers to full-time and part-time employees, temporary employees and personnel, and contractors and consultants who are "resident" on the company's site.</i>	
	Requirement	Relevant ECS Functionality
12.1	Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	Establishing policy is clearly a process issue. However, ECS greatly facilitates enforcing many of the policies identified in Requirement 12, particularly those that relate to internal and external network access control, as specified. For example, requirements 12.3.6 and 12.5.5 are policies that are difficult to enforce without a network access control solution such as ECS.
12.2	Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	
12.3	Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal data/digital assistants (PDAs), e-mail usage and Internet usage) to define proper use of these technologies for all employees and contractors. Ensure these usage policies require the following:	
12.3.2	Authentication for use of the technology	
12.3.6	Acceptable network locations for the technologies	
12.3.9	Activation of remote access technologies for vendors only when needed by vendors, with immediate deactivation after use	
12.5.4	Administer user accounts, including additions, deletions, and modifications	
12.5.5	Monitor and control all access to data.	

**Summary**

The PCI Data Security Standard has evolved considerably and many of the additions to the standard as it moved from version 1.0 to version 1.1 required greater control over access to internal network resources, particularly for systems that house cardholder data. These requirements are difficult and, in many cases, impossible to achieve using either traditional firewall technology or host-based identity management or access control systems. Version 1.2 of the standard added significant new requirements regarding access control, web application security, and it changed a number of requirements in the area of wireless security.

Network access control (NAC) solutions emerged several years ago to address new threats to internal networks. Products like Aruba Networks's ECS provide the robust identity management, endpoint compliance, and usage policy enforcement capabilities that are needed by retailers and others in the payment card processing chain to not only comply with PCI, but to more effectively secure their networks.

ECS greatly enhances the ability of payment card industry participants to comply with PCI DSS, addressing nine of the twelve high-level PCI DSS requirements.

## About Compliance Research Group

Compliance Research Group is a consulting and research firm focused on these areas:

- IT Risk
- Compliance
- IT Security

We conduct end-user research into various aspects of risk, compliance, and security. We also research and provide analysis on the supply side of the risk, compliance, and security markets. Compliance Research Group provides consulting services for organizations in these areas as well. Our focus is on helping end users, vendors, and channel participants to better understand the critical issues and requirements that exist in these dynamic markets. The principals of Compliance Research Group have a deep technical understanding of the risk, compliance, and security markets and technologies. Our analysts and consultants hold multiple CISSP and GIAC certifications, including GSEC-Gold and GCFW-Gold certifications from SANS/GIAC.

Compliance Research Group is proud to have been able to partner with other leading organizations in the security, risk, and compliance areas, including the SANS Institute, Logical Security, and The Open Group. We maintain active memberships in ISC(2) and ISSA. For more information please visit [www.complianceresearchgroup.com](http://www.complianceresearchgroup.com).

## About Aruba Networks

People move. Networks must follow. Aruba securely delivers networks to users, wherever they work or roam. Our unified mobility solutions include Wi-Fi networks, identity-based security, remote access and cellular services, and centralized multi-vendor network management to enable the Follow-Me Enterprise that moves in lock-step with users:

- Follow-Me Connectivity: Adaptive 802.11a/b/g/n Wi-Fi networks optimize themselves to ensure that users are always within reach of mission-critical information
- Follow-Me Security: Identity-based security assigns access policies to users, enforcing those policies whenever and wherever a network is accessed
- Follow-Me Applications: Remote access solutions and cellular network integration ensure uninterrupted access to applications as users move
- Follow-Me Management: Multi-vendor network management provides a single point of control while managing both legacy and new wireless networks from both Aruba and its competitors

The cost, convenience, and security benefits of our unified mobility solutions are fundamentally changing how and where we work. Listed on the NASDAQ and Russell 2000 Index, Aruba is based in Sunnyvale, California, and has operations throughout the Americas, Europe, Middle East, and Asia Pacific regions. To learn more, visit Aruba at <http://www.arubanetworks.com>.

## Appendix A

### Summary of Significant Changes, PCI DSS 1.1 to 1.2

The most recent version of the PCI Data Security Standard, version 1.2, introduced a number of major changes. The most significant changes in this version revolve around access control, application security, and wireless networks.

