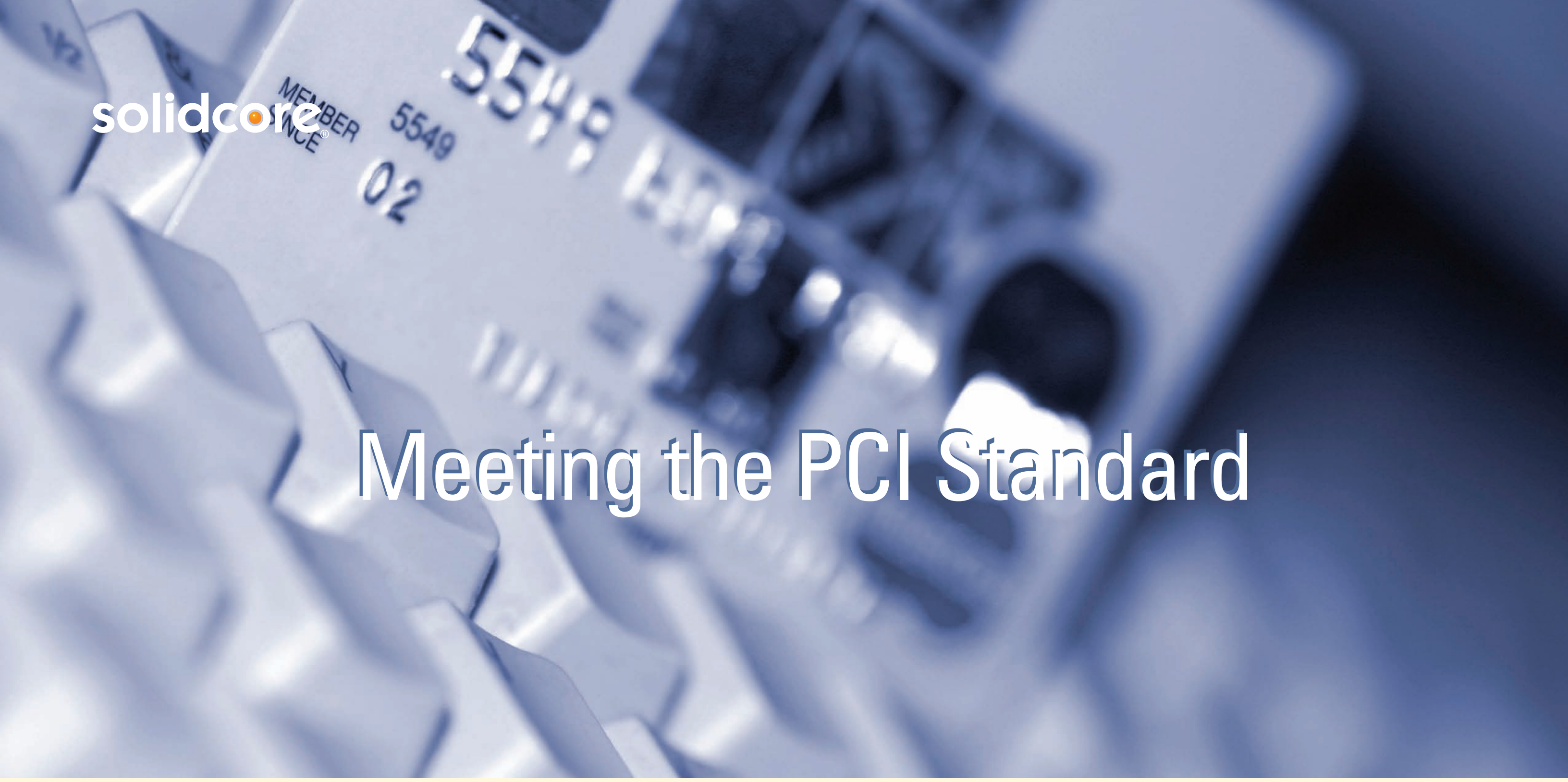


Meeting the PCI Standard

Solidcore Systems, Inc. delivers innovative software solutions that provide capabilities to cost-effectively gain control of its customers IT infrastructure and realize immediate and tangible value in support of change control, compliance, and security. These benefits enable retailers and other credit card processing entities to significantly reduce the cost of complying with the Payment Card Industry Data Security Standard (PCI DSS). This white paper describes how Solidcore automates data collection for, and validation and enforcement of, IT controls in the PCI Data Security Standard.

Overview

Identity theft and credit card fraud is a large and growing problem. The Federal Trade Commission estimates that almost 10 million consumers were affected last year, at a cost of close to $50 billion. In order to combat this growing menace, Visa, MasterCard, American Express, Diners Club, Discover and other major credit card providers have joined together to introduce a compliance standard - the Payment Card Industry (PCI) Data Security Standard. The standard unites and supersedes the individual compliance standards such as Visa's CISP and MasterCard's SDP standards.

This program is intended to protect cardholder data wherever it resides, ensuring that members, merchants and service providers maintain the highest levels of information security. The PCI standard came into effect on December 14th, 2004, and merchants and service providers were originally required to be PCI compliant by June 30th, 2005. The PCI Security Standards Council released DSS standard version 1.1 in September 2006 to tighten certain requirements and clarify ambiguous ones in the 1.0 release. As of January 1, 2007 all new certifications and newly initiated re-certifications are to be based on DSS version 1.1.

