Comprehensive PCI DSS Compliance Enforcement and Automation

Atomicorp Ensures Compliance in the Cloud, the Datacenter and in Hybrid Environments

Introduction

Payment Card Industry Data Security Standard (PCI DSS) is a collection of security controls that businesses and government agencies that collect credit card data are required to implement. Founded in 2004, PCI DSS is comprised of 12 general requirements and associated sub-controls. Any organization that processes any type of payment card; debit or credit, must meet these requirements or face fines and possible termination of the rights to process payment cards. If an organization does not receive payment card information, but are responsible for storing or transmitting such data, they are still held under the PCI DSS requirements.

It's not sufficient for organizations that must adhere to PCI DSS requirements to meet those requirements at a given point in time. They are required to maintain a consistent state of compliance which is challenging for many organizations. It requires comprehensive, continuous visibility into system settings, configuration and security control implementations. It also requires proactive and continuous system monitoring to ensure systems remain compliant without lapses.

It requires quick and easy assessment of system security posture and control compliance at any time and rule sets to perform compliance checks. Detailed reports are needed to assist in compliance efforts and Assessment and Authorization (A&A) activities. Inevitably, automation is required.

The remainder of this white paper looks at each of the PCI DSS requirements that can be met with the aid of software and how Atomic Enterprise OSSEC (AEO) and Atomic Workload Protection (AWP), from Atomicorp, can be used to help organizations meet 99 of the 100 controls that can be met with the aid of software.

Payment Card Industry Data Security Standard (PCI DSS) Controls

For purposes of this whitepaper, the PCI DSS controls are consolidated into these five categories:

Build and maintain a secure network

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

Protect cardholder data

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

Maintain a vulnerability management program

Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement strong access control measures

Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access

Regularly Monitor and Test Networks

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

Of course, there are only so many controls that can be brought into compliance using software. Physically securing premises that house cardholder data or establishing a strong security policy are beyond the scope of software. Out of the 100 PCI DSS controls that can be met using software solutions, Atomic Enterprise OSSEC and Atomic Workload Protection are the only two solutions on the market today that can meet 99 of those. Let's explore that further...

Build and maintain a secure network

Atomicorp solutions include an integrated stateful firewall that automatically configures itself based on system policy, PCI DSS requirements and a least privilege "deny all" policy restricting inbound and outbound traffic to only that which is required for the cardholder data environment. AEO and AWP force the changing of all vendor defaults at installation and automatically harden systems to virtually any standard including Center for Internet Security (CIS), International Organization for Standardization (ISO), SysAdmin, Audit, Network and Security Institute (SANS), and the National Institute of Standards and Technology (NIST) (recommended by PCI DSS). They also automatically disable all unnecessary services and disable insecure protocols and weak / vulnerable ciphers. AEO and AWP reconfigure systems to use strong protocols such as TLS 1.0-1.2, and reconfigure services to the most secure settings (example: disable root logins in SSH, require two-factor-authentication, etc.).

Protect cardholder data

AEO and AWP detect cardholder information on the system and prevent egress (data loss) by automatically redacting it. Role Based Access Control enables the enforcement of mandatory access controls, limiting access to only those who should have access. AEO and AWP also generate strong cryptographic keys and secure the storage of these keys.

As previously mentioned, these software solutions automatically reconfigure systems to use strong protocols. They also, disable weak ciphers and enable strong ciphers (for example they ensure TLS based services to meet at least A-grade levels as defined by Qualys SSL labs). These enforcements occur for both the client and server-side connections.

PCI DSS controls include the restriction of using PAN (live production) data for testing or development. AEO and AWP can detect PAN data which can then be used to enforce this requirement.

Maintain a Vulnerability Management System

AEO and AWP include anti-virus software and automatically remove or quarantine malware. These solutions prevent the disablement of the anti-virus software by end users unless specifically authorized by management on a case-by-case basis for a limited time period. Alerts are generated if disablement is attempted.

Unlike other solutions on the market, AEO and AWP automatically remove web malware in real-time from compromised websites without quarantining compromised code and

even modifying code on the disk. AEO and AWP integrate with vulnerability scanners and reconfigure the system based on scan results. Audit logs are retained in accordance with PCI DSS requirements.

