



A Websense® Research Brief

Prevent Data Loss and Comply with Payment Card Industry Data Security Standards

Standards for Credit Card Security

Modern commerce relies heavily on credit card transactions, providing convenience to consumers and more sales opportunities for merchants. With vast amounts of financial capital transferring via these means, it's no wonder that credit card fraud amounts to over a billion dollars in the US alone, according to the US Treasury. The Payment Card Industry Data Security Standards (PCI DSS) were developed by a consortium of credit card issuers, including MasterCard and Visa, to provide best practices for securing IT systems and establishing processes for the use, storage, and transmission of credit card data in electronic commerce.

PCI DSS consists of six categories:

1. Build and maintain a secure network
2. Protect cardholder data
3. Maintain vulnerability program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

"I highly suspect we will see outbound content monitoring and filtering in the next revision of PCI DSS...Consider this your first warning."

Rich Mogull (former Gartner analyst), Securiosis blog, February 2008

In an age of phishing scams, malware, and pursuit of profits by hackers, compliance with PCI DSS is usually interpreted as a way to mitigate the risk of an external threat. Secure Sockets Layer (SSL), Transport Layer Security (TLS), Internet Protocol Security (IPSEC), and other technologies are recommended as safeguards against these threats, focusing on anti-theft and anti-intrusion measures. However, the ultimate concern is the unauthorized use of credit card data, so safeguarding the data, then, is essential to mitigating this risk. Data Loss Prevention (DLP) is the solution to help safeguard this credit card data.

While PCI DSS has done much to establish a common set of security best practices to minimize external hacks into networks where credit card data is transmitted, stored or collected, it has not explicitly mandated the monitoring of this data. As many industry analysts and forward-thinking enterprises have already acknowledged, DLP must be a part of a PCI compliance and credit card data security policy, given that even a single instance of data loss can lead to penalties from card holding institutions and banks, high remediation costs, damage to an organization's reputation, and loss of market share.

DLP is Essential for Compliance with PCI DSS

The PCI DSS does not discriminate between internal and external threats; data loss is data loss, whatever the cause. Yet, the emphasis on external threats is often a distraction from the more likely risk of loss—employees or insiders leaking data. According to Open Security Foundation resource for data loss incidents sponsored by the Open Security Foundation, at least 28 percent of all data loss incidents are attributed to insiders and close to 60 percent of these are attributed to accidental leaks of confidential data.

"Data loss via the Web is four times more likely than email."

Source: Data Loss Open Security Foundation

The causes of data loss are numerous and seemingly mundane, such as:

- Emailing sensitive data using personal accounts (e.g., Yahoo! Mail, Gmail, or Hotmail)
- Posting data to a social networking or other Web 2.0 site (e.g., Facebook, Twitter, or blogs)
- Copying customer data from a CRM or bill payment system to a removable storage drive
- Emailing data to the wrong person, inside or outside your organization
- Emailing unencrypted account numbers to customers, partners, or vendors

Whether erroneous or intentional, the outcome is equally damaging since once customer credit card information is accessed by an unauthorized user, the data is assumed to be compromised.

Restoring customer confidence following a leak is not easy. The damage to a customer's credit and confidence combined with the tarnished reputation of the company (a merchant, payment service provider or any entity storing, processing, or transmitting credit card data) can last for years. Often, a breach can require credit monitoring services for affected customers, payment of legal settlements, and result in lost business. Internally, the company would have to reengineer business processes to avoid such a leak in the future, invest in restoring the brand, and pay for information control audits for up to five years. In the end, the loss of credit card information can impact the bottom line and the business may never be the same.

A data loss prevention solution, consisting of secure business processes, employee education, and technology can reduce the risk of leaks and help you attain PCI DSS compliance. In a transaction-heavy environment, an automated solution is critical to be operationally feasible. DLP technologies can monitor the enterprise and automatically enforce information controls and notify business managers. However, it's important to note that not all DLP solutions are equal. Different technology approaches yield varying results. For thorough PCI DSS compliance, a careful DLP solution selection process is necessary.

