

Zurich, 1st August 2015

Rapid PCI-DSS / CISP Compliance with Airlock

This document is for the attention of

All merchants, financial institutions and all
entities involved in
card processing, transmit or store credit
cardholder data

AIRLOCK
by ergon

Please contact

Ergon Informatik AG
Gernot Bekk-Huber
+41 44 268 8721
gernot.bekk-huber@ergon.ch

Autoren

Urs Zurbuchen
Gernot Bekk-Huber

Table of contents

1.	Why should I care about the Payment Card Industry Data Security Standard (PCI DSS)?	3
2.	Rapid PCI Compliance with Airlock WAF	4
3.	Detailed Requirements of the PCI Standard and Benefits of Airlock Suite	5
3.1	Build and Maintain a Secure Network (Requirements 1 – 2)	5
3.2	Protect Cardholder Data (Requirements 3 – 4)	5
3.3	Maintain a Vulnerability Management Program (Requirements 5 – 6)	5
3.4	Implement Strong Access Control Measures (Requirements 7 – 9)	7
3.5	Regularly Monitor and Test Networks (Requirements 10 – 11)	7
3.6	Maintain an Information Security Policy (Requirement 12)	7
4.	Summary of PCI DSS Compliance with Airlock Suite	8

The data security standard of the payment card industry (PCI DSS) became effective by end of September 2007. The current version of the PCI DSS is V3.1 from April 2015. Every company that does not protect credit card data or transactions sufficiently will face severe consequences and penalties. The web application security solution Airlock Suite combines a web application firewall (Airlock WAF) and an identity and access management solution (Airlock Login / IAM) and significantly helps to comply with the strict security standard.

1. Why should I care about the Payment Card Industry Data Security Standard (PCI DSS)?

What is worse than being attacked by a hacker? Not even knowing about it! Other than a few years ago, Hacker attacks today are highly motivated by organized criminal backgrounds and financial benefits. Hacker attacks on the application level are most of the times not even recognized. Stealing credit cardholder data is the most typical example for a successful and silent hacker attack. Sophisticated attack methods are continuously improved by hackers and present a huge risk to all companies who process, transmit or store credit cardholder data.

Threatened by today's application level attacks, the PCI Security Standards Council has been created to provide a common data security standard across all payment brands. Founders of the PCI Security Standards Council are the major credit card companies such as American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International. The Payment Card Industry Data Security Standard (PCI-DSS) describes 12 security requirements to ensure safe handling of sensitive information and prevent attacks against cardholder data and transactions.

All merchants, financial institutions and all entities involved in card processing, transmit or store credit cardholder data have to comply with the standard. Non-compliance will lead to restrictions, fines and additional fees. A special focus of the Payment Card Industry Data Security Standard is on preventing attacks on the application layer. All applications are concerned as the following quote from the PCI DSS clearly shows:

“System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is that part of the network that possesses cardholder data or sensitive authentication data.”

<...>

“Applications include all purchased and custom applications, including internal and external (Internet) applications.”

