Product Brief

AT&T Consulting

SureScan Payment Card Industry (PCI) Approved Scanning Vendor Solutions

Today's vulnerability landscape is ever changing. New threats and vulnerabilities are discovered on a daily basis. Merchants must constantly test their infrastructure in order to ensure that their core assets are protected and that their commitments to comply with the PCI Data Security Standards (PCI DSS) are met.

PCI DSS Security Scanning

All companies that store, process or transmit credit card data are required to comply with the PCI DSS. This standard mandates that merchants and service providers' environments must undergo thorough security vulnerability testing. One of the PCI DSS requirements (PCI DSS Section 11.2) states that an organization must assess its external network through vulnerability scanning on a quarterly basis and after any significant change to the network. Merchants and service providers must arrange for a quarterly scanning review to help ensure that their internet facing systems are free from higher threat vulnerabilities. This must be provided by an "Approved Scanning Vendor" such as AT&T. With AT&T's SureScan PCI Scanning Service, you can meet this requirement.

Vulnerabilities are being discovered continually by malicious individuals and by security consultants, and are also being introduced by new software. System components, processes, and custom software should be tested frequently to ensure security is maintained over time. Testing of security controls is especially important for any environmental changes such as deploying new software or changing system configurations.

Our Methodology

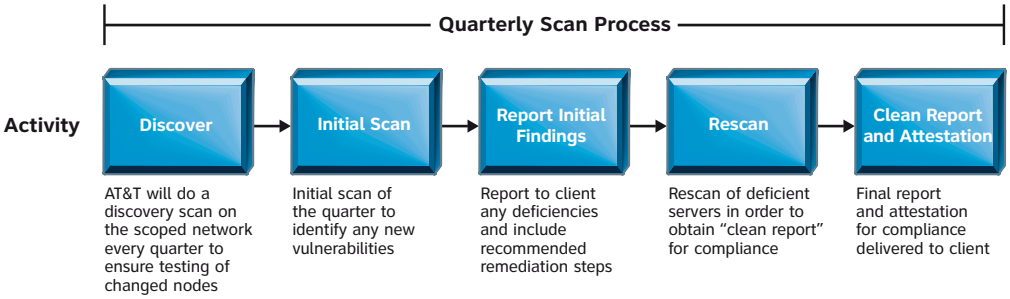
Our approach to PCI scanning is designed to conduct a thorough vulnerability test of your external facing infrastructure. These tests are conducted over the internet and are intended to be non-intrusive to your environment. Our approach is highly collaborative and we will work closely with you during the scan and re-scan process to ensure compliance with scanning timeframes and target scope. The test results are analyzed by a PCI Qualified Security Assessor and submitted to you for review. Once the results are satisfactory, an Attestation report is generated for submission to your acquiring bank. Our goal with this service is to help you achieve and maintain PCI compliance with your scanning obligation.

Benefits

- Provide guidance to remediate potential risks to cardholder data
- Help achieve and maintain PCI Compliance
- Assist with False Positive Management
- Help understand critical exposure points
- Deliver accurate, reliable scanning from an approved PCI scanning vendor
- Conduct non-intrusive scans that will not disrupt your network
- Provide QSA and security expert review of scan results

Features

- Network level vulnerability scans
- Application level vulnerability scans
- Rescans as required



at&t

Pre-assessment Preparation

You would provide a list of IP addresses/ ranges and/or domain names to be included in the test. AT&T provides the originating IP addresses of the scanners to you so that exclusions can be placed in your IDS/IPS systems. This is done to prevent any adaptive traffic suppression by your systems. Before scanning AT&T verifies that no filtering is being performed by your network devices.

Vulnerability Identification

Discovery scanning is conducted using the Internet-facing IP addresses or ranges and DNS names you provide in order to identify active IP addresses (or domains) and services. The IP address found are confirmed with you for correctness and completeness.

