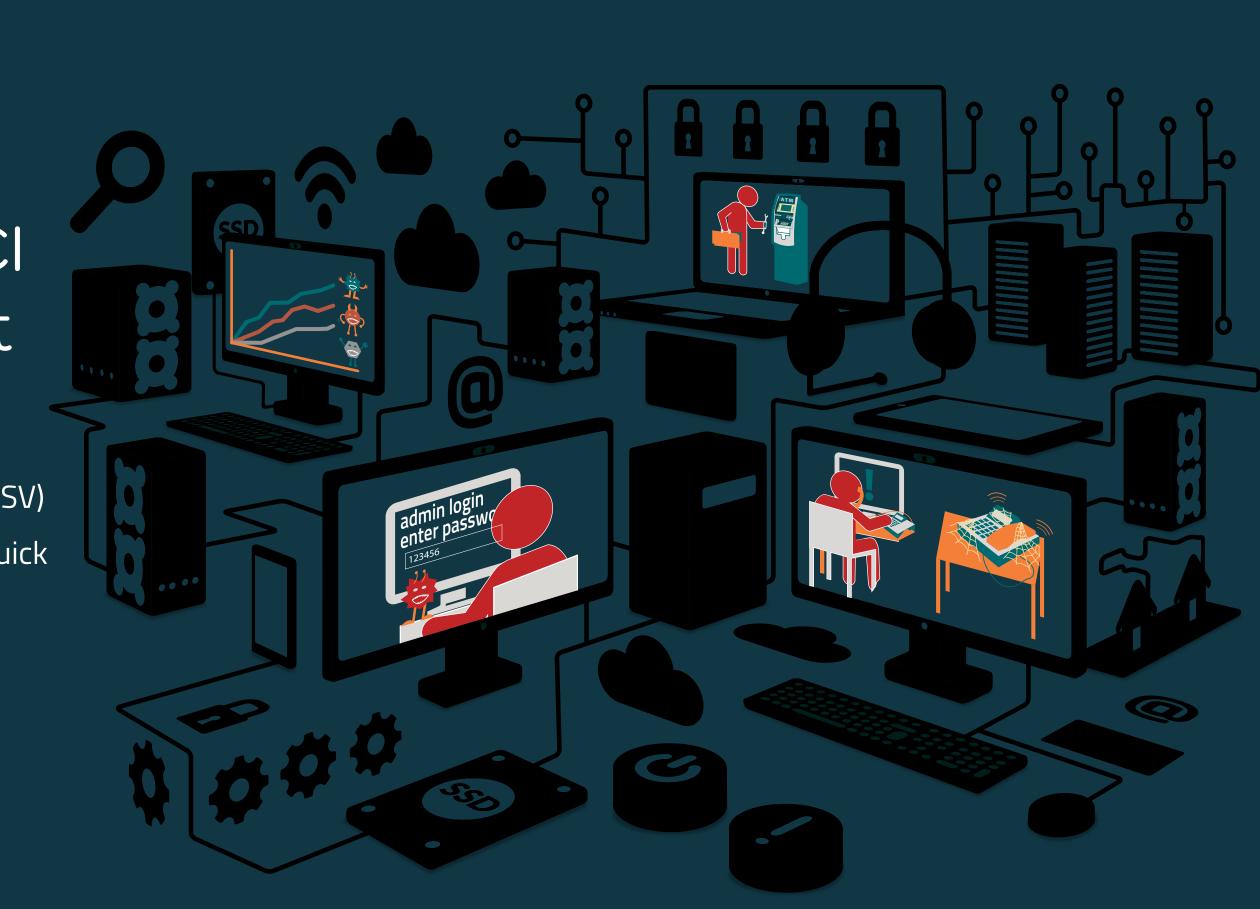


PCI DSS Compliance Services

Let The Experts Help You Meet PCI Compliance and Secure Payment Card Data

Paladion is a Qualified Security Assessor (QSA) and Approved Scanning Vendor (ASV) with well-defined methodologies and technological backup to ensure easy and quick Payment Card Industry Compliance and Certification Solutions. As an industry leader, Paladion provides best in class Information Security Solutions to not only help organizations comply with PCI DSS requirements, but to implement policies and procedures for network architecture, security management, and software design that keep you secure long after certification is attained.