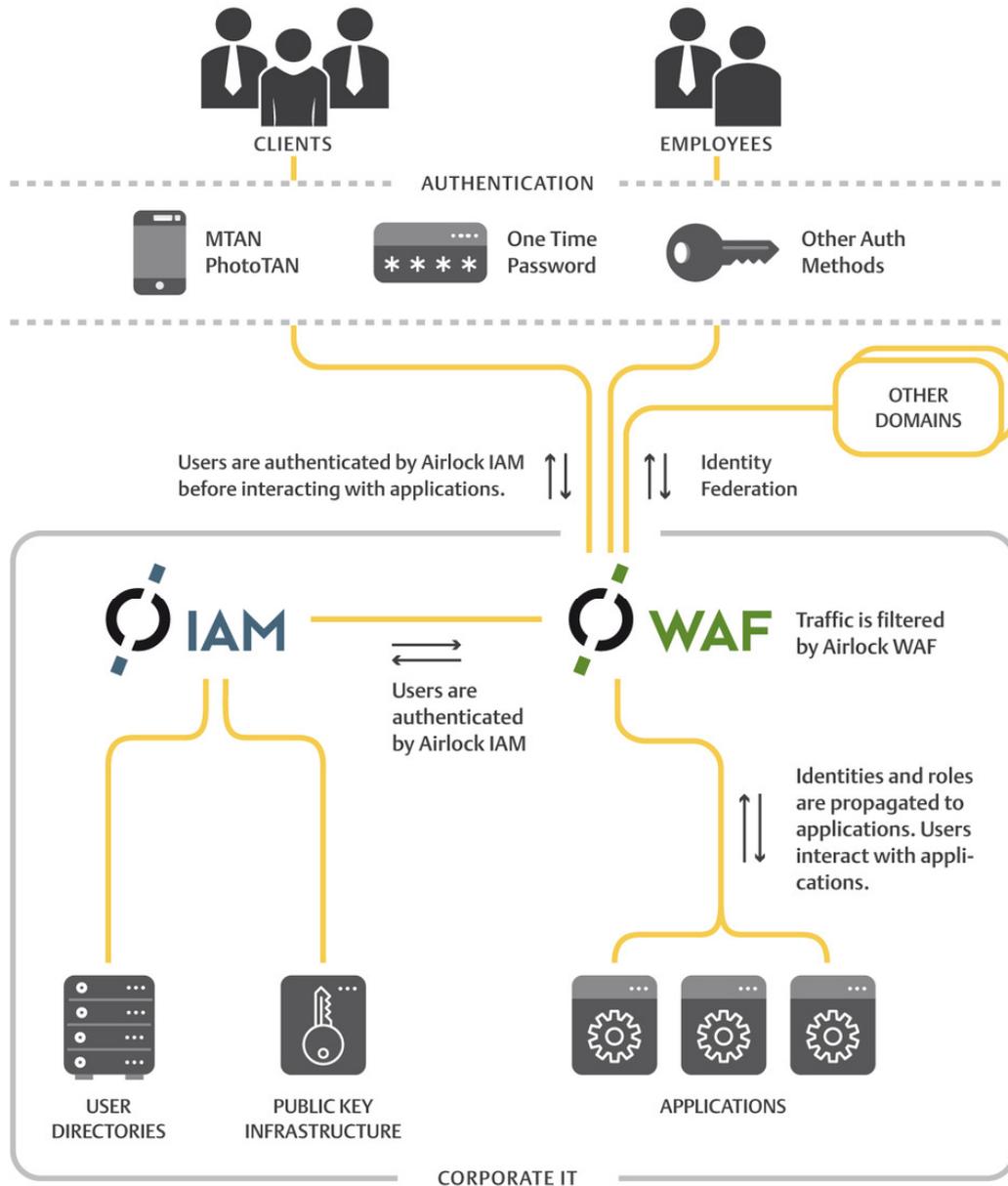
More information about the Payment Card Industry Data Security Standard (PCI DSS) can be found at the Web site of the PCI Security Standards Council:

<http://www.pcisecuritystandards.org>

Airlock provides the Web Application Firewall (WAF) Airlock WAF and the Identity and Access Management Solution Airlock IAM that significantly help you to comply with the PCI Data Security Standard while lowering costs at the same time. Section 6.6 of the PCI DSS recommends implementing a Web Application Firewall for application level security tasks.

2. Rapid PCI Compliance with Airlock WAF

Airlock Suite dramatically reduces time, efforts, complexity and costs in achieving compliance with the standard. In contrast to competitive products, Airlock covers the whole Web application security requirement scope and efficiently helps to meet the PCI requirements regarding the protection of applications.



3. Detailed Requirements of the PCI Standard and Benefits of Airlock Suite

The PCI Data Security Standard describes the following 12 security requirements. For at least 7 out of the 12 requirements, *Airlock* instantly helps to comply with the standard.

3.1 Build and Maintain a Secure Network (Requirements 1 – 2)

PCI Requirement 1 & 2: Install and maintain a firewall configuration to protect cardholder data. Do not use vendor supplied defaults for passwords and other security parameters. The first two requirements describe today's best practice for a multi-tier network architecture with a DMZ, network firewalls, routers, switches, application servers, databases, etc. All incoming/outgoing connections have to be described in a network firewall policy and justified. Frequent reviews of the firewall and router rule sets are required to verify the implementation of the policy. As a focused Web Application Firewall (WAF), *Airlock WAF* is placed behind the perimeter network firewall to specifically validate and analyze all Web application traffic (HTTP/ HTTPS). It therefore supports requirement 1 as a Web Application Firewall with specific security functions on the Web application layer. Requirement 2 needs to be fulfilled and documented in a policy to comply with the standard.