Like all compliance programs, PCI consists of two separate components, both of which must be implemented in order to be PCI compliant:

1. Compliance with PCI requirements, and
2. Validation of PCI compliance

Each of these components is discussed in more detail below.

PCI Requirements

The PCI DSS mandates that all merchants follow the twelve requirements, listed in the following table. In addition, there is an implicit thirteenth requirement to verify compliance with the PCI DSS – often overlooked but an integral part of any PCI compliance program.

PCI Requirements	
1	Install and maintain a firewall configuration to protect data
2	Do not use vendor-supplied defaults for passwords and security parameters
3	Protect stored cardholder data
4	Encrypt transmission of cardholder data and sensitive information across public networks
5	Use and regularly update anti-virus software
6	Develop and maintain secure systems and applications
7	Restrict access to data by business "need to know"
8	Assign unique ID to each person with computer access
9	Restrict physical access to cardholder data
10	Track and monitor all access to network resources and cardholder data
11	Regularly test security systems and processes
12	Maintain a policy that addresses information security

The requirement to verify PCI compliance is discussed in more detail in the next section.

PCI Compliance

Credit card issuers divide its merchants into four levels based on the number of transactions processed every year, as shown in the table below.

Merchant Level	No. of transactions
Level 1	> 6 million
Level 2	150,000 – 6 million
Level 3	20,000 – 150,000
Level 4	< 20,000

Each level is subject to a different set of compliance activities, with the strictest rules applied to level 1 merchants. In addition to transaction volume, any merchant that suffered a hack or an attack that resulted in account data compromise will automatically be required to meet level 1 compliance requirements. Further, the card issuer may, at their discretion, require any merchant in its network to meet level 1 requirements. In view of this, Solidcore's recommended best practice is to follow level 1 requirements regardless of activity level. This white paper will focus on the compliance validation activities required of level 1 merchants.

Participating merchants must pay for their own PCI compliance assessment, and the cost of compliance depends on the extent to which they are already in a compliant state. A level 1 merchant needs to submit an annual **Report on Compliance**, validated by an approved independent auditor, or by an internal audit department, provided that a letter signed by an executive-level officer of the company accompanies the report.

For level 1 merchants required to undergo an annual compliance review, the scope of validation is focused on systems or system components related to authorization and settlement where cardholder data is processed, stored, or transmitted.

Solidcore Enforcement: A Powerful Differentiator

In addition to words like "track" and "monitor", the PCI DSS and other regulatory standards use words like "restrict", "deny", "disable", "limit", "protect", and "ensure" to describe specific controls that apply to infrastructure components (servers, applications, network devices, data sets, etc.) that are included in or connected to the cardholder environment.

Solidcore S3 Control is a powerful tool to track changes and gain visibility across your infrastructure to identify hot spots, unauthorized activity and risky behavior. These capabilities allow you to drive accountability into your change processes and reduce mean-time-to-repair (MTTR) problems. But that is just the beginning. More than simply tracking changes, Solidcore alerts and prevents unauthorized changes before they happen. This is a powerful differentiator and eliminates exposures to various risks between the times a violation is detected and communicated; root cause is determined; a fix is proposed, assigned and tested; and finally, the problem is remediated on the production system.

S3 Control eliminates the possibility for any user or process to access or modify selected files associated with an application, OS, utility or other configurations. This restriction can be configured to be relaxed if and only if

1. a specific, authorized program is used to make the change – e.g. using an automated patch management, provisioning, or remediation product;
2. a change request has been approved in an enterprise change management system; and
3. the change occurs during an approved maintenance time window.

S3 Control also prevents unauthorized processes or applications from starting on designated systems.

These capabilities eliminate risks to system or service stability, performance problems, and downtime due to viruses, unauthorized actions and rogue user activity. Solidcore brings mean-time-to-repair to zero by preventing erroneous change . In this way, Solidcore S3 Control is the only solution capable of enforcing many of the requirements described in the PCI DSS and many other regulatory or best-practice control frameworks.

Addressing the PCI Requirements: The Solidcore S3 Control Solution

Solidcore provides categorical oversight and control over the IT infrastructure, enabling retailers and other merchants to fulfill PCI requirements and validate and enforce PCI compliance in an efficient and cost-effective manner. The section below describes Solidcore S3 Control's capabilities for each of the major requirements in the PCI DSS.

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

The controls in this section are focused on establishing approved configurations, and developing and enforcing change policies for firewalls that protect cardholder data.

Solidcore S3 Control provides real-time change detection, detailed device configuration history and audit trails providing information on who changed what and when, and quick restoration to trusted configurations.

Requirement 2: Do not use vendor-supplied defaults for passwords and security parameters

The controls in this section require the elimination of vendor-supplied default passwords on firewalls, routers and wireless routers. Additionally, they recommend implementing only one primary function on servers and disabling/removing unnecessary services and scripts.

Solidcore S3 Control identifies breaches in the security (e.g. password) policies adopted by your organization using built-in reports that identify non-complying configurations in your databases, and ensures that security configurations and access control lists do not change outside of an approved process. Solidcore S3 Control greatly reduces exposure to availability and stability problems by validating and enforcing that designated servers provide one and only one primary function. S3 Control audits the removal of applications, utilities, and scripts; tracks and alerts on initiation of rogue processes or applications; and disables installation of new applications.