Benefits Of Paladion's PCI DSS Compliance



Showcase the implementation of enhanced security

Enhanced Resilience

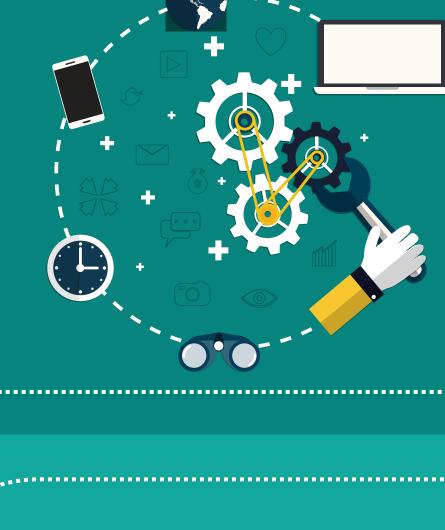
controls to regulators and customers, especially in the wake of recent high profile data breaches at service providers and merchants.

Enable your organization to comfortably extend services

Extended Services

from major payment brands including VISA, Master Card, American Express and acquiring banks in the region.





your organization's security compliance automatic

Expanded Recognition

global recognition.

Satisfying the PCI DSS international standard will give

day zero, putting you first among similar organizations in

Elevated Competition

your region.

Enter into the market as a PCI DSS certified entity from



regularly monitors and tests networks

Goal

The PCI DSS Requirement

Develop and maintain secure systems and applications

Maintain a vulnerability management program that

Regularly test security systems and processes

- Internal and External (ASV) Vulnerability scans Internal and External Network Penetration Tests
- Code Review

PCI Module

- Application Penetration Tests (Black box and Grey box)
- Routers and Switches) Configuration Reviews

Application Security Training

Authorized and Unauthorized (Rogue) Access Points Detection

Access Control List review (for Firewall,

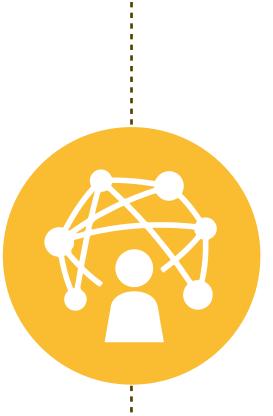
Solution Paladion's PCI Compliance Suite offers solutions

necessary for security testing

Wireless Penetration Tests







run vulnerability scans to help you comply with all standards. PCI Internal and External Network

Penetration Test

PCI Code Review

PCI requirement 11.3 states that you must "Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification." Paladion offers continuous testing of over 200 networks each year to maintain ongoing compliance and ongoing security.

PCI Section 6.3.7 requires a "Review of custom code prior to release to

Paladion has vast experience in code reviewing applications that include

online banking, embedded systems, online trading and document

production or customers in order to identify any potential coding vulnerability."

PCI Standard 11.2 requires that an organization "Run internal and external

the network." As an Approved Scanning Vendor (ASV) and certified by the PCI

council, Paladion uses the industry's leading internal and external scanners to

network vulnerability scans at least quarterly and after any significant change to



PCI Application Penetration Tests PCI Section 11.3.2 asks organizations to "Verify that the penetration test

management systems.

experience in testing more than 1000 applications. Application Security Training PCI requirement 6.5a requires that a company "Verify that processes require training in secure coding techniques for developers, and are based on guidance

such as the OWASP guide." Paladion provides an Application Security Training

Service specifically designed to satisfy this requirement with online training to

includes application-layer penetration tests at least once a year." Paladion has

one of the largest application penetration testing practices in the world with



Access Control List Review (For Firewall, Routers And Switches)

prepare all of your developers in the most cost-effective way.

