



# The McAfee SECURE™ Standard

December 2008

What is the McAfee SECURE Standard?	3
McAfee SECURE Comparison	3
Evaluating Website's Security Status	4
Websites Not In Compliance with McAfee SECURE Standard	4
Benefits of Complying with McAfee SECURE standard	5

The McAfee SECURE™ standard is an aggregate of industry best practices, designed to provide a level of security that an online merchant can reasonably achieve to help provide consumers with better protection when interacting with websites and shopping online.

**What is McAfee SECURE standard?**

In order for a merchant to display the McAfee SECURE trustmark, it is required to submit, at minimum, the target website for auditing and pass the required tests. Sites using Akamai for content distribution should also submit the origin server for audit and review. The website(s) must be audited by McAfee Inc.'s Automated Vulnerability Assessment technology on a daily basis without interference by Intrusion Detection or Intrusion Prevention System.

The McAfee SECURE data security standard is separate from the Payment Card Industry Data Security Standard (PCI-DSS). McAfee SECURE requires daily auditing and certification, whereas PCI DSS requires quarterly scanning by an ASV and SSL doesn't require auditing at all. The appearance of the McAfee SECURE trustmark on a website is not related to the retailer's PCI compliance.

**McAfee SECURE Comparison**

	Security Risk/Issue Identified			Required for Certification		
	McAfee SECURE	PCI	SSL Certificate	McAfee SECURE	PCI	SSL Certificate
SQL Injection	•	•		•	•	
Blind SQL Injection	•	•		•	•	
SQL Database Error Disclosure	•	•		•	•	
Local File and Remote File Includes	•	•		•	•	
Directory Traversals	•	•		•	•	
Improper Error Handling	•	•		Optional	•	
Application Source Code Disclosure	•	•		•	•	
Authentication Bypass	•	•		•	•	
Insufficient Session Expiration	•	•		Optional	•	
Command Injection	•	•		•	•	
SSI Injection	•	•		•	•	
Malicious CGI scripts	•	•		•	•	
Buffer Overflows	•	•		•	•	
Client Side Vulnerabilities	•	•		Optional	•	
Directory Indexing	•	•		Optional	•	
Server Misconfigurations	•	•		Optional	•	
SSL Encryption	•	•	•	Optional	•	•
Malicious Downloads	•			•		
Malicious Affiliations (Links)	•			•		
Phishing Scams	•			•		
Browser Exploits	•			•		
Misuse of personal information	•			•		
Annoyances (excessive Pop-ups)	•			•		
Scams (Business Practices)	•			•		
Scan Frequency	Daily	Quarterly	N/A	Daily	Quarterly	N/A

**Key Points**

**McAfee SECURE Service**

- Comprehensive web security service
- Aggregate of industry best practices
- Daily vulnerability assessment
- Review of web application content

Complying with the standard allows merchants to publicly display their security status with McAfee SECURE trustmark.

**Evaluating Website's Security Status**

When evaluating a website's security, the McAfee SECURE standard considers both the results of a daily vulnerability assessment as well as a review of the web application's content. When reviewing the website's content McAfee looks for malicious downloads (adware, spyware, viruses, trojans), malicious affiliations (links), phishing scams, browser exploits, misuse of personal information (spam), annoyances (excessive pop-ups), and other online scams (business practices). When a security issue/risk is found that violates the McAfee SECURE standard, customers using the trustmark must remediate based on the requirements below.

Additionally, McAfee may also elect to incorporate any credible information obtained from other outside resources. This information may affect the merchant's ability to display the McAfee SECURE trustmark. McAfee supports ongoing research with Responsible Disclosure and works with the security community to foster a collaborative exchange of information as a way to improve a merchant's security and to protect the consumer.

**Websites Not In Compliance with McAfee SECURE standard**

In the event that McAfee discovers a vulnerability that prevents a merchant's website from complying with the McAfee SECURE standard, the merchant will have a 72-hour remediation window. In instances where McAfee believes confidential customer data is at immediate risk, or in those cases where McAfee has evidence of prior compromise, the McAfee SECURE trustmark may be removed before expiration of this 72-hour window.

Domains that have suffered a pre or post-sales compromise must meet additional criteria. In order for these domains to maintain compliance with the McAfee SECURE standard, at least one of the following criteria must be met:

1. Customers must undergo a forensic examination by a PCI Security Standards Council approved Qualified Incident Response Assessor and provide the Report of Compliance. A list of qualified CISP Incident Response Assessors is available at: [http://usa.visa.com/download/merchants/cisp\\_qualified\\_cisp\\_incident\\_response\\_assessors\\_list.pdf](http://usa.visa.com/download/merchants/cisp_qualified_cisp_incident_response_assessors_list.pdf)
2. Customers must relocate their platform to a Visa Validated Payment Application and outsource all credit card transactions: A list of validated payment applications is available at: [http://usa.visa.com/download/merchants/validated\\_payment\\_applications.pdf?it=r/merchants/risk\\_management/cisp\\_payment\\_applications.html|Validated%20Payment%20Applications](http://usa.visa.com/download/merchants/validated_payment_applications.pdf?it=r/merchants/risk_management/cisp_payment_applications.html|Validated%20Payment%20Applications)
3. Customers must host their shopping cart with a Level One certified Application Service Provider on a certified ecommerce application. Usage of Yahoo! Stores, Monster Commerce or another McAfee SECURE trusted provider is acceptable. A list of certified service providers is available at: [http://usa.visa.com/download/merchants/cisp\\_list\\_of\\_cisp\\_compliant\\_service\\_providers.pdf](http://usa.visa.com/download/merchants/cisp_list_of_cisp_compliant_service_providers.pdf)

### Benefits of Complying with McAfee SECURE standard

Vulnerability assessment and the subsequent required remediation are costs that many merchants often choose to avoid. This leaves the consumer unprotected and unaware of the risk to their personal information. The McAfee SECURE service is the de facto method for creating a positive ROI for security. By requiring the merchant to meet a defined level of security and then allowing them to publicly display their achievement in meeting the McAfee SECURE standard, consumers benefit from increased security and awareness. Merchants benefit by the consumer's greater willingness to purchase from sites that display the McAfee SECURE trustmark.

McAfee SECURE service is intended to be one part of an overall security solution that includes properly configured firewalls, intrusion detection and protection systems, antivirus, manual code evaluations, penetration testing and ongoing education. The greatest security is derived from defense in depth, where layers of security provide complementary protection.

