orca
optimizing application ecosystems

Achieving and Maintaining PCI DSS Compliance with Centralized, Automated Application and Middleware Change Control

TECHNICAL WHITE PAPER

Table of Contents

Executive Summary

Many organizations are already PCI DSS compliant. Then something changes. Often the change is small and seemingly innocuous such as a configuration update to a web based application or middleware. Perhaps a configuration setting drifted and it needed to be reset. Perhaps IT Operations wrote a PowerShell script in order to deploy a configuration update across multiple servers. In the process of deploying that intended change, that well-meaning IT Operations employee inadvertently caused an unintended change as well, one that opened a security vulnerability. Changing this broke that.

…that well-meaning IT Operations employee inadvertently caused an unintended change as well, one that opened a security vulnerability.

Orca is a robust configuration management solution that 1) automatically detects then corrects configuration drift, 2) centrally secures and controls application and middleware changes and 3) provides compliance audit trails indicating the nature, timing, locations and approvers behind each change.

PCI DSS Breaches. Huge Problem. Severe Consequences.

"What keeps you up at night?" It is a classic question that countless IT sales makers ask of CIOs. And without fail, "Security and Compliance" tops the list year after year. Unless they are receiving an industry award, few CIOs want to read about their company's security on the front page of the New York Times. Concern about security and compliance is not misplaced. According to PwC, companies have experienced a compound annual growth rate of 66% in "Security Incidences" since 2009. Verizon Enterprise data indicates that "45% of Americans say they or a household member have been notified by a card issuer, financial institution, or retailer that their credit card information had possibly been stolen as part of a data breach." And In late 2014 53 million Home Depot customers suffered the loss of their Email Addresses due to a successful cyber-attack on Home Depot's data center. In the process, Home Depot suffered the loss of brand value and customer loyalty of those 53 million customers.

While security breaches of all kinds cause headaches for IT security professionals and CIOs, breaches that result in losing control of private data are particularly damaging to reputations and to financials.

Loss of private data is devastating to the individual victims causing them a great deal of fear as well as hours of hassles investigating damage, repairing their reputation with credit agencies and in many cases financial losses.

To the organization that was entrusted by those same consumers to protect their data, a loss of customer payment information can truly destroy years of trust and market cap overnight. Careers are terminated in the process. PCI DSS standards are designed to preempt this turmoil. But adhering to PCI DSS standards is much easier said than done.

In layman's terms, bad guys are casing your cyber home, looking for opportunities and oversights on your part, hoping you and your team have mistakenly left one of your doors or windows unlocked. The more people (visitors, renovation contractors, friendlies) that you grant access to your home, the more opportunities that someone will leave a door or window open (or even a spare key lying around). And just like that home that is undergoing renovations, your business and its mission-critical software is constantly changing.

Software Changes.

But hackers and other intruders only need to be successful once.

Software changes. That's what it does. It improves. It becomes more robust, handling more and different types of situations and users. But each software change, even from well-intentioned employees and trusted contractors, represents a new opening and a new risk. Most software and middleware configuration changes are executed without negative consequences. But hackers and other intruders only need to be successful once.

Common approaches to controlling change: People, Process, Spreadsheets

Naturally, many PCI DSS requirements focus on controlling those risky changes.

Many PCI DSS requirements focus on controlling those risky changes.

People: Some organizations choose to achieve control through a people approach, focusing on hiring quality, experienced staff and giving them regular training with regular updates.

Process: Other organizations focus on process - implementing a series of checks and approvals, review committees and even structural approaches, such as ITIL, as mechanisms for controlling changes to their application and middleware ecosystems.

Spreadsheets: Many organizations seek to control application and middleware configuration changes using technology that includes homegrown or spreadsheet-based tools.

While each of these approaches has merits, each approach also has limitations. Training is expensive and is not a systematic approach to error-prevention. Process frameworks like ITIL

can become an enormous time sink, so layered with procedures and checks that to be effective, people will operate outside of the officially sanctioned process. Homegrown tools can become unreliable and unwieldy, requiring a special skill set just to operate and maintain them. Hiring for this unique skill set creates its own challenges as well. And spreadsheets have long been notorious for failing to automatically track updates or even maintain version control.