PCI DSS and Websense Data Security Suite

The Websense® Data Security Suite takes a unique approach to data loss prevention and information control which can be applied to the specific challenge of protecting credit card data.

Websense offers both a comprehensive and modular solution which grants full visibility into key business activities where confidential data may be handled. Destination awareness and control for Web and email on the network, combined with application and device control for endpoints, exceed typical DLP offerings while addressing operational concerns around deployment and ongoing management. The solution delivers accuracy and policy granularity providing knowledge of **who** sent the data, **how** it is being sent or used, **where** it is going, and **what** type of data it is, such as credit card data. With this level of accuracy, appropriate enforcement actions to protect the data can be made without fear of disrupting legitimate business processes.

Websense Data Security Suite includes four integrated modules, managed under a single policy framework, which together provide visibility and control over network and endpoint data loss as well as comprehensive data discovery across enterprise storage systems. Depending on which infrastructure area is deemed to be of highest risk, one or more of these modules can be deployed at any given time.

- [Websense Data Monitor](#) – Monitors network for data loss across Web, email, and instant messaging channels, and includes enhanced visibility with destination awareness and

user details

- Websense Data Protect – (includes Websense Data Monitor) Monitors network channels and enforces automated, policy-based controls to block, quarantine, encrypt, audit and log, or notify users of violations
- Websense Data Endpoint – Monitors and enforces automated, policy-based controls for data usage via applications and peripheral devices on user desktops or laptops. Discovers and classifies confidential data stored on end-user systems.
- Websense Data Discover – Discovers and classifies confidential data stored in enterprise repositories. Automatically remediates discovered data based on policy.

The solution ships with PCI DSS templates that can be modified to align with specific information security policies. For example, you can configure it to alert stakeholders only if an email has at least five instances of records containing a credit card number and the associated three-digit or four-digit CVV (card verification value, to protect against card-not-present fraud). The reason for this threshold may be that an email with only one credit card record may indicate a personal transaction. If needed, the five-record threshold could be changed to as low as one or as high as the organization deems appropriate based on PCI DSS compliance policies. For even more accurate detection of a high-risk leak, a customer data file containing portions of credit card data (e.g. last four digits), could be “fingerprinted”, allowing this snapshot to be compared with what is identified by the solution, to determine if an actual customer’s data was compromised or if a non-customer credit card number was detected.

A comprehensive yet modular DLP offering with accuracy in credit card detection as well as user and destination awareness has established Websense as a leader in the DLP space and makes Websense Data Security Suite an ideal choice for protecting credit card data in enterprises where PCI compliance is a must.

To learn more about Websense DLP solutions through a demonstration of the solution, visit www.websense.com/evaluations.

The designated DLP modules below indicate the *minimum* solution offering required to address the respective PCI requirements. The Websense Data Security Suite, comprising all modules, addresses all of the listed PCI requirements. Modules are designed to address visibility and control in different areas of the enterprise: network communications, network storage servers, and end-user systems.

PCI DSS Requirement	Requirement Satisfaction	Websense Data Security Suite			
		Data Monitor	Data Protect	Data Discover	Data Endpoint
3.1: Keep cardholder data storage to a minimum. Develop a data retention and disposal policy. Limit storage amount and retention time to that which is required for businesses, legal, and regulatory purposes, as documented in the data retention policy.	Automatically discover cardholder data stored throughout the enterprise—on desktops, laptops, file servers (including SharePoint), and email servers (including Exchange) and in databases (with native connectors)—that is in violation of the PCI data retention and disposal policy. Once discovered, the solution can automatically enforce pre-defined actions based on policy, including file quarantining, encryption (through third-party file encryption solution), transfer, replacement and removal. Ensures that copies of cardholder data are not stored in violation of corporate and regulatory policy.	●		●	
3.2: Do not store sensitive authentication data subsequent to authorization (even if encrypted). Sensitive authentication data includes the data as cited in the requirements 3.2.1 through 3.2.3.	Automatically discover sensitive authentication data, card validation codes, and personal identification numbers stored throughout the enterprise. It can also monitor for use or transmission of any such information. Once identified, data can be remediated by any number of pre-defined or custom actions, including file quarantining, encryption, transfer, replacement and removal.			●	
3.3: Mask the primary account number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed).	Credit card data can be found in transit on the network, stored on network servers, or on end-user systems. Incident management reports provide forensics of PCI violations while masking the PAN. Configuration with role-based access control to limit administrator and auditor views of incident details further mitigate risk of unauthorized user seeing credit card data.	●	●	●	●
3.4: Render PAN, at minimum, unreadable anywhere it is stored (including on portable digital media, backup media, in logs).	Identify and report on the location of primary account numbers stored throughout the enterprise. Based on policy, automatically enforce file encryption and other custom actions to remediate the violation.		●	●	●

