

Cfengine and PCI Compliance

A Business White Paper

PCI DSS is a set of 12 high-level requirements designed to secure and protect credit card customer payment data. If you store, process or transmit any cardholder data electronically or manually, then your business must comply with PCI-DSS. Cfengine Nova can help meet many of the requirements automatically, and verify not only once, but on a continuous basis bringing compliance reports and successful audits

DISCLAIMER: Under no circumstances will any part of the Cfengine company be held responsible for errors or omissions in this document.

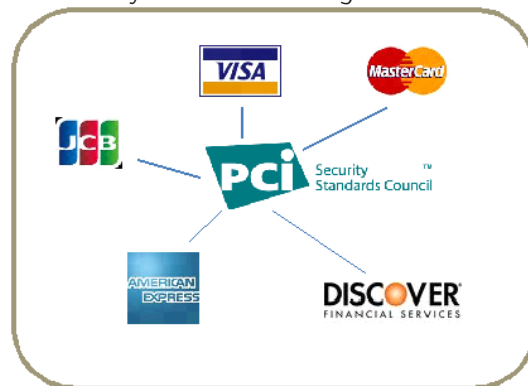
Copyright © 2010 Cfengine AS

Table of Contents

PCI Compliance	1
The Data Security Standard.....	1
Top 10 reasons for using Cfengine Nova as part of PCI-compliance.....	1
Reason #1: Automate most of the technical PCI-requirements.	1
Reason #2: Automate file, log and database security	2
Reason #3: Automate building and securing the network.....	2
Reason #4: Automate testing and reporting	2
Reason #5: Quick and successful audits through compliance reports	2
Reason #6: Uptime of security and scanning applications with conditional fallbacks ensured.....	2
Reason #7: One of the most secure and stable technology solution in the industry.....	2
Reason #8: Flexible framework, allows you to model the solution according to organizational needs.....	2
Reason #9: Cross-platform, one common set of policies for all operating systems.....	3
Reason #10: Lightweight solution will not impact your machines performance	3
Cfengine's role	3
Nova Benefits:.....	4
Nova Benefits:.....	5
Nova Benefits:.....	5
Nova Benefits:.....	5
Nova Benefits:.....	6
Requirement 12:.....	6
Nova Benefits:.....	6
Conclusions.....	6

PCI Compliance

The Payment Card Industry Data Security Standard, also known as PCI DSS is a set of comprehensive requirements for enhancing payment account data security. It was developed by the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa International, to help facilitate the broad adoption of consistent data security measures on a global basis.



PCI DSS is a set of 12 high-level requirements designed to secure and protect credit card customer payment data. If you store, process or transmit any cardholder data electronically or manually, then your business must comply with PCI-DSS. Cfengine Nova can help meet many of the requirements automatically, and verify not only once, but on a continuous basis bringing compliance reports and successful audits

The Data Security Standard

To date, criminals have stolen millions of customer card records. The industry is facing a steep increase in the threat of data theft. This is a main reason why card payment companies joined forces to create the Payment Card Industry Data Security Standard (PCI DSS) with the aim of safeguarding sensitive card data. A checklist of almost 300 points is required to be passed before a PCI-compliance is granted. Cfengine can help companies automate many of these points. Using a high-level policy language, Cfengine can align systems with the required Company Security Policy. Becoming PCI-compliance is not only about passing checklists, but equally important is the implementation of internal procedures and human behavior.

Top 10 reasons for using Cfengine Nova as part of PCI-compliance

The main reason for using Cfengine Nova is automation and the ability to prove compliance through reporting and Knowledge Management. Many of the technically solvable requirements can be handled directly with Cfengine's built-in functionality, whilst other more domain-oriented requirements, like security scans, can be managed by Nova by integrating third-party software, ensuring that it runs on time and takes appropriate action depending on outputs.

Below is a list of top 10 reasons for using Cfengine Nova as part of your organization's PCI-compliance.

Reason #1: Automate most of the technical PCI-requirements.

Directly or indirectly Cfengine Nova can ensure a majority of the PCI-requirements. Almost all the requirements that can be solved through scripts, third party software or other non-human

solutions, should be managed by Nova to ensure a consistent and policy related behavior of the system.

Reason #2: Automate file, log and database security

Cfengine Nova manages files, logs and databases effectively. It ensures the existence or non-existence of files. Using its built-in tripwire functionality, any change in files or logs can be reported or undone. Same thing applies to missing database tables and fields. Nova comes with file access control list support, which makes it effective to comply to most of the PCI file related requirements. To change file-permissions or policies, changing the Cfengine policy accordingly is all that is needed. The implementation of updated policy is automatically taken care of by Cfengine.

