HP Application Security Center and the Payment Card Industry (PCI) Data Security Standard (DSS)

Fact sheet

Legislative summary

The Payment Card Industry (PCI) Data Security Standard (DSS) results from a collaborative effort by Visa, MasterCard, American Express and Discover to protect customers' personal information. The standard establishes 12 security requirements to which all members, merchants and service providers must adhere.

The PCI policy requires that all PCI members, merchants and service providers that store, process or transmit cardholder data must verify all of their purchased and custom web applications, including internal and external web applications.

Mandated since June 2001, the Visa USA-instituted Cardholder Information Security Program (CISP) is intended to protect Visa cardholder data and help members, merchants, and service providers maintain the highest information security standards.

In 2004, as a result of collaboration between Visa and MasterCard, the CISP requirements were incorporated into the PCI DSS. Visa USA maintains CISP as the managing program for data security compliance, endorsing the PCI DSS.

In addition, Visa has developed Payment Application Best Practices to assist software vendors in creating secure payment applications for merchant compliance with the PCI DSS. Software vendors can validate their payment applications against the recommendations outlined in this document.

Achieving legal and regulatory compliance

HP Application Security Center software creates compliance reports that can help you address legal and regulatory compliance for your web applications and web services. These compliance reports support more than 20 laws, regulations and best practices, including PCI DSS. HP Application Security Center software runs automated security checks against the PCI DSS requirements that pertain to web application security and produce a resulting PCI DSS compliance report.

All HP Application Security Center software—HP Assessment Management Platform software, HP WebInspect software, HP QAInspect software and HP DevInspect software—include compliance reports that help you:

- Assess and prove application security throughout the application lifecycle
- Use application security assessment policy templates for each regulation or customize them to fit your environment
- Produce security reports tailored to each regulation and categorized by the sections related to application security
- Stay up to date with changing regulations through immediate SmartUpdate of compliance policies and report changes

Web application requirements for the PCI DSS

HP Application Security Center software helps you comply with sections 6, 11 and 12 of the PCI DSS:

PCI DSS requirements	HP support
Requirement 6: Develop and maintain secure systems and applications Unscrupulous individuals use security vulnerabilities to gain privileged access to systems. Many of these vulnerabilities are fixed via vendor security patches, and all systems should have patches to protect against exploitation by employees, external hackers and viruses. For in-house developed applications, numerous vulnerabilities can be avoided by using standard system development processes and secure coding techniques. In September 2006, Section 6.6 was added to Section 6 of the PCI DSS. HP Application Security Center software meets the web application requirements to review custom application code for common vulnerabilities.	X
Requirement 11: Regularly test security systems and processes Vulnerabilities are continually being discovered by hackers and researchers and introduced by new software. Systems, processes and custom software should be tested frequently to maintain security over time and through changes.	X
Requirement 12: Maintain a policy that addresses information security for employees and contractors A strong security policy sets the security tone for the whole company and lets employees know what is expected of them. All employees should be aware of the sensitivity of data and their responsibilities for protecting it.	X

The following HP Application Security Center capabilities directly support 6, 11 and 12 of the PCI DSS:

- Assess web applications for vulnerabilities that may result in disclosure of sensitive or private information
- Verify that web application access to sensitive information is controlled by authentication and authorization
- Review all custom application code for common vulnerabilities
- Identify web application command injection vulnerabilities that may allow malicious code or programs to be executed
- Validate that web application inputs are properly validated and not vulnerable to command injection or cross-site scripting attacks
- Assess that all data communication is encrypted
- Check for vulnerability to denial of service attacks
- Check for improper application error handling
- Create detailed security assessment reports categorized by PCI DSS sections

To learn more, visit www.hp.com/go/software

4AA1-5366ENW, September 2007

invent