sets at least every six months." Paladion provides comprehensive assessment of Access Control List reviews for firewalls, routers and switches to assist organizations in remediating and meeting PCI DSS compliance requirements. Configuration Review:

PCI requirement 2.2.3.a requires that a company "Inspect configuration settings

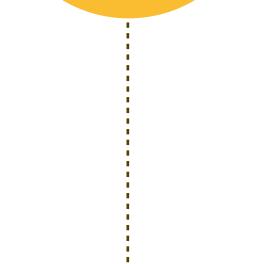
to verify that security features are documented and implemented for all insecure

configuration review methodology, we use scripts developed in-house to collect

configuration settings. The results from these scripts are then analyzed against

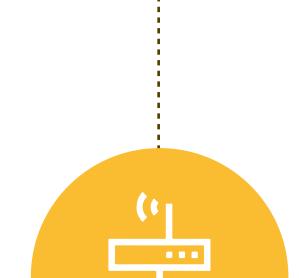
services, daemons, or protocols." In addition to Paladion's non-intrusive

PCI requirement 1.1.7 requires that a company "Review firewall and router rule



the secure configuration checklist from which reports are prepared. Our secure configuration checklist is based on well known standards such as CISecurity,

SANS Top 20, Vendor guidelines, NIST guidelines and our industry experience that complies with PCI DSS requirements. Authorized And Unauthorized (Rogue) Access Points Detection PCI requirement 11.1 demands that a PCI compliant organization "Test for the presence of wireless access points by using a wireless analyzer at least quarterly or deploying a wireless IDS/IPS to identify all wireless devices in use." Paladion



offers cost effective services to detect authorized and unauthorized (rogue) Wireless access points in your network, assist in remediating them and meet the wireless scanning requirements.

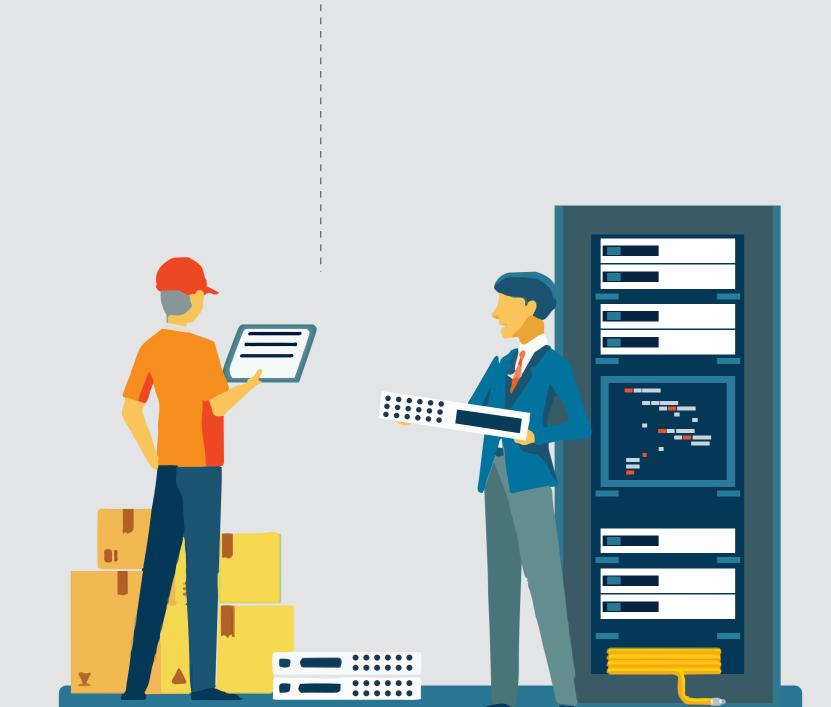
(if any) and meet PCI DSS requirements.

Wireless Penetration Tests As part of PCI requirement 11.3 on penetration tests, the intent of the standard requires penetration tests to be performed on the authorized wireless access points as part of the CDE. Paladion offers cost effective services to conduct

comprehensive wireless penetration tests and recommendations to fix the gaps







Goal

Regularly monitor and test networks

The PCI DSS Requirement

Track and monitor all access to network resources and cardholder data

PCI Module

Remote monitoring and log management

Solution

Paladion's PCI Compliant Log Monitoring Solution is designed specifically to comply with PCI requirements for businesses of all sizes.