Reason #3: Automate building and securing the network

Cfengine can manage many firewall applications and system configurations. This way you can rely on Cfengine preventing unauthorized access to files or areas. Nova ensures that Security policies are automatically implemented wherever requested. For instance, ensuring the existence of certain processes in the firewall DMZ, is easy with Nova. If for some reason, the processes are not running, Nova will restart the process, and if stated in the policy, after some time, Nova can execute plan B.

Reason #4: Automate testing and reporting

Using Nova to control scripts and security software, you can be sure validation test are run on schedule. Outputs from the tests are available in reports, and actions can be taken dependent on the outcome. Cfengine agents generate reports every time they run, and the agents ensure execution of various test-procedures.

Reason #5: Quick and successful audits through compliance reports

Nova comes with many out-of-the-box reports in its Knowledge Map. Compliance reports showing time of compliance, deviations, and successful or unsuccessful repairs are available.

Reason #6: Uptime of security and scanning applications with conditional fallbacks ensured

Enforcing a policy stating that a virus scanner should always be running on all machines is straightforward with Nova. If the process is down, Nova will automatically re-start or execute alternatives. You can have Nova manage indefinite number of processes on your machines.

Reason #7: One of the most secure and stable technology solution in the industry

Cfengine has been around since 1993. It is characterized by stability and security. Since its inception there has been no real security flaw. Industry leaders around the world depend on the solution every day. More than 1 million machines run Cfengine.

Reason #8: Flexible framework, allows you to model the solution according to organizational needs

Cfengine Nova is an evolutionary solution that grows with your company. You can start-off automating only a couple of processes, then gradually implement more and more. Unlike high



risk all-or-nothing solutions, Cfengine is a low cost, unintrusive system. The solution scales very well. Companies with more than 150,000 machines run Cfengine for CPI compliance.

Reason #9: Cross-platform, one common set of policies for all operating systems

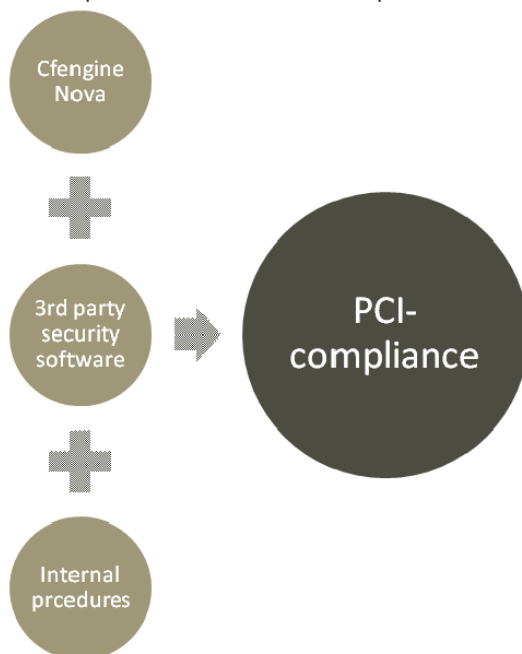
Cfengine runs on most operating platforms. Use a single set of policies, and have Cfengine implement these on all your platforms.

Reason #10: Lightweight solution will not impact your machines performance

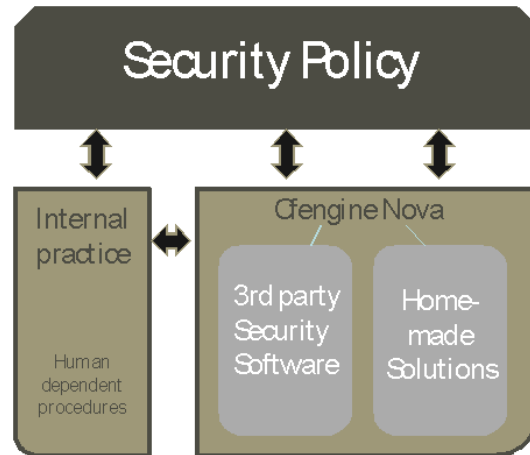
Cfengine Nova is written in a lightweight programming framework. The agents are small in size and runs efficiently. This makes Cfengine Nova highly adapted for virtualization.

Cfengines role

Cfengine Nova can manages all the software related procedures, third party solutions and in-house specifics that cover requirements and internal procedures.



Becoming PCI-compliant requires employees to accord with the Security Policy, which will most likely require a change in behavior. By using Cfengine Nova as your main automation tool in the PCI-compliance process, you are ensured desired end-state is always kept. Nova acts as a wrapper, both solving core problems, integrating and orchestrating additional products. The illustration shows the way we suggest looking at Nova as part of an organizations PCI compliance process.