AEO and AWP produce regular threat reports, cross referenced with vulnerabilities and weaknesses that the solutions have provided protection against as well as vulnerabilities not previously identified. Both solutions generate alerts when patches are missing and include a "virtual patching" capability which in many cases, eliminates the need to install patches. This virtual patching system is designed to either immunize the system from weaknesses (making vulnerabilities that rely on them inert and patching therefore unnecessary) or virtually patching the application, eliminating the vulnerability.

AEO and AWP can detect PAN data, thereby preventing it from being used in testing or development environments. Additional security is provided by reconfiguration of the system to prevent use of insecure communications. Furthermore, improper error handling is detected and users are prevented from the display of this data.

Implement Strong Access Control Measures

AEO and AWP incorporate strong access control capabilities. Alerts are sent on inactive accounts and the products can be configured to automatically disable them. AEO and AWP also send alerts when accounts are used outside of authorized time periods. They detect and block repeated access attempts by locking out the account and can block further access from the source(s) to other accounts. Accounts are locked out for a minimum of 30 minutes or until an administrator re-enables the ID. This is all configurable and lock time limits can be as long as required. These solutions can enforce re-authentication of idle accounts after a period of time (default is 15 minutes).

AEO and AWP configure services to user two-factor-authentication for services that allow it and send alerts on services that don't. The system is automatically configured to use cryptographically secure protocols and require strong passwords in excess of the PCI DSS requirements. Alerts are sent and legacy accounts are locked that do not meet these requirements. These Atomicorp solutions configure the system to require user password / passphrase changes at least every 90 days. System restrict password changes are automatically configured in accordance with PCI DSS requirements. AEO and AWP remove or lock out standard shared accounts and can be configured to do this for additional accounts.

Regularly Monitor and Test Networks

Real-time File Integrity Monitoring (FIM) is provided in AEO and AWP and detects and alerts changes to logs and cryptographically signs the logs making modification both preventable and detectable. They limit the viewing of audit trails to just those people with a job-related need and can add additional safeguards through Role Based Access Control. Audit trails require prompt back up to a centralized log server or media that can't be altered. AEO supports this by allowing audit trail files to be sent to remote servers using multiple methods including remote system log, JSON, XML, remote database(s) and Amazon Glacier. Role Based Access Control also detects and alerts on unauthorized modifications of critical system files, configuration files, and content files.

PCI DSS recommends that logs and security events for all system components be reviewed daily to identify anomalies or suspicious activity. AEO and AWP incorporate continuous monitoring and logging of security events, system components and much more. Audit trails are automatically retained for one year and provide a minimum of 3 months immediate availability for analysis.

Atomicorp solutions include a host vulnerability scanner that automatically runs hourly to meet the test requirements of security systems and processes. For network intrusion protection, these solutions include a web application firewall, host-based intrusion protection, and network intrusion protection.

The following are specific PCI DSS Requirements that Atomicorp solutions meet:

Requirement 1: Install and maintain a firewall configuration to protect cardholder data	
1.1.4	Establish and implement firewall and router configuration standards that include a firewall at each internet connection and between any demilitarized zone and the internal network zone.
1.2.1	Build firewall and router configurations that restrict inbound and outbound traffic to that which is necessary for the cardholder data environment and specifically deny all other traffic.
1.3.1	Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.
1.3.2	Limit inbound Internet traffic to IP addresses within the DMZ.
1.3.3	Implement anti-spoofing measures to detect and block forged source IP addresses from entering the network.
1.3.4	Prohibit direct public access between the Internet and any system component in the cardholder data environment.
1.3.5	Permit only "established" connections into the network.
1.3.6	Place system components that store cardholder data in an internal network zone, segregated from the DMZ and other untrusted networks.

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters	
2.1	Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network.
2.1.1	For wireless environments connected to the cardholder data environment or transmitting cardholder data, change ALL wireless vendor defaults at installation, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: Center for Internet Security (CIS), International Organization for Standardization (ISO).
2.2.2	Enable only necessary services, protocols, daemons, etc., as required for the function of the system.
2.2.3	Implement additional security features for any required services, protocols, or daemons that are considered to be insecure.
2.6	Shared hosting providers must protect each entity's hosted environment and cardholder data as detailed in Appendix A1.
Requirement 3: Protect stored cardholder data	
3.4	Render PAN unreadable anywhere it is stored by using any of the following approaches: one-way hashes based on strong cryptography, truncation, index tokens and pads or strong cryptography with associated key-management processes and procedures.
3.5.1	Document and implement procedures to protect keys used to secure stored cardholder data against disclosure and misuse.
3.6	Fully document and implement all key-management processes and procedures for cryptographic keys used for encryption of cardholder data.
3.6.1	Generate strong cryptographic keys.
3.6.3	Secure cryptographic key storage.
Requirement 4: Encrypt transmission of cardholder data across open, public networks	
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data during transmission.
Requirement 5: Use and regularly update anti-virus software or programs	
5.1	Deploy anti-virus software on all systems.
5.1.1	Deploy anti-virus software on systems capable of detecting, removing and protecting against all known types of malicious software.
5.1.2	Ensure that anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.
5.2	Ensure that all anti-virus mechanisms are kept current, perform periodic scans and generate and retain audit logs.
5.3	Ensure that anti-virus mechanisms are actively running and cannot be disabled or altered by users, unless specifically authorized.