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

The PCI DSS recommends keeping storage of cardholder data to a minimum via a data retention and disposal policy.

Solidcore S3 Control monitors and reports on deletion of files and database tables, and validates those actions when performed based on a change request. S3 Control can be used to validate your cardholder data retention policies by providing the evidence of retention or removal of this data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks

The PCI DSS recommends encrypting cardholder data as a means of protecting it during transit across any public network like the internet, WiFi, GSM or GPRS.

S3 Control's capabilities ensure encryption of cardholder data by tracking and preventing changes to critical security device configurations, application configuration files or registry entries. S3 Control provides powerful change and configuration control over network devices and system configuration files.

Maintain a Vulnerability Management Program

Requirement 5: Use and update anti-virus software

The PCI DSS requires that anti-virus software be used on all systems commonly affected by viruses to protect them from malicious software.

Solidcore S3 Control tracks changes to anti-virus signature and configuration files, detects unauthorized changes or attempts to uninstall the anti-virus software, and can validate changes via an approved change request or maintenance window. S3 Control ensures that only an authorized process can update the anti-virus signature file with a new virus definition adding enforcement protection to your critical security mechanisms.

Requirement 6: Develop and maintain secure systems and applications

A large part of the PCI standard requires that:

1. all system and software configuration changes follow approved change control procedures,
2. security patches are performed in a timely manner, and
3. those changes and patches are tested in a separate environment prior to being deployed into production.

Applying sound change management practices is critical to maintaining the stability and security of IT services for any enterprise, especially those that have customers that rely on those services. Solidcore S3 Control automates the tracking and control of changes in real-time, providing visibility, accountability and enforcement for enterprises at any level of process maturity.

- **Visibility**: Real-time detection of all change activity on in-scope systems and applications enables the enterprise to gain a comprehensive understanding of how change is occurring in their environment, where it is occurring, and by whom. Audit trails provide evidence of data retention and removal, user account changes, and security patches, all of which are key to this section of the PCI DSS.

- **Accountability**: Solidcore S3 Control validates that security patches and configuration changes have been applied according to approved change procedures. This is done by correlating change actions to approved change requests in your enterprise change management system, a change manifest or to an approved maintenance window. S3 Control provides additional validation by automatically correlating changes that have been applied and tested in a development environment to those deployed into production, identifying untested patches when they occur to satisfy another key control in the PCI DSS.

- **Enforcement**: Solidcore S3 Control is differentiated from any other automated solution in its ability to lock critical application, system or data files. Files can be locked-down such that no user or process can alter them unless explicitly allowed via an approved change request from a change management system, or via a specified automated provisioning or patching application. This provides S3 Control customers with the utmost control over critical business systems and applications, eliminating legacy methods of remediating erroneous changes in reaction to a service degradation ot outage.

Implement Strong Access controls

Requirement 7: Restrict access to cardholder data by business need-to-know

The PCI DSS requires access restrictions on computing resources and cardholder data to only those who have a need based on job description and that security settings on share resources are set to “deny all” by default.

S3 Control tracks access to sensitive data stored in databases by user, providing an audit trail of all access that data. It also monitors changes to access control lists in Active Directory to capture the addition of any new user or changes to user privileges. Computing resources monitored include databases, access control lists, firewalls and other network equipment.

Requirement 8: Assign a unique ID to each person with computer access

PCI requires that the addition, deletion and modification of user IDs must be controlled, and that certain account settings (e.g. password policies) are employed for all users by default with unused or terminated users accounts disabled in a timely manner.

Solidcore S3 Control tracks changes to user IDs, credentials and privileges and has built-in reports to identify weak passwords, inactive user IDs and unsuccessful login attempts. When password files are used, S3 Control can be configured to proactively prevent any change except when an authorized process or approved change ticket exists. These controls and reports strengthen existing access control systems and processes reducing risk of malicious behavior inside an organization.

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data

PCI requires tracking and generation of audit trails for actions of users with elevated privileges (e.g. root user) and specifies required content for audit entries. In addition, it requires that audit logs are protected and cannot be compromised.

Solidcore S3 Control provides strong coverage of Requirement 10 as it is the independent mechanism that generates and logs activities against network resources, cardholder data and systems. Collected event data is secured and protected using Oracle database security mechanisms and S3 Control capabilities, rendering it tamper-proof. Other in-scope audit logs or files that contain event data that must be secured can be monitored for access, changes, or can be locked down to prevent all changes except those executed by the approved process or application.

Requirement 11: Regularly test security systems and processes

PCI requires that file integrity monitoring software be deployed on critical data, operating system and application files. These files are typically those that do not change as a part of normal operations and when they do, typically represent a material change to the operation, performance or configuration of the system or application.

Solidcore S3 Control provides tracking, validation and enforcement of change policies and controls for files of any type. S3 Control tracks modification of files and validates changes against those first executed in the test environment or those approved by change requests. Additionally, it can be configured to restrict file modifications when no matching change request exists or when an unapproved process attempts to modify the file. Pre-defined filter profiles for supported operating systems and applications are provided out-of-the-box for faster deployments in your environment.