The different PCI-requirements and how Nova can help The PCI-requirements are divided into 6 main categories. Under each of these there are sub-requirements that again holds a set of check-point, 220 in total. The 6 main categories are:

1. Build and Maintain a Secure Network
2. Protect Cardholder Data
3. Vulnerability Management Program
4. Strong Access Control Measures
5. Monitor and Test Network
6. Maintain an Information Security Policy

Under each of these categories there are in total 12 sub-requirements. These requirements are listed below along with an explanation on how and what related benefit one can expect for each of these by implementing Cfengine Nova.

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

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

By using Nova to build and maintain your secure network, you can automate and ensure required check-points. Application firewall configurations can be automated. Have Nova verify traffic restrictions and document the results of these. Nova can help manage public access between the internet and any system and component in the cardholder environment. The requirement for having only one function per server, can be part of your automated policy.

Nova Benefits:

Novas self-repair technology ensures settings not only once, but continuously

Desired end-state of configurations always ensured Automatic verification of security settings and network traffic 17 of 36 checkpoints can be automated and ensured by Cfengine Nova.

Requirement 3: Protect stored cardholder data

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

Managing Cardholder Data, is about managing the files and databases containing the sensitive data. Nova can ensure batch-jobs are run and database tables, files and logs are maintained. Ensure that security keys are changed frequently and expire on time. According to the standard all traffic must be over SSL using the latest software patches all things Nova can manage. Have Nova inspect files and logs and automatically make changes according to pre-defined security policies.

Nova Benefits:

- Manage files, logs, database tables and fields.
- Manage encryption and privacy standards.
- Ensure critical software patches automatically
- Compliance reports easily available (click here to see an example)

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

Cfengine Nova can verify that programs and applications are deployed on the right machines at the right time, and ensure that programs are running. Patch-lists from vendors can be implemented, and Nova can help you verify operational tests after a change in an application or home-made web-based solution.

Before moving an update to production, Nova can ensure that the necessary vulnerability-scripts have been run successfully. If they are not successful Nova will not deploy the application or program.

Nova Benefits:

Ensure automatic conditional software deployments Ensure right application at the right machines; always Ensure the uptime of any application on continuous basis Detect vulnerability issues automatically Never miss a step in the quality assurance procedure

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

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

Requirement 9: Restrict physical access to cardholder data

Nova can manage access control based on users or group of users, i.e. ensure that no one has access to new files or folders without explicit assignment of privileges. By managing system configuration settings, Nova ensure proper password management throughout the life-cycle (from creation to deletion). Nova can also interface with operating systems user management modules.

Nova Benefits:

- Nova comes with enhanced file access control capabilities
- All system configuration settings ensured to stay in compliance
- Detect and repair unauthorized file access automatically
- One set of rules allowing for all operating systems



- Requirement 10:** Track and monitor all access to network resources and cardholder data
- Requirement 11:** Regularly test security systems and processes

Nova manages files automatically. It can verify the presence of specific content, e.g. within log-files. Protect against accidental deletion of a log-file or unauthorized attempts to change a file. Nova reports changes if needed, and can restore the original version of the file. Nova can encapsulate third-party scanning software schedule it for execution and take action based on the results. Nova can further ensure the presence and execution of intrusion-detection and/or intrusion-prevention systems. Logs and files can easily be viewed in Nova Knowledge Map, together with the insight about how they interrelate.

Nova Benefits:

- Manage log-files according to overall security policy
- Avoid accidental deletion of a file or unauthorized access
- Ensure the existence and backup of critical files
- Ensure security scanning programs are run according to schedule
- View reports directly in the Knowledge Map

Requirement 12:

Maintain a policy that addresses information security for employees and contractors

Thanks to its high-level language Cfengine Nova can facilitate and document internal processes using its Knowledge Map. Examples show how promise theory has helped organizations reduce their lead-time and ensure procedural steps are kept. Especially big organizations with more management levels and long lead-time can gain big benefits by applying this theory. Large organizations in particular can benefit from the principles embodied in promise theory a methodology in which security is built in from the start.

Nova Benefits:

- 24/7 incident response and monitoring
- Ensure that employees read the organization security policy annually
- Get a list of usage policies and personnel authorized to use the devices
- Apply promise theory to organizational procedures and routines

Conclusions

Cfengine Nova enables organizations become PCI-compliant by applying automatic procedures. There are 3 components involved in pursuing a PCI-process; internal procedures, third party security software and Cfengine Nova. Internal procedures must ensure employees become aware of the PCI-requirements and adjust their behavior thereafter. New procedures must be developed, documented and kept.

Certain PCI-requirements may only be achieved by third-party security-domain software. Cfengine Nova can still take overall responsibility for successful executions. Join the ranks of our PCI success stories by choosing Cfengine Nova.