Requirement 6: Develop and maintain secure systems and applications	
6.1	Establish a process to identify security vulnerabilities, using reputable outside sources for security vulnerability information, and assign a risk ranking to newly discovered security vulnerabilities.
6.2	Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.
6.4.3	Production data (live PANs) are not used for testing or development.
6.5	Address common coding vulnerabilities in software development processes.
6.5.2	Buffer overflows.
6.5.3	Insecure cryptographic storage.
6.5.4	Insecure communications.
6.5.5	Improper error handling.
6.5.6	All "high risk" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.1).
6.5.7	Cross-site scripting (XSS).
6.5.8	Improper access control (such as insecure direct object references, failure to restrict URL access, directory transversal, and failure to restrict user access to functions).
6.5.9	Cross-site request forgery (CSRF).
6.5.10	Broken authentication and session management.
6.6	For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either: reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; or by Installing an automated technical solution that detects and prevents web-based attacks in front of public-facing web applications, to continually check all traffic.
Requirement 7: Restrict access to cardholder data by business need to know	
7.1	Limit access to system components and cardholder data to only those individuals whose job requires such access.
7.1.1	Define access needs for each role, including system components and data resources required for a job function and level of privilege required.
7.1.2	Restrict access to privileged user IDs to least privileges necessary to perform job responsibilities.
7.1.3	Assign access based on individual personnel's job classification and function.
7.1.4	Require documented approval by authorized parties specifying required privileges.
7.2.1	Establish an access control system(s) for all systems components that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.
7.2.2	Assignment of privileges to individuals based on job classification and function.
7.2.3	Default "deny-all" setting.

Requirement 8: Assign a unique ID to each person with computer access	
8.1.4	Remove/disable inactive user accounts within 90 days.
8.1.5	Manage IDs used by third parties to access, support, or maintain system components via remote access: enabled only during the time period needed, disabled when not in use and monitored when in use.
8.1.6	Limit repeated access attempts by locking out the user ID after not more than six attempts.
8.1.7	Set the lockout duration to a minimum of 30 minutes or until an administrator enables the user ID.
8.1.8	If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.
8.2	Ensure proper user- authentication management for non-consumer users and administrators on all system components by employing at least one of the following methods to authenticate all users: something you know, something you have, something you are.
8.2.1	Using strong cryptography, render all authentication credentials (such as passwords/phrases) unreadable during transmission and storage on all system components.
8.2.3	Passwords/passphrases must meet the following: a minimum length of at least seven characters and contain both numeric and alphabetic characters.
8.2.4	Change user passwords/passphrases at least once every 90 days.
8.2.5	Do not allow an individual to submit a new password/passphrase that is the same as any of the last four passwords/passphrases he or she has used.
8.2.6	Set passwords/passphrases for first-time use and upon reset to a unique value for each user, and change immediately after the first use.
8.3	Secure all individual non-console administrative access and all remote access to the CDE using multi-factor authentication.
8.5	Do not use group, shared, or generic IDs, passwords or other authentication methods.
Requirement 10: Track and monitor all access to network resources and cardholder data	
10.1	Implement audit trails to link all access to system components to each individual user.
10.2	Implement automated audit trails for all system components to reconstruct the following events:
10.2.1	All individual user accesses to cardholder data.
10.2.2	All actions taken by any individual with root or administrative privileges.
10.2.3	Access to all audit trails.
10.2.4	Invalid logical access attempts.
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.
10.2.6	Initialization, stopping, or pausing of the audit logs.
10.2.7	Creation and deletion of system-level objects.