Requirements	Key Changes in PCI DSS v1.2
1. Install and maintain a firewall configuration to protect cardholder data	Minor changes - clarification, restructuring some requirements, and changes to requirements language. Added testing procedures for requirements.
2. Do not use vendor-supplied defaults for system passwords and other security parameters	Minor changes - clarification, restructuring some requirements, and changes to requirements language. Added testing procedures for requirements.
3. Protect stored cardholder data	Minor changes - clarification, restructuring some requirements, and changes to requirements language and testing procedures. Added testing procedures for requirements.
4. Encrypt transmission of cardholder data across open, public networks	<b>Major changes</b> - changed requirements in 4.1.1 to eliminate WEP as an acceptable encryption protocol over time. Clarification, restructuring some requirements, and changes to requirements language. Added testing procedures for requirements.
5. Use and regularly update anti-virus software	<b>Major changes</b> - expanded language and scope from "anti-virus" to all types of malicious software. Clarification, restructuring some requirements, and changes to requirements language and testing procedures. Added testing procedures for requirements.
6. Develop and maintain secure systems and applications	<b>Major changes</b> - significant changes to enable secure application development. Integrates the OWASP top-10 application vulnerabilities as guidance, and requires either a regular web application vulnerability assessment, or the use of a web application firewall (or both).
7. Restrict access to cardholder data by business need-to-know	<b>Major changes</b> - version 1.1 had just two vague and high level requirements (7.1 and 7.2) related to the objective. Version 1.2 added a total of eight sub-requirements (7.1.1 through 7.1.4, plus 7.2.1 through 7.2.4) which specify implementation of an automated access control system, and that describe the use of role-based access control in achieving the objective.
8. Assign a unique ID to each person with computer access	Minor changes - clarification, restructuring some requirements, and changes to requirements language and testing procedures. Added testing procedures for requirements.
9. Restrict physical access to cardholder data	Minor changes - clarification, restructuring some requirements, and changes to requirements language and testing procedures. Added testing procedures for requirements.
10. Track and monitor all access to network resources and cardholder data	Minor changes - clarification, restructuring some requirements, and changes to requirements language and testing procedures. Added testing procedures for requirements.
11. Regularly test security systems and processes	<b>Major changes</b> - added test procedures related to wireless network usage (11.1.a, b, and c) that require using a wireless analyzer, ensuring that a wireless IDS/IPS is generating alerts, and that incident response addresses unauthorized wireless device use. Clarification, restructuring some requirements, and changes to requirements language and testing procedures. Added testing procedures for requirements.
12. Maintain a policy that addresses information security	<b>Major changes</b> - expanded language in requirements from "modems" to "remote access technologies". Changed language from "third parties" to "service providers". Clarification, restructuring some requirements, and changes to requirements language and testing procedures. Added testing procedures for requirements.

The changes to Requirement 7 are particularly significant from a network security standpoint, as they are really best addressed at the network level through the use of Network Access Control technology like ECS. In addition, the addition of test procedures related to detecting the unauthorized use of wireless access argues strongly for using a system like ECS, which provides a "get out, stay out" capability for unauthorized devices attempting to access the network.

## Appendix B

### The Payment Card Industry Data Security Standard

In 2004, the VISA Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) Program requirements were incorporated into an industry standard known as the Payment Card Industry (PCI) Data Security Standard (DSS). This standard resulted from collaboration between Visa and MasterCard to create common industry security requirements. As previously mentioned, the standard has evolved from 1.0 to 1.1, and a new and updated version is expected in fall, 2008.

PCI DSS compliance is required of all merchants and service providers that store, process, or transmit cardholder data. The program applies to all payment channels, including retail, mail/telephone order, and e-commerce. It is important to note that the five major payment card brands (VISA, Mastercard, Diners Club, American Express, and JCB) all require PCI DSS compliance. The details regarding specifics of compliance, including dates and fines for non-compliance are managed by the individual brands themselves.

### Merchants

A merchant is any entity, such as a retail store, that processes credit card transactions. As of July 18, 2006, merchant level definitions for PCI DSS have changed. The current merchant levels are:

Merchant Level	Description
1	Any merchant - regardless of acceptance channel - processing over 6,000,000 transactions per year. Any merchant that has suffered a hack or an attack that resulted in an account data compromise. Any merchant identified by any other payment card brand as Level 1.
2	Any merchant - regardless of acceptance channel - processing 1,000,000 to 6,000,000 transactions per year.
3	Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.
4	Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants - regardless of acceptance channel - processing up to 1,000,000 transactions per year.

In addition to adhering to the PCI DSS, compliance validation is required for Level 1, Level 2, and Level 3 merchants, and may be required for Level 4 merchants. These validation requirements for VISA are shown below. For all merchants, the due dates for compliance have passed and all merchants are now required to be in compliance.

Merchant Level	Validation Action	Validated By
1	Annual On-site PCI Data Security Assessment Quarterly Network Scan	Qualified Data Security Company or Internal Audit if signed by Officer of the company Qualified Independent Scan Vendor
2	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan	Merchant Qualified Independent Scan Vendor
3	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan	Merchant Qualified Independent Scan Vendor
4	Annual PCI Self-Assessment Questionnaire Quarterly Network Scan	Merchant Qualified Independent Scan Vendor

### Service Providers

Service providers are organizations that process, store, or transmit cardholder data on behalf of members, merchants, or other service providers. Service provider levels are:

Merchant Level	Description
1	All VisaNet processors (Member and nonmember) and all payment gateways. VisaNet refers to the systems and services through which Visa delivers authorization, clearing, and settlement services for its members.
2	Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 credit card transactions annually.
3	Any service provider that is not in Level 1 and stores, processes, or transmits less than 1,000,000 credit card transactions annually.

---

**PCI Requirements Mapping for Aruba Networks' Endpoint Compliance System(ECS)**

---

In addition to adhering to the PCI Data Security Standard, compliance validation is required for all service providers. These validation requirements are defined below:

Merchant Level	Validation Action	Validated By
1	Annual On-site PCI Data Security Assessment	Qualified Data Security Company
	Quarterly Network Scan	Qualified Independent Scan Vendor
2	Annual On-site PCI Data Security Assessment	Qualified Data Security Company
	Quarterly Network Scan	Qualified Independent Scan Vendor
3	Annual PCI Self-Assessment Questionnaire	Service Provider
	Quarterly Network Scan	Qualified Independent Scan Vendor

**DISCLAIMER**

This document provides general information about personal privacy and compliance initiatives in North America. It is intended to be used for resource and reference purposes only and does not constitute legal advice, nor should it be construed as providing any warranties or representations with respect to the products and/or services discussed herein. Readers of this paper are encouraged to speak with their legal counsel to understand how the general issues discussed above apply to their particular circumstances. Compliance Research Group and Aruba Networks disclaim any and all liability for damages, costs, lost profits, fines, fees or financial penalties of any kind suffered by any party acting or relying on the general information contained herein.