3.2 Protect Cardholder Data (Requirements 3 – 4)

Requirement 3: Protect stored cardholder data. This requirement clearly states the importance of safe handling of sensitive credit cardholder data and the way it is stored (either electronically or on print-outs etc.). PCI auditors check for storage policies and how they are implemented. You need to describe carefully how cardholder data is stored and how the stored data is protected. The Web Application Firewall *Airlock WAF* does not help with this requirement as it does not store application data.

Requirement 4: Encrypt transmission of cardholder data across open, public networks. This requirement is provided as a core function (SSL termination) by *Airlock WAF*. *Airlock WAF* provides convenient mechanisms to handle SSL certificates, CRLs and it supports hardware accelerated SSL termination as well as HSMs for secure private key storage. The applications do not have to deal with SSL and its vulnerabilities in any way; it's all offloaded to *Airlock WAF*! [With automatic virtual patching functionalities new vulnerabilities can be fixed within hours over all applications.](#)

3.3 Maintain a Vulnerability Management Program (Requirements 5 – 6)

Requirement 5: Use and regularly update anti-virus and malware software. This requirement demands active and up-to-date Anti-Virus solutions to protect the applications against viruses/worms/ trojans. You need to make sure that an updated Anti-Virus solution is in place, especially on user PCs in your company network. Regarding the security of your application servers, *Airlock WAF* significantly leverages your investment into the Anti-Virus solution as the Web Application Firewall supports file upload Anti-Virus scanning via the ICAP interface. All upload content to the applications is checked against viruses/worms/trojans on-the-fly by *Airlock WAF*. Especially for Web applications where users may upload files this is a key benefit. Additionally, *Airlock WAF* provides a positive security enforcement module with a multi-stage filtering engine and URL encryption mechanisms that prevent viruses or worms to get to your applications.

Requirement 6: Develop and maintain secure systems and applications. This requirement and its sub-requirements are the new core of the PCI Data Security Standard regarding application security enforcement. It is the requirement where *Airlock WAF* presents its key functions and USPs to help you to comply with the PCI Data Security Standard. *Airlock WAF* is developed with a clear focus on these requirements. Experience of leading business enterprises has shown that the application security requirement is very complex to be met over time. Only a dedicated and focused product such as *Airlock WAF* makes it possible to address the different aspects of the problem in a unified, cost-efficient and easy-to-use way. Let's look into the details of requirement 6 to get a better picture:

Requirement 6.1 demands latest security patches to be installed for your systems. However, there is always a period of time (between finding the vulnerability and the patch release) where the system is exposed to a certain wide-spread vulnerability (so-called “zero day” exploits). *Airlock WAF* protects applications against known and even unknown attacks. Therefore, as an additional positive protection layer, *Airlock WAF* significantly reduces the pressure of patching and the operations team gets back into a pro-active mode of work instead of reactive.

Requirement 6.2 demands a process to identify new security vulnerabilities. Same as with 6.1: *Airlock WAF* greatly reduces the risk because the Web Application Firewall protects against known and even unknown attacks with its positive security model.

Requirement 6.3 demands integrated security into the development of the application source code and throughout the development life cycle. It is definitely good advice to comply with best practice regarding security relevant issues in the development cycle as it is described in 6.3. However, experience shows that it is not sufficient and secure code is a myth. The problem is that the application development life cycle is driven by functional requirements. On the other hand the security threat scenario is unlimited and a new attack method may occur just the next day. There will be no application development team available on call just to improve the application instantly to deal with it. Even if there are application developers around to do it, it is not be cost-effective and it requires a whole application release deployment (including analyzing, coding, QA, live testing, productive deployment) whenever a security problem is recognized. Last but not least, the PCI Data Security Standard requires all applications to be protected, also purchased 3rd party products that cannot be adapted quickly to specific customer needs. *Airlock WAF* focuses on protecting any Web application environment independent if custom built or purchased. It dramatically reduces the requirements for integrated security into existing application source code and provides real comprehensive Web application security. Instead of implementing all security functions repeatedly into each application, *Airlock WAF* provides a sophisticated set of security functions for all Web applications at the same time. As a focused Web Application Firewall, *Airlock WAF* stays up-to-date and protects the applications even against most recent attacks.

Requirement 6.4 demands strict change control procedures for all system and software configuration changes.