10.3	Record at least the following audit trail entries for all system components for each event:
10.3.1	User identification.
10.3.2	Type of event.
10.3.3	Data and time.
10.3.4	Success or failure indication.
10.3.5	Origination of event.
10.3.6	Identity or name of affected data, system component, or resource.
10.4.2	Time data is protected.
10.4.3	Time settings are received from industry-accepted time sources.
10.5.1	Limit viewing of audit trails to those with a job-related need.
10.5.2	Protect audit trail files from unauthorized modifications.
10.5.3	Promptly back up audit trail files to a centralized log server or media that is difficult to alter.
10.5.4	Write logs for external-facing technologies onto a secure, centralized, internal log server or media device.
10.5.5	Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts.
10.6.1	Review the following at least daily: all security events; logs of all system components that store, process, or transmit CHD and/or SAD; logs of all critical system components; logs of all servers and system components that perform security functions.
10.6.2	Review logs of all other system components periodically based on the organization's policies and risk management strategy, as determined by the organization's annual risk assessment.
10.7	Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis.
Requirement 11: Regularly test security systems and processes	
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change in the network.
11.2.1	Perform quarterly internal vulnerability scans. Address vulnerabilities and perform rescans to verify all "high risk" vulnerabilities are resolved in accordance with the entity's vulnerability ranking. Scans must be performed by qualified personnel.
11.3	11.3 Implement a methodology for penetration testing that includes the following: · Is based on industry-accepted penetration testing approaches (for example, NIST SP800-115) · Includes coverage for the entire CDE perimeter and critical systems · Includes testing from both inside and outside the network · Includes testing to validate any segmentation and scope-reduction controls · Defines application-layer penetration tests to include, at a minimum, the vulnerabilities listed in Requirement 6.5 · Defines network-layer penetration tests to include components that support network functions as well as operating systems · Includes review and consideration of threats and vulnerabilities experienced in the last 12 months · Specifies retention of penetration testing results and remediation activities results.

11.3.1	Perform external penetration testing at least annually and after any significant infrastructure or application upgrade or modification.
11.3.2	Perform internal penetration testing at least annually and after any significant infrastructure or application upgrade or modification.
11.4	Use intrusion-detection and/or intrusion-prevention techniques to detect and/or prevent intrusions into the network. Monitor all traffic at the perimeter of the cardholder data environment as well as at critical points in the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion-detection and prevention engines, baselines, and signatures up to date.
11.5	Deploy a change-detection mechanism such as FIM to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.
Appendix A1: Additional PCI DSS Requirements for Shared Hosting Providers	
A.1.1	Ensure that each entity only runs processes that have access to that entity's cardholder data environment.
A.1.2	Restrict each entity's access and privileges to its own cardholder data environment only.
A.1.3	Ensure logging and audit trails are enabled and unique to each entity's cardholder data environment and consistent with PCI DSS Requirement 10.
A.1.4	Enable processes to provide for timely forensic investigation in the event of a compromise to any hosted merchant or service provider.

Conclusion

Atomicorp offers the most comprehensive automated solutions available for PCI DSS compliance. Comprehensive visibility and quick, easy, and continuous assessment of an organization's security posture and compliance give administrators and risk governance personnel the assurance they need. Coupled with the disablement of unused accounts, protection and archiving of log files to meet log retention requirements, and disablement of insecure protocols and services, these solutions ensure continuous compliance without the fear of lapses.

Beyond compliance, Atomicorp products offer unified workload security for the cloud, data center and hybrid environments. Built on OSSEC, the world's leading open source server protection platform, Atomicorp solutions extend its power by adding a management GUI, technical support, product upgrades and more, making it a full enterprise-ready solution. AEO and AWP support the DevOps process through automation and integration that enables security and compliance without hindering continuous delivery of new releases. Furthermore, they employ advanced filtering that reduces the "noise" for security operations teams and maintain a light footprint that doesn't increase cloud costs, resulting in demonstrable ROI.

About Atomicorp

Building on the power of OSSEC, the world's leading open source intrusion detection platform, Atomicorp shields enterprise workloads from attack -- in the cloud, on-premise, or in hybrid environments. Atomicorp's automated and adaptive approach to workload protection simplifies both security and operations, ensuring that enterprises can move fast without introducing risks.

ATOMICORP

Headquarters:

10549 Conference Center Drive, Suite 180, Chantilly VA 20151

(703) 299-6667
www.atomicorp.com
info@atomicorp.com