Requirement 12: Maintain a policy that addresses information security for employees and contractors

PCI requires the implementation of an incident response plan to ensure preparation to respond to a system breach including alerts from file integrity monitoring software.

Solidcore S3 Control provides a real-time detection capability vs. snapshot-based systems and alerts appropriate personnel when a critical system or application configuration is modified. If desired, S3 Control can go a step beyond this by avoiding the possibility of this kind of breach altogether using its enforcement capabilities.

The table below provides some key Solidcore S3 Control capabilities against specific requirements in the PCI DSS.

PCI Requirement		Solidcore S3 Control Automation
1	Install and maintain a firewall configuration to protect data	Validate configuration, monitor drift, validate change
1.1.1	Establish firewall configuration standards that includes… A formal process for approving and testing all external network connections and changes to the firewall configuration	- Tracks changes on network devices like routers, switches, firewalls, etc in real-time - Out-of-the-box templates provide common rules and S3 Control **enforcement** ensures that these rules are not changed - Configurations are versioned to allow administrators to revert to a known working version
1.1.8	Establish firewall configuration standards that includes… Quarterly review of firewall and router rule sets... and configuration standards for routers. Build a firewall configuration that denies all traffic from "untrusted" networks and hosts...	- Generates quarterly reports, and distributes accordingly showing devices with deviations from accepted configuration standards - Maintains startup configurations for comparison against running versions
1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.5, 1.3.6, 1.3.7, 1.4.2	Build a firewall configuration that restricts connections… restricts inbound traffic…, disallows internal addresses to pass…, implements stateful inspection…, restricts inbound and outbound traffic…, …synchronizes router configurations…, deny traffic by default…, … restrict outbound traffic from payment card apps…	- Performs regular scan of firewalls and devices - Detects deviations from accepted configuration standard - Rollback to approved or previous configuration - **Enforces** integrity of laptop firewall software by locking configuration files to changes

PCI Requirement		Solidcore S3 Control Automation
2	Do not use vendor-supplied defaults for passwords and security parameters	Validate configuration, monitor drift, **enforce** single function server
2.1, 2.1.1	Always change vendor-supplied defaults before installing a system on the network (e.g. passwords, SNMP community strings, elimination of unnecessary accounts, WEP keys, SSID, SSID broadcast, enable WPA and encryption, etc.)	- Validates new device configurations against approved standards - Monitors and tracks changes by change type, device and user
2.2.1, 2.2.2, 2.2.3, 2.2.4	Implement only one primary function per server (for example, web servers, database servers, and DNS should be implemented on separate servers), disable all unnecessary and insecure services and protocols…, Configure system security parameters to prevent misuse, Remove all unnecessary functionality, such as scripts, drivers…	- Provides approved run-time configuration for servers - **Enforces** run-time configuration disallowing installation of new applications, utilities or services - Tracks changes to system configurations - Tracks removal of applications, utilities, drivers, etc.
3	Protect stored cardholder data	Validate data retention and removal, track key management, validate key changes
3.1	…Develop a data retention and disposal policy. Limit storage amount and retention time…	Tracks, validates and reports file and DB table content deletion
3.6.4, 3.6.5, 3.6.7, 3.6.7	Implement key management including… periodic changing… destruction of old keys… prevention of unauthorized substitution… replacement of compromised keys	- Tracks and validates key changes - Tracks, validates and **enforces** key file deletion, unauthorized modification
4	Encrypt transmission of cardholder data and sensitive information across public networks	Validate encryption configurations on firewalls and applications, monitor drift, validate change, **enforce** configuration integrity
4.1, 4.1.1	Use strong cryptography to safeguard cardholder data transmission… encrypt the transmissions by using WPA or WPA2, IPSEC VPN, or SSL/TLS. … Rotate WEP keys…, restrict access based on MAC address…	- Validates new network device configurations against approved standards - Tracks and **enforces** integrity of OS or application configuration files that contain encryption related settings - Tracks changes by object, type, device and user
5	Use and regularly update anti-virus software	Validate changes to anti-virus software, **enforce** anti-virus application file integrity
5.1, 5.2	Deploy anti-virus software on all systems commonly affected by viruses (particularly personal computers and servers). Ensure that all anti-virus mechanisms are current, actively running, and capable of generating audit logs.	- Tracks and validates changes to anti-virus software - **Enforces** change policy for patches by approved updater, request or maintenance window - **Prevents** uninstallation of anti-virus software
6	Develop and maintain secure systems and applications	Validate changes against those tested, audit activities of users across environments, maintain versions for rollback
6.3.1, 6.3.2, 6.3.3	Test all security patches and system and software configuration changes before deployment… separate test, development and production… and… separation of duties	- Tracks changes to all systems and software and automatically reconciles with approved change requests - Validates production changes against those tested in development/QA environments - Tracks changes by user to provide evidence of separation of duties across environments
6.4.4	…follow change control procedures including… testing of operational functionality… back-out procedures	- Tracks and automatically reconciles and validates changes against enterprise change management (CM) system requests - Maintains archive version of configuration files for easy roll-back
7	Restrict access to data by business "need to know"	Track, validate and enforce data access
7.1, 7.2	Limit access to computing resources and cardholder information…, Establish a mechanism … that restricts access ...and is set to "deny all" unless specifically allowed.	- Tracks access to data in databases by user - Tracks changes to access control lists (file or Active Directory) like new users or modified attributes - **Enforces** change policy on files that store local user accounts