Even if this requirement results in a well-documented policy and procedure, *Airlock WAF* significantly simplifies change control mechanisms for Web application with its virtual application mappings and the independent security policies.

Administrators can create different configuration sets in parallel and easily switch between them.

Requirement 6.5 summarizes typical application level vulnerabilities and demands secure coding guidelines similar to 6.3 in order to achieve secure application code. As mentioned for 6.3, secure code is a myth and it is practically impossible to keep application code on a high security level over time. It is definitely good advice to follow secure coding guidelines but it is not sufficient. *Airlock WAF* provides a multi-level filtering engine with cryptographic URL encryption and HTML form protection that protect Web applications successfully against the mentioned vulnerabilities. Because the positive security model of *Airlock WAF* dynamically protects the application at runtime, even unlisted and unknown attacks are prevented. [Secure authentication and session management or broken authentication can also be handled centrally over all applications.](#)

Requirement 6.6 demands regular source code reviews by external third parties to maintain the desired level of security over time or to install a Web Application Firewall (WAF). As outlined in 6.3 and 6.5 it is a good idea to follow best practice and secure coding guidelines. In order to keep the security level high over time while keeping the costs low it is much more efficient to install the Web Application Firewall *Airlock WAF*! The PCI DSS also recommends to implement a Web Application Firewall because it provides the desired level of security instantly for all applications and makes it easier to keep the applications continuously protected over time.

3.4 Implement Strong Access Control Measures (Requirements 7 – 9)

Requirement 7: Restrict access to cardholder data by business need-to-know. This requirement is supported by *Airlock WAF and Airlock IAM* by providing secure access and session control for Web applications and application parts for different user groups. Based on the authenticated session credentials *Airlock WAF* only lets users access the applications if they are entitled to.

Requirement 8: Assign a unique ID to each person with computer access. This requirement demands unique user IDs that can be tracked. *Airlock WAF* provides strong multi-factor authentication enforcement combined with secure session handling providing unique user ID and even unique request IDs that can be tracked within the sophisticated log analyzer. *Airlock WAF* simplifies the integration of strong authentication by offloading it from the application's business logic. Additionally, it provides detailed monitoring and reporting functions on the tracked users and sessions. With *Airlock IAM* you can manage the number Login attempts, automatic session timeouts after 15 minutes idle, automatic password expiration and much more centrally. Strong user authentication, token management user management over the whole life cycle including user self-services and proper user-authentication management can be implemented over all applications on one central point.

Requirement 9: Restrict physical access to cardholder data. This requirement demands policies and processes to guarantee physical security mechanisms to access cardholder data. You need to make sure that physical access to cardholder data is protected and that physical access policies are well documented. Again strong authentication is needed to protect card holder data.

3.5 Regularly Monitor and Test Networks (Requirements 10 – 11)

Requirement 10: Track and monitor all access to network resources and cardholder data This requirement demands overall monitoring functions to track all Web application activity. *Airlock* provides a sophisticated monitoring and reporting engine that provides detailed information about all application requests enriched with user and session information. As a central security enforcement unit in front of the Web application servers, *Airlock* provides comprehensive log messages and events for your whole Web application environment, independent of the specific application being used. With an interface for Splunk you can generated aggregated management reports in a ready to us product. The fully integrated solution from Qumram achieves legally compliant data archiving and cross channel recording over all web applications.

Requirement 11: Regularly test security systems and processes. This requirement demands regular tests of the involved systems and processes. It is best practice to perform penetration tests on a regular basis to verify the implementation of the security policies. The penetration test will also show you that the Web Application Firewall *Airlock WAF* prevents your Web applications from being attacked.

3.6 Maintain an Information Security Policy (Requirement 12)

Requirement 12: Maintain a policy that addresses information security. This requirement addresses the need for well documented policies that need to be communicated to employees and contractors.

4. Summary of PCI DSS Compliance with Airlock Suite

As described in the previous sections, *Airlock Suite* instantly helps to meet at least 7 out of the 12 PCI DSS requirements. Many requirements of the PCI DSS are also found in other security compliance regulations and are therefore important “best practice” guidelines for responsible companies that use Web applications for parts of their business. *Airlock* strictly focuses on providing IT security solutions on the application level. Don’t hesitate to contact us to discuss your open questions with us regarding the most efficient way to achieve a high level of application security while keeping costs low.