Protecting Cardholder Payment Transaction Environment with ARCON | PAM

PCI Security Standards Council®

arcon

What does the PCI Security Standards Council mandate ?

Implementing standard security procedures and technologies to mitigate threats of cardholder data thefts and protect payment card transaction environment.

Who should comply with PCI security standards?

All entities that store, process and transmit cardholder data and/or sensitive authentication data.

Manufacturers
(PCI PTS)

Payment Card Issuing Banks & Merchants
(PCI DSS)

For vendors making payment applications and store, process card holder data
(PCI PA DSS)

Why it mandates?

Rampant security breaches in the digitized age

One of the popular US clothing retailers fell prey to hackers as they stole credit card information across the country all through 2017

A North American airliner confirmed personal information breach of 20,000 its mobile app users in August 2018

One of the widely used online travel operator's subsidiary suffered security breach exposing information on 880,000 payment cards in March 2018

The PCI Data Security Standards

Build and maintain a secure network and systems

1. Install and maintain a firewall configuration to protect cardholder data.
2. Do not use vendor supplied defaults for systems passwords and other security parameters

Protect Cardholder data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management program

5. Protect all systems against malware and regularly update antivirus software or programs
6. Develop and maintain secure systems and applications

Implement strong access control measures

7. Restrict access to cardholder data by business need to know
8. Identify and authenticate access to system components 9. Restrict physical access to cardholder data

Regularly monitor and test networks

9. Track and monitor all access to network resources and cardholder data
10. Regularly test security systems and process

Maintain an Information Security Policy

12. Maintain a policy that addresses information security for all personnel

arcon

PCI Security Standard Council recommends a three pronged approach to protect the payment card transaction environment

Assess

Identifying all locations of cardholder data, taking an inventory of your IT assets and businesses processes and analyzing them for vulnerabilities that could expose card holder data

Repair

fixing identified vulnerabilities, securely removing any unnecessary cardholder data storage and implementing secure business process

Report

documenting assessment and remediation details and submitting compliance reports to the acquiring bank and card brands you do business with

Road to Robust Security: ARCON Privileged Access Management

In most cases, security breaches occur due to compromised privileged credentials. The malicious actor (compromised insider or third party element) uses sophisticated technique and other fraudulent ways to get hold of privileged credentials for gaining access to privileged accounts. These super user administrative accounts provide greater scope for targeting confidential information such as card details than individual accounts do.

Privileged Access Management provides robust security framework and builds foundation of best practices in identity and access control management. It not only protects an organization's payment card processing environment from compromised insiders and third party risks but also from advanced cyber threats targeting privileged access.

ARCON | Privileged Access Management enables an organization to overcome the challenge of identity and access control. The solution provides a secure gateway to target systems. It acts a centralized policy engine to authorize and authenticate privileged end users and provides granular control, real time monitoring and robust password vaulting to ensure secure and authorized access to target systems in payment card processing environment.

PCI DSS compliance with ARCON | PAM

Authenticate end users

Reinforcing access control in your payment card environment through strong authentication measures

Identify end users and strengthen logical access control:

Segregate end users and their access to payment devices, privileged accounts in payment card environment and payment applications based on "need-to-know" and "need-to-do-basis"

Restrict privileged users

Monitor and control privileged users in payment card transaction environment through granular level control

Password security

Frequently change and rotate password through robust password vaulting

Centralized policy framework

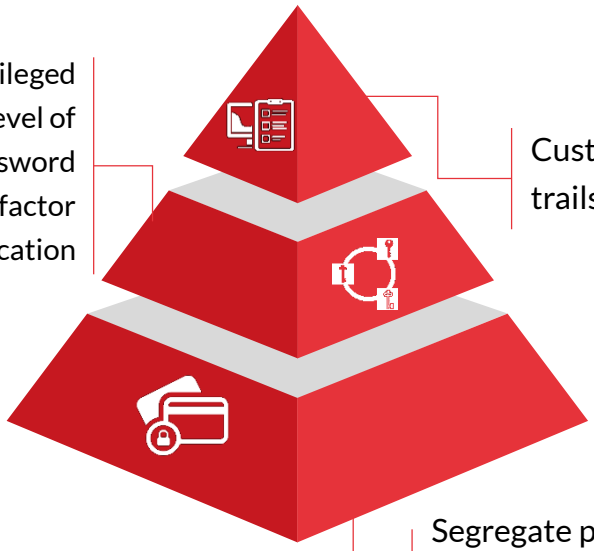
Defining users' role and privileged access to systems and devices

Reporting and audit

Capture logs and generate comprehensive reports on all activities around payment card environment via audit trails

Safeguarding card processing & transaction environment

Restrict and monitor privileged users by applying deepest level of granular control, robust password vaulting and multi factor authentication



Customized report and audit trails of all privileged activities

Segregate privileged users and control payment card environment through centralized policy framework

arcon

PCI DSS guidelines and compliance mapping

7.1	**Limit access to system components and cardholder data to only those individuals whose job requires such access**
Guidance	The more people who have access to cardholder data, higher the risk to user's account of being maliciously used. Limiting access to those with a legitimate business reason helps an organization prevent mishandling of cardholder data from malicious actors such as compromise insiders.
Solution	ARCON | PAM Solution provides the feature of Access Control. The solution enables Virtual Grouping that allows classification of servers (On the Basis of Type) and Users (On the Basis of Teams) so that the access can be controlled. It also provides time based access to end users. Further ARCON | PAM Solution has feature of restriction and elevation of commands (For Database and SSL based connection) and Process (for Windows) which can restrict critical activities on target device even when end user has access to a target device using privilege IDs.