PCI Requirement		Solidcore S3 Control Automation
8	Assign unique ID to each person with computer access	Track changes to ACLs, track deviations from best-practice configuration
8.5.1, 8.5.3 - 8.5.6, 8.5.8 - 8.5.15	Control addition, deletion, and modification of user IDs, credentials..., set first-time passwords and change immediately…, revoke access for terminated users…, remove inactive accounts, enable for remote maintenance during specific time period, do not use shared accounts, change passwords every 90 days, require minimum length with numeric and alphabetic characters, do not allow repeated passwords, set lockout duration.., set idle timeout.., etc.	- Tracks user account adds, deletes or attribute modifications (Active Directory, LDAP) - Reconciles and validates user account adds, deletes or modifications against CM requests - Tracks changes to local password files - **Enforces** change policy on files that store local user accounts
9	Restrict physical access to cardholder data	N/A
10	Track and monitor all access to network resources and cardholder data	Track access to data, **enforce** access to and modification of audit trails, retain audit data
10.1, 10.2.1, 10.2.2, 10.2.3, 10.2.7, 10.3, 10.5.1, 10.5.2, 10.5.5. 10.7	Establish a process for linking all access to system components (especially access done with root) to each individual user, Implement automated audit trails for…user accesses to cardholder data, actions taken by any individual with root or administrative privileges, Access to all audit trails, Record the following audit trail entries for each event: UID, type, time, etc. Secure audit trails, limit viewing, protect from unauthorized modifications, use file integrity monitoring and change detection on logs, retain audit trail history...	- Tracks all change and events by user - original user if "su root" is used - Tracks all access to sensitive data in your databases - Tracks and maintains audit records with event type, user, timestamp, device **Enforces** third-party log file integrity so only the authorized process can update the log **Enforces** integrity of S3 Control event data rendering tamper-proof
11	Regularly test security systems and processes	Track and **enforce** system and application file integrity
11.4, 11.5	Use network intrusion detection systems, host-based intrusion detection systems, and intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date, Deploy file integrity monitoring software to alert personnel to unauthorized modification of critical system or content files… Other critical files, such as those for custom applications, must be evaluated and defined…	- Tracks all activity against critical resources, applications, operating systems, databases and network devices - Tracks modifications to critical files - Validates changes to critical resources - **Enforces** file integrity
12	Maintain a policy that addresses information security	Track access to data, **enforce** write access to and modification of sensitive data (file-based)
12.5.2, 12.5.5, 12.9.5	Monitor, analyze and distribute security alerts, Monitor and control all access to data, Implement an incident response plan to include alerts from file integrity monitoring software.	- Generates e-mail and SNMP trap alerts for all types of tracked events including file integrity breaches - Tracks access to data stored in databases by user - **Enforces** write access to file-based data

Real World Examples and Reports

Solidcore provides evidence of PCI Compliance

The goal of auditing, validating and, in some cases, automatically enforcing IT controls specified in the PCI DSS is not only to ensure that your systems and data are always in compliance, but also to be able to readily provide evidence of compliance to management and auditors. That evidence is summarized in out-of-the-box reports that demonstrate PCI compliance, thus reducing the cost of PCI compliance verification.

Below are real-world examples of reports that provide a view into the enterprise's level of compliance for individual PCI controls:

PCI Control Requirement: Section 1.3.6

Description: Securing and synchronizing router configuration files. For example, running configuration file (for normal functioning of the routers) and start-up configuration files (when machines are rebooted), should have the same secure configuration.

Solidcore Automation: Solidcore S3 Control tracks network device configuration changes in real-time and generates an alert when any mismatch between running configurations and the specified baseline occurs. The display below shows the dashboard view of this type of PCI requirement violation.

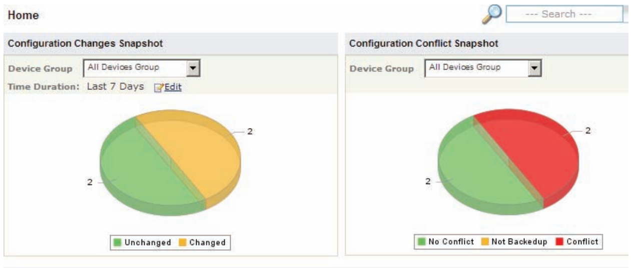
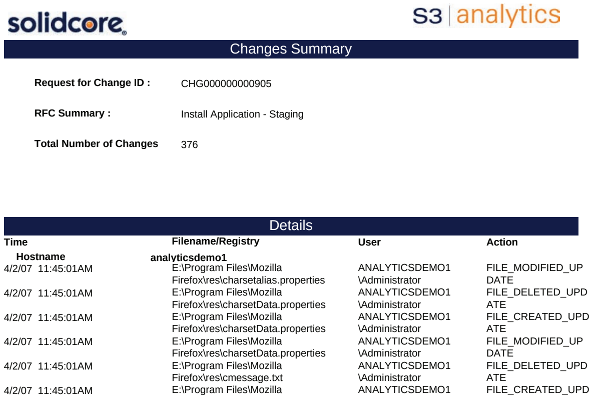


Fig 1: Dashboard shows that two devices have conflicting (different) startup and running configurations.