Log Services - What You Need



- Real time detection, alert and response
- Attack correlation of logs from multiple sources
- Multi-vendor and platform support
- Support for small and large networks
- Smart utilization of bandwidth
- Incident management Historic forensic analysis
- Online reports
- 250+ pre-defined report templates

The PCI DSS Implementation Methodology

Rich visualization

Scope Identification



- PCI DSS Awareness workshop to highlight the goals and objectives of the standard
- Card business process identification and analysis
- Card data flow analysis and discovery
- Network Segmentation Analysis

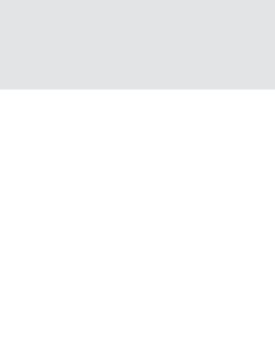
Cardholder Data Matrix and Scope Finalization

Gap Analysis



- Benchmarking existing controls with latest version of PCI DSS
- Identification of security controls achieving compliance
- Suggest roadmap to compliance and assist organizations in achieving certification.

Implementation Support



dashboards and PMO support. Design and Document security processes to meet compliance requirements and

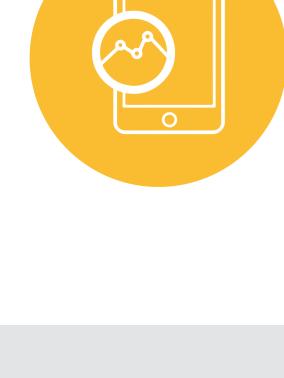
Fine-grained Implementation Tracker with detailed action item mapping,

- assist in implementation of these processes. Evaluate security technological solutions and assist in implementation
- Technical Assessments as per PCI DSS requirements
- ASV Scans
- Security Awareness and Training
- Risk Assessment as per PCI DSS requirements

Conduct external audit by a PCI council approved Qualified

Securty Assessor (QSA)

Certification



- Provide certification documents legally recognized in the globe Report Of Compliance (ROC) and Attestation of Compliance (AOC)
- Provide certification documents recognized globally for branding and marketing purposes - Paladion Digi-seal and certificate

Effective Ways to Achieve PCI Compliance

Fast, Easy and Cost



methodology for clients to achieve PCI compliance in a quick and cost effective manner. An established repository of tools and knowledge for implementing PCI DSS requirements

Paladion has leveraged its extensive experience in the

design, implementation, and maintenance of security

processes and infrastructure to devise a proven

- implementing key controls and meeting documentation and filing requirements
- Cost effective implementation with focus on minimizing investment in new technology and leveraging existing infrastructure

Skilled resources that take ownership for

- Quick and assured achievement of PCI DSS certification Ongoing Security Management Program for PCI DSS
- An easy to use Merchant Compliance Portal

Compliance

WHY PALADION?

Paladion are the experts and leaders in the field with over 400 customers in North America, Asia, and Europe that rely on Paladion for all of their compliance needs. If you are preparing for PCI

compliance, Paladion provides what you need to ensure you exceed all

standards and more importantly, keep your sensitive data secure in the long term. You can select the entire Paladion PCI Compliance suite for comprehensive protection or choose specific modules for an immediate customized compliance program.

ABOUT PALADION

Paladion is a global cyber defense company that provides Managed Detection and Response Services, DevOps Security, Cyber Forensics, Incident Response, and more by tightly bundling its Al platform - Al.saac and advanced managed security services. Paladion is consistently rated and recognized by leading independent analyst firms, and awarded by CRN, Asian Banker, Red Herring, amongst others. For 18 years, Paladion has been actively managing cyber risk for over 700 customers from its

Please visit www.paladion.net for more information.

five Al-Driven SOCs placed across the globe.