7.1.1	Define access needs for each role, 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.
Guidance	In order to limit access to cardholder data to only those individuals who need access, first it is necessary to define access needs for each role (for example, system administrator, call center personnel, store clerk), the systems/devices/data each role needs access to, and the level of privilege each role needs to effectively perform assigned tasks. Once roles and corresponding access needs are defined, individuals can be granted access accordingly.
Solution	Security team can define L1, L2 or L3 access to target device for each end user. Further we can use command and process restriction and elevation to control the access at granular level.

PCI DSS guidelines and compliance mapping

7.1.2	**Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.**
Guidance	When assigning privileged IDs, it is important to assign individuals only the privileges they need to perform their job (the "least privileges"). For example, the database administrator or backup administrator should not be assigned the same privileges as the overall systems administrator. Assigning least privileges helps prevent users without sufficient knowledge about the application from incorrectly or accidentally changing application configuration or altering its security settings. Enforcing least privilege also helps to minimize the scope of damage if an unauthorized person gains access to a user ID.
Solution	There are multiple ways to define access control for each end user and target device. ARCON's secure gateway server serves as a centralized policy engine to restrict, control, and monitor privileges to a target devices. It enables to assign and segregate end-users with access to target systems based on roles/departments/teams. Thus, it mitigates the chances of illegitimate data processing or data breach as all end-users in PCI environments are granted access to any database only on centralized governing policy. The solution enforces the principle of least privilege. All administrators, IT operators and other privilege users are allowed to login to any target device only on 'need-to-know' and ' need-to-do' basis.

PCI DSS guidelines and compliance mapping

7.1.3	Assign access based on individual personnel's job classification and function.
Guidance	Once needs are defined for user roles (per PCI DSS requirement 7.1.1), it is easy to grant individuals access according to their job classification and function by using the already-created roles.
Solution	ARCON | PAM Solution has a feature of User Access Review. Time interval can be set for a periodic review.

7.1.4	Require documented approval by authorized parties specifying required privileges.
Guidance	Documented approval (for example, in writing or electronically) assures that those with access and privileges are known and authorized by management, and that their access is necessary for their job function.
Solution	ARCON | PAM Solution provides Audit Trails of all the privileges assigned to Users. This can be reviewed at any time by management to validate their privileges

7.2	Establish an access control system(s) for systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
Guidance	Without a mechanism to restrict access based on user's need to know, a user may unknowingly be granted access to cardholder data. Access control systems automate the process of restricting access and assigning privileges. Additionally, a default "deny-all" setting ensures no one is granted access until and unless a rule is established specifically granting such access. Entities may have one or more access controls systems to manage user access.
Solution	ARCON | PAM enables command and process restriction and elevation to control the access at granular level thus protecting the payment card processing environment.

PCI DSS guidelines and compliance mapping

7.2.2	Assignment of privileges to individuals based on job classification and function.
Guidance	The PCI Security standards essentially requires that access control systems are configured to enforce privileges assigned to individuals based on job classification and function.
Solution	Privileges and access to Each Device can be defined for individual End User based on his Job classification and function.

8.1.2	Control addition, deletion, and modification of user IDs, credentials, and other identifier objects
Guidance	To ensure that user accounts granted access to systems are all valid and recognized users, strong processes must manage all changes to user IDs and other authentication credentials, including adding new ones and modifying or deleting existing ones.
Solution	Workflow with multiple level of approvals can be implemented for adding, deletion and modification of end-users and devices through ARCON | PAM.

10.2.2	All actions taken by any individual with root or administrative privileges
Guidance	Accounts with increased privileges, such as the “administrator” or “root” account, have the potential to greatly impact the security or operational functionality of a system. Without a log of the activities performed, an organization is unable to trace any issues resulting from an administrative mistake or misuse of privilege back to the specific action and individual.
Solution	ARCON | PAM Solution Logs each and every activity performed by end user on Target Device in video and text form. Every command or query executed by the end user gets captured. Further we can also set real time alerts to ARCON | PAM Solution Administrators when any Critical Command/ Queries are executed by End User on Target Device.

PCI DSS guidelines and compliance maping

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
Guidance	Without knowing who was logged on at the time of an incident, it is impossible to identify the accounts that may have been used. Additionally, malicious users may attempt to manipulate the authentication controls with the intent of bypassing them or impersonating a valid account.
Solution	Each and every activity performed by end User is captured in text and video format. ARCON | PAM Solution also has a feature to discover privilege IDs present on the target device and will also show if it is managed or not managed by ARCON | PAM Solution.

About ARCON

ARCON is a leading Information Risk Management solutions provider specializing in Privileged Access Management and Continuous Risk Assessment solutions.

ARCON Privileged Access Management (PAM) is a leading global product and a robust solution that mitigates risks arising out of privilege identity and access management.

Connect with us