PCI Control Requirement: Section 6.4

Description: Follow change control procedures for all system and software configuration changes.

Solidcore Automation: Solidcore S3 Control integrates with enterprise change management systems like BMC Remedy and HP ServiceCenter. The software automatically reconciles change activity to approved change requests, and generates an audit trail that is appended to a correlated request. Changes that cannot be reconciled to an approved request are flagged as unauthorized violations of this PCI DSS requirement.


solidcore
S3 | analytics

Changes Summary

Request for Change ID :	CHG000000000905
RFC Summary :	Install Application - Staging
Total Number of Changes	376

Details

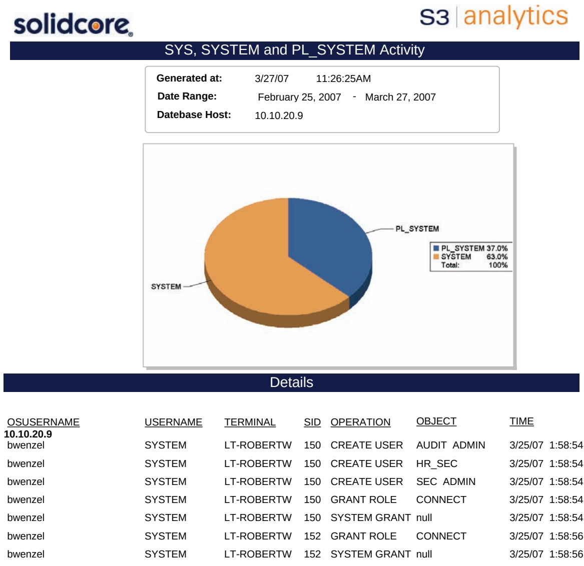
Time	Filename/Registry	User	Action
Hostname	**analyticsdemo1**		
4/2/07 11:45:01AM	E:\Program Files\Mozilla Firefox\res\charsetalias.properties	ANALYTICSDEMO1 \Administrator	FILE_MODIFIED_UPDATE
4/2/07 11:45:01AM	E:\Program Files\Mozilla Firefox\res\charsetData.properties	ANALYTICSDEMO1 \Administrator	FILE_DELETED_UPDATE
4/2/07 11:45:01AM	E:\Program Files\Mozilla Firefox\res\charsetData.properties	ANALYTICSDEMO1 \Administrator	FILE_CREATED_UPDATE
4/2/07 11:45:01AM	E:\Program Files\Mozilla Firefox\res\charsetData.properties	ANALYTICSDEMO1 \Administrator	FILE_MODIFIED_UPDATE
4/2/07 11:45:01AM	E:\Program Files\Mozilla Firefox\res\cmessage.txt	ANALYTICSDEMO1 \Administrator	FILE_DELETED_UPDATE
4/2/07 11:45:01AM	E:\Program Files\Mozilla	ANALYTICSDEMO1	FILE_CREATED_UPD

Fig 2. This auto-generated report provides a manifest of all changes associated with an approved change request

PCI Control Requirement: Section 10.1

Description: Establish a process for linking all access to system components (especially access done with administrative privileges) to each individual user.

Solidcore Automation: Solidcore S3 Control tracks change information in real-time, including the six primary aspects of change (who, what, when, where, why and how). This information is used to create audit trails and exception reports. Fig 3. shows a report detailing all changes made by the 'SYS', 'SYSTEM' or 'PL_SYSTEM' users on an Oracle database linking it to the actual user who made the change (bwenzel). Fig 4. shows that two users have performed the maximum number of changes on the servers under consideration.



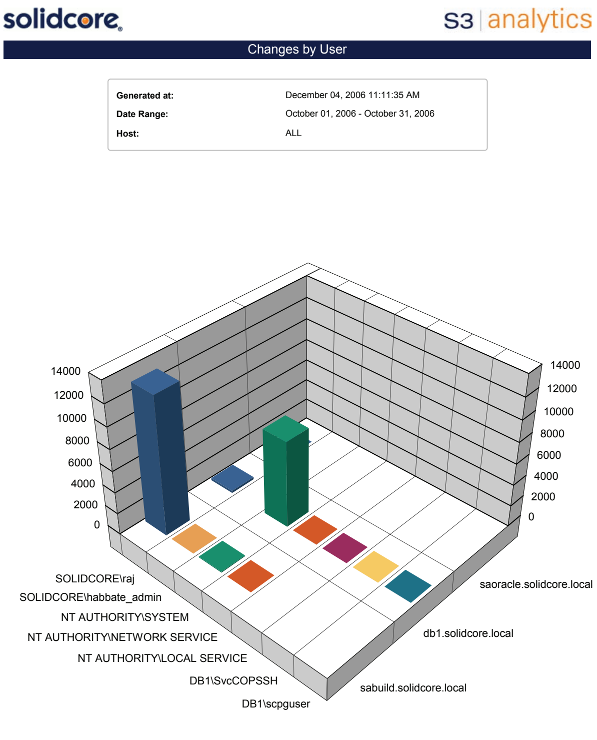
SYS, SYSTEM and PL_SYSTEM Activity

Generated at:	3/27/07	11:26:25AM
Date Range:	February 25, 2007 -	March 27, 2007
Datebase Host:	10.10.20.9	