The Orca Approach to Controlling and Cataloging Changes

Orca centrally controls changes: the "what", "when", "where", "who" and even who can approve.

Orca takes an enterprise technology solution approach to software configuration changes, centrally controlling what changes can be made, when and where changes can be applied, who can make changes and who can approve them. Even before those software configuration changes are applied, Orca users "Preview" and "Dry Run" intended changes to validate that changes will be successful and will be applied to intended nodes.

Unlike a simple PowerShell script that can indiscriminately apply system-wide changes without central console-level oversights, Orca is an application-centric and middleware configuration management solution that centrally controls the changes that can inadvertently introduce security vulnerabilities. Because of its central control and its scripting-free automation, Orca eliminates the need for direct access to servers, a major source of uncontrolled IT changes.

After applying changes, Orca users (who have access privileges) can view change audit logs that record the "who", "what", "why", "when" and "where" behind those changes.

How Orca addresses specific PCI DSS compliance problems

The attached table is excerpted from the "PCI DSS v 3.1 Self-Assessment Questionnaire D and Attestation of Compliance for Merchants." It is modified to map how Orca addresses several PCI DSS elements. Please use the accompanying table to assist you and to correct possible gaps in your PCI DSS Compliance journey.

PCI DSS v3.1 Self-Assessment Questionnaire D and Attestation of Compliance for Merchants

PCI DSS v 3.1 Self-Assessment Questionnaire D and Attestation of Compliance for Merchants	How Orca (www.orcaconfig.com) addresses this topic
6.4 Are change control processes and procedures followed for all changes to system components to include the following:	
6.4.1 (a) Are development/test environments separate from the production environment?	✓ Once Orca administrators define distinct Dev, Test and Prod environments, any approved changes in those environments are contained to those intended nodes.
6.4.1 (b) Is access control in place to enforce the separation between the development/test environments and the production environment?	✓ Orca employs a robust role based access control (RBAC) system that controls which individuals and groups have view, edit or approve privileges. These privileges can be set to restrict at granular levels who has access to Dev, Test and Prod environments.
6.4.5 (a) Are change-control procedures for implementing security patches and software modifications documented and require the following? Documentation of impact; Documented change control approval by authorized parties; Functionality testing to verify that the change does not adversely impact the security of the system; Back-out procedures (b) Are the following performed and documented for all changes:	
6.4.5.1 Documentation of impact? Trace changes to change control documentation; Examine change control documentation	✓ Orca's RBAC system controls the type and scope of software configuration changes allowed as well as which individuals and groups can make those changes. Each change is automatically logged.

6.4.5.2 Documented approval by authorized parties?	✓ Orca administrators determine which individuals and groups are authorized to approve changes in each application ecosystem (e.g. ecommerce) and environment (e.g. Production). This information is automatically documented and changes to approver lists are logged.
6.4.5.4 Back-out procedures?	✓ Orca uses scripting-free automation to automatically deploy approved changes. This change automation ability can be used to perform back-out procedures.
7.1 Is access to system components and cardholder data limited to only those individuals whose jobs require such access, as follows: Is there a written policy for access control that incorporates the following? Defining access needs and privilege assignments for each role; Restriction of access to privileged user IDs to least privileges necessary to perform job responsibilities; Assignment of access based on individual personnel's job classification and function; Documented approval (electronically or in writing) by authorized parties for all access, including listing of specific privileges approved	
7.1.1 Are access needs for each role defined, including: System components and data resources that each role needs to access for their job function? Level of privilege required (for example, user, administrator, etc.) for accessing resources?	✓ Orca administrators determine specific levels of view, edit or approve access for individuals and groups.
7.1.2 Is access to privileged user IDs restricted as follows: To least privileges necessary to perform job responsibilities? Assigned only to roles that specifically require that privileged access?	✓ Access levels in Orca are set and enforced by administrators. Access can be established by the administrator to match privileges with roles.