The discovered hosts are then subjected to a set of iterative, non-intrusive vulnerability issues which include both network and application level tests. These tests seek to identify the following:

- Operating system type (Fingerprinting)
- Potential vulnerabilities
- Configuration issues
- Obsolete software
- Built in accounts
- Possible backdoor applications
- SSL/TLS testing (versioning, certificate validity/authenticity, matching host name)

The tests are able to test many different platforms and technologies including but not limited to the following:

- Routers
- Firewalls
- Servers (operating systems)
- Databases
- Web Servers
- Applications
- DNS Servers
- Mail Servers
- Wireless Access Points
- Load Balancers

Plug-ins that cause denial-of-service are disabled by default before scanning, unless you specifically request in writing that this not be done.

PCI Data Security Standards

Build & Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data
	2. Do not use vendor-supplied defaults for system 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. Use and regularly update anti-virus
	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. Assign a unique ID to each person with computer access
	9. Restrict physical access to cardholder data
Regularly Monitor & Test Networks	10. Track and monitor all access to network resources and cardholder data
	11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

Categorization and Reporting

The scan results are manually analyzed, correlated and confirmed with the given scope of the tested environment. The framework for this calculation, as required by the PCI DSS, is the Common Vulnerability Scoring System (CVSS), Version 2. CVSS scores range from 0 to 10.0, with 4.0 or higher indicating failure to comply with the PCI standards. For vulnerabilities that are not defined according to the CVSS, the vulnerability severity is determined using the legacy PCI scoring system. This system ranks vulnerabilities on a severity scale from 1-5. Any vulnerability ranking above 2 indicates failure to comply with the PCI standards. In addition, any vulnerability leading to XSS or SQL injection will indicate failure, regardless of CVSS score.

If you believe that certain of AT&T's scan findings are "false positives," you should provide AT&T with documentation and explanation of your concern. AT&T will review your explanation for accuracy and applicability. If we agree that the scan result is a false positive, the scan results will be updated by AT&T.

The overall assessment produces one of two possible results:

- PASSED indicates that the scope is compliant with the PCI DSS
- FAILED indicates that the tested scope is not compliant with the PCI DSS

In addition, the pass/fail of each vulnerability found can be determined by applying the CVSS score logic outlined above.

Reports are created which contain the results of the vulnerability tests of each scanned component and associated infrastructure. The scan report details the type of vulnerability, the severity of the finding, a diagnosis of the issue and guidance on how to fix or patch each vulnerability. Vulnerabilities are categorized by IP address and severity, with the most critical vulnerabilities listed first. Severity is determined by the 1-5 vulnerability categorization that is outlined in the Technical and Operational Requirements for Approved Scan Vendors document[1]. The scan report details are specifically broken down as follows:

- Name
- Industry reference (e.g., Bugtraq ID, CVE, CAN)
- Severity Level
- Common Vulnerability Scoring System (CVSS)
- Comprehensive Explanation
- Solution or Mitigation Recommendations
- Additional References

Each report includes an executive summary as well as a detailed scan findings report. The reports are generated in PDF form and sent to you in a secure fashion. Findings are discussed with you.

PCI Compliance

AT&T can also help you with the other elements of your PCI compliance needs. As a PCI Qualified Security Assessor (QSA), AT&T Consulting performs PCI assessments, PCI readiness assessments and PCI Health Checks for numerous clients (merchants and Service Providers) on an annual basis. AT&T Consulting also offers several managed security services as well as additional security consulting services to help you meet the requirements of the PCI Data Security Standard. These services include vulnerability scanning, penetration testing (network and application), incident response workshops, secure coding training, forensic review and cardholder (or PII) data discovery. AT&T's suite of compliance and compliant services helps reduce the cost and complexity of meeting the PCI Data Security Standard.

Security Solutions: Expertise from a Trusted Provider

AT&T provides a unique and world-class portfolio of compliance and related security services. Our experience, expertise and commitment to open standards have established us as a strategic and trusted advisor. By leveraging AT&T, you can expect best-in-breed solutions, a global network of proven technology, and a cost-effective program-based approach to meet your compliance needs.

Notes

1. https://www.pcisecuritystandards.org/pdfs/pci_dss_technical_and_operational_requirements_for_approved_scanning_vendors_ASVs_v1-1.pdf

For more information, contact an AT&T Representative or visit www.att.com/consulting/security.

10/12/10 AB-2009