Details

OSUSERNAME	USERNAME	TERMINAL	SID	OPERATION	OBJECT	TIME
10.10.20.9						
bwenzel	SYSTEM	LT-ROBERTW	150	CREATE USER	AUDIT ADMIN	3/25/07 1:58:54PM
bwenzel	SYSTEM	LT-ROBERTW	150	CREATE USER	HR_SEC	3/25/07 1:58:54PM
bwenzel	SYSTEM	LT-ROBERTW	150	CREATE USER	SEC ADMIN	3/25/07 1:58:54PM
bwenzel	SYSTEM	LT-ROBERTW	150	GRANT ROLE	CONNECT	3/25/07 1:58:54PM
bwenzel	SYSTEM	LT-ROBERTW	150	SYSTEM GRANT	null	3/25/07 1:58:54PM
bwenzel	SYSTEM	LT-ROBERTW	152	GRANT ROLE	CONNECT	3/25/07 1:58:56PM
bwenzel	SYSTEM	LT-ROBERTW	152	SYSTEM GRANT	null	3/25/07 1:58:56PM

Fig 3. This report provides a list of all privileged accesses and links it back to the user who performed the change on the Oracle database.



Changes by User

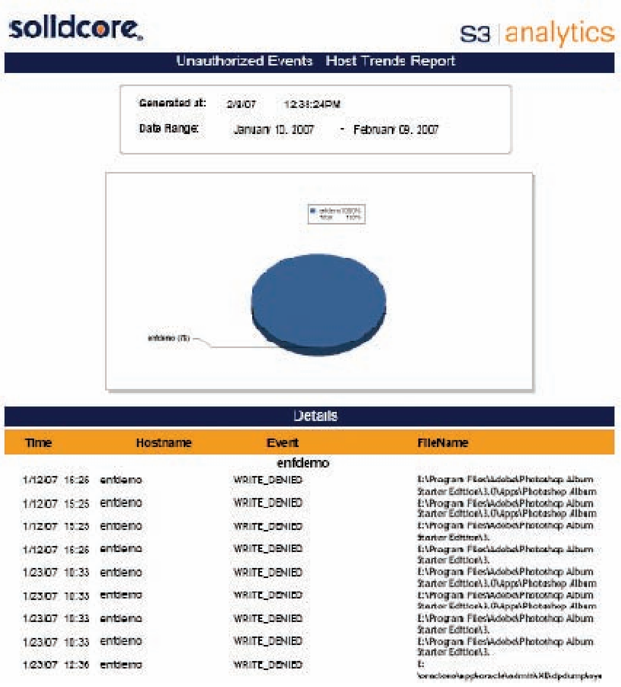
Generated at:	December 04, 2006 11:11:35 AM
Date Range:	October 01, 2006 - October 31, 2006
Host:	ALL

Fig 4. This report provides a list of users who made changes on the servers under consideration.

PCI Control Requirement: Section 10.5.5

Description: Use file integrity monitoring and change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).

Solidcore Automation: Solidcore S3 Control's alerting capabilities immediately notify administrators when unauthorized changes are detected. The Solidcore S3 Control enforcement capability can be used to prevent changes except when performed in concert with approved ticket or by an approved automated process. Fig 5 shows a report of all changes that were prevented by Solidcore S3 Control.



solidcore S3 | analytics

Unauthorized Events Host Trends Report

Generated at: 2/4/07 12:31:24PM
Date Range: January 10, 2007 - February 09, 2007

Details

Time	Hostname	Event	FileName
	enfdemo		
1/12/07 16:26	enfdemo	WRITE_DENIED	E:\Program Files\Adobe\Photoshop Album Starter Edition\3.0\Apps\Photoshop Album
1/12/07 15:25	enfdemo	WRITE_DENIED	E:\Program Files\Adobe\Photoshop Album Starter Edition\3.0\Apps\Photoshop Album
1/12/07 15:25	enfdemo	WRITE_DENIED	E:\Program Files\Adobe\Photoshop Album Starter Edition\3.
1/12/07 16:26	enfdemo	WRITE_DENIED	E:\Program Files\Adobe\Photoshop Album Starter Edition\3.
1/23/07 10:33	enfdemo	WRITE_DENIED	E:\Program Files\Adobe\Photoshop Album Starter Edition\3.0\Apps\Photoshop Album
1/23/07 10:33	enfdemo	WRITE_DENIED	E:\Program Files\Adobe\Photoshop Album Starter Edition\3.0\Apps\Photoshop Album
1/23/07 10:33	enfdemo	WRITE_DENIED	E:\Program Files\Adobe\Photoshop Album Starter Edition\3.
1/23/07 10:33	enfdemo	WRITE_DENIED	E:\Program Files\Adobe\Photoshop Album Starter Edition\3.
1/23/07 12:36	enfdemo	WRITE_DENIED	E:\oracle\app\oracle\admin\XE\dpdump\xe

Fig 5. Solidcore S3 Control can prevent unauthorized changes to critical files and generate a report of unsuccessful attempts to make these changes. In this example, the user unsuccessfully tried to change critical application files belonging to Photoshop and Oracle.