7.1.3 Are access assigned based on individual personnel's job classification and function?	✓ Access levels in Orca are set and enforced by administrators. Access can be established by the administrator to match privileges with roles. ✓ Orca ties internal roles and permissions to Microsoft Active Directory (AD) groups so management of 'who can do what' stays centralized in their AD knowledge base.
7.1.4 Is documented approval by authorized parties required, specifying required privileges?	✓ Orca enforces change approvals that are set by administrators. Access privileges and changes are documented and logged by Orca.
7.2 Is an access control system in place for system components to restrict access based on a user's need to know, and is it set to "deny all" unless specifically allowed, as follows:	
7.2.1 Are access control systems in place on all system components?	✓ Orca administrators can establish application ecosystems (e.g. ecommerce) linking applications, middleware, database and configurations as well as access privileges to each.
7.2.3 Are access control systems configured to enforce privileges assigned to individuals based on job classification and function?	✓ Within the Orca solution, access view, edit or approve changes to configurations can be granted to named individuals or based on job classification and function.
10.1 (a) Are audit trails enabled and active for system components?	✓ Audit trails are enabled for the environments that Orca manages.
10.1 (b) Is access to system components linked to individual users?	✓ Orca can be used to control access to system components that are linked to individual users.
10.2 Are automated audit trails implemented for all system components to reconstruct the following events:	

10.2.1 All individual user accesses to cardholder data?	✓ Orca audit logs can be used to track individual user access to ecosystems that manage cardholder data.
10.2.2 All actions taken by any individual with root or administrative privileges?	✓ Orca audit logs track actions taken by individual users with root or administrative privileges.
10.2.5 Use of and changes to identification and authentication mechanisms–including but not limited to creation of new accounts and elevation of privileges – and all changes, additions, or deletions to accounts with root or administrative privileges?	✓ Uses of and changes to identification and authentication mechanisms are tracked by Orca's RBAC. Changes, additions or deletions of accounts with root or administrative privileges are also tracked and logged by Orca.
10.3 Are the following audit trail entries recorded for all system components for each event:	
10.3.1 User identification?	✓ Orca audit trails identify the user that initiated or approved a change.
10.3.2 Type of event?	✓ Orca creates audit trails indicating the nature of the configuration change that was made.
10.3.3 Date and time?	✓ Orca audit trails that log the date and time of configuration changes.
10.3.4 Success or failure indication?	✓ Orca audit trails log and notify users whether configuration changes were successfully applied.
10.3.5 Origination of event?	✓ Orca audit trails logs the origination of each configuration change event.
10.3.6 Identity or name of affected data, system component, or resource?	✓ Orca audit trails log the identity or name of affected data, system component, or resource.
10.5 Are audit trails secured so they cannot be altered, as follows:	
10.5.1 Is viewing of audit trails limited to those with a job related need?	✓ Administrators can set Orca's RBAC to limit audit trail views to those with a job related need.

10.5.2 Are audit trail files protected from unauthorized modifications via access control mechanisms, physical segregation, and/or network segregation?	✓ Audit trails are secured in the Orca database and are subject to on premise database security management.

The approximately 400 PCI requirements in SAQ D *only* indicate the work that your IT staff has to comply with. Orca assists you in *becoming* compliant and more importantly *maintaining* that compliance at a fraction of the cost and with certainty that negative consequences to your changing IT landscape will not be expensive to manage.

Summary

Among its many requirements, PCI DSS Compliance demands that organizations demonstrate a repeatable system of change controls and audit trails.

This degree of change control can be difficult to achieve even with diligent IT professionals on staff. Long-term, focused and documented change control is difficult to achieve in any department, but in a fast paced IT environment it's especially challenging. Without a robust technology solution in place to enforce configuration change control in software application and middleware ecosystems and environments, unauthorized changes are nearly inevitable and their consequences are unpredictable. Homegrown configuration tools lack dedicated third party support with improvement road maps and often require manual scripting and "tribal knowledge". Alternatively, server and OS configuration tools require scripting to control changes to applications and middleware and often have limited support in Windows environments.

By contrast, Orca is a full configuration management solution that automatically detects and corrects configuration drift. Orca also centrally secures and controls application and middleware changes and provides compliance audit trails indicating the nature, timing, locations and approvers behind each change.