PCI Control Requirement: Section 10.7

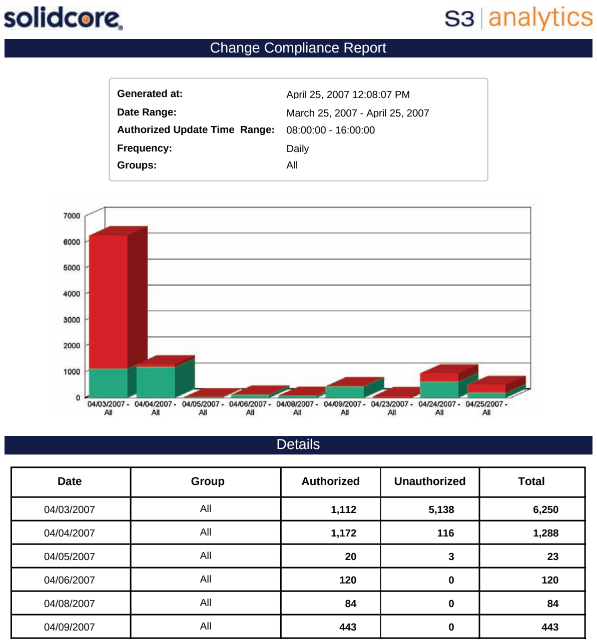
Description: Retain audit trail history for at least one year, with a minimum of three months available online.

Solidcore Automation: Solidcore S3 Control is an independent system back-ended by a secure enterprise-class Oracle database. It affords limited access via secure logins and audit trails are tamper-proof and archived separately to ensure data integrity.

PCI Control Requirement: Section 11.5

Description: Deploy file integrity monitoring to alert personnel to unauthorized modification of critical system or content files.

Solidcore Automation: Solidcore S3 Control can be used to track changes on Servers, Databases and Network Devices. Fig 6 and 7 show changes that were made outside authorized maintenance windows, and changes that were not part of the approved manifest respectively.



solidcore S3 | analytics

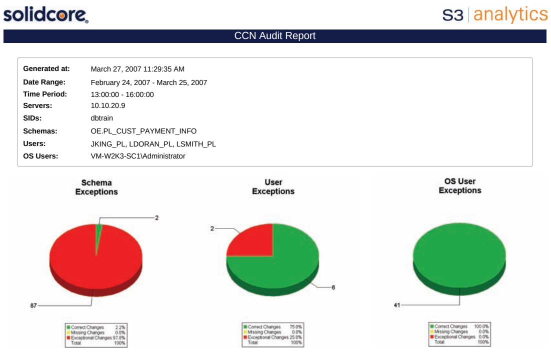
Change Compliance Report

Generated at:	April 25, 2007 12:08:07 PM
Date Range:	March 25, 2007 - April 25, 2007
Authorized Update Time Range:	08:00:00 - 16:00:00
Frequency:	Daily
Groups:	All

Details

Date	Group	Authorized	Unauthorized	Total
04/03/2007	All	**1,112**	**5,138**	**6,250**
04/04/2007	All	**1,172**	**116**	**1,288**
04/05/2007	All	**20**	**3**	**23**
04/06/2007	All	**120**	**0**	**120**
04/08/2007	All	**84**	**0**	**84**
04/09/2007	All	**443**	**0**	**443**

Fig 6. This report identifies all changes made outside authorized maintenance windows as unauthorized and risky changes.



solidcore S3 | analytics

CCN Audit Report

Generated at:	March 27, 2007 11:29:35 AM
Date Range:	February 24, 2007 - March 25, 2007
Time Period:	13:00:00 - 16:00:00
Servers:	10.10.20.9
SIDs:	dbtrain
Schemas:	OE.PL_CUST_PAYMENT_INFO
Users:	JKING_PL, LDORAN_PL, LSMITH_PL
OS Users:	VM-W2K3-SC1\Administrator

Fig 7. This report identifies all unapproved changes that were made to critical database objects that were not part of the Change Request. It can also be used to identify unauthorized users who made changes.

Summary

Solidcore S3 Control is widely used for PCI compliance by organizations ranging from large level 1 merchants to small level 4 merchants. It is a deploy-and-forget solution that provides coverage and benefits for a significant portion of the PCI DSS control objectives and individual requirements. Solidcore automates the process for gathering critical data and demonstrating PCI compliance to internal and external auditors.

Solidcore S3 Control is supported on a wide range of platforms including various versions of Microsoft Windows, Red Hat Linux, AIX, HP-UX and Solaris operating systems, Oracle, DB2, SQL Server and Sybase databases and over 300 network devices including routers, switches and firewalls from major vendors like Cisco, Juniper and Nortel.

About Solidcore Systems

Solidcore is a leading provider of change control for critical systems.

Solidcore's S3 Control software is the industry's first and only solution to automate the enforcement of change management policies. Solidcore automatically reconciles infrastructure changes against change tickets, and provides real-time change auditing so enterprises can measure the effectiveness of change management processes and policies.

Customers trust Solidcore to improve service availability, implement ITIL initiatives, and lower costs related to compliance. Solidcore also provides change control for embedded systems and is used by major device manufacturers to securely leverage open systems to meet their business requirements.

Solidcore is headquartered in Cupertino, California. For more information, visit www.solidcore.com.

solidcore®

Solidcore Systems, Inc.
20863 Stevens Creek Blvd, Suite#300
Cupertino, CA 95014

Email: sales@solidcore.com
Web: http://www.solidcore.com
Tel: 888.210.6530