PCI DSS Requirement	Requirement Satisfaction	Websense Data Security Suite			
		Data Monitor	Data Protect	Data Discover	Data Endpoint
3.5: Protect cryptographic keys used for encryption of cardholder data against both disclosure and misuse.	Monitors internal and external communications channels, including Web, email, FTP, IM, print, and more and can automatically detect unsecured encryption keys and prevent misuse and disclosure. The solution can also automatically trigger rights management to restrict access controls to encryption key based on custodial policies. Built-in discovery capabilities enable managers to transparently scan the enterprise for unsecured keys and secure them.	●	●	●	●
4.2: Never send unencrypted PANs by email.	Monitors email communications—both internal and external—and can accurately identify unencrypted PANs (including in attachments) and route the communication to an email encryption gateway for encryption. This methodology is widely used to protect cardholder data and other confidential information. Automated enforcement by blocking, routing to an encryption gateway, or quarantining the data addresses this requirement.		●		
6.3.4: Production data (live PANs) are not used for testing and development.	Discover live PANs resident on test systems (servers, end-user systems) and automatically enforce a predefined or manual action to secure the data (e.g. remove the data; copy it to a secure location). It can also monitor network communications between test systems to ensure cardholder information is not in use over email, Web, FTP, or printing. Attempts by end users to transfer this data to removable media can also be blocked.	●	●	●	●
7.1: Limit access to system components and cardholder data to only those individuals whose job requires such access.	Identify cardholder information stored in inappropriate locations or with inappropriate access permissions and, with integration with rights management technologies, automatically apply the appropriate access rights to secure its use.			●	●
7.2: Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed.	Restrict file access to specified users based on the type of information they are attempting to access. Administrators can quickly configure a default policy to deny all access to files containing cardholder data unless otherwise specified. Additionally, the solution can restrict all or specified users from cut, copy, paste, print, and print screen if cardholder data is displayed on screen (e.g., by an application).			●	●

PCI DSS Requirement	Requirement Satisfaction	Websense Data Security Suite			
		Data Monitor	Data Protect	Data Discover	Data Endpoint
8.4: Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	Accurately identify cardholder data transmitted on the network over business communication channels and enforce encryption (via integration with an encryption gateway). It can also apply file-level encryption (with integration) for data discovered on network file and storage systems.		●	●	
10: Track and monitor all access to network resources and cardholder data.	Main requirement in this section is to provide a detailed audit trail of access to credit card data. The solution passively monitors access to files containing cardholder data, as well as actions taken when users copy, paste, print, email, FTP, or post to the Web. The solution includes detailed forensics, reporting, and audit tools to provide auditors with the requisite information.	●		●	●
12.2: Develop daily operational security procedures that are consistent with requirements in this specification.	Includes built-in, automated workflow to enable PCI compliance, for both administrators and end users. Automated incident alerts, workflow (e.g. assign incident to data owner), built-in PCI violation reports and integration with security information management (SIEM) solutions streamline the process for administrators. End users can also be automatically notified of their violation in real-time, preventing unnecessary helpdesk calls and improving PCI compliance over time.	●	●	●	●
12.3: Develop usage policies for critical employee-facing technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, personal digital assistants, email use and Internet usage) to define proper use of these technologies for all employees and contractors.	Automated notifications and confirmations of policy violations for employees and contractors. Includes alerts for users and managers, message quarantining (requires manager approval for release). The system is configurable for autonomous operation, utilizing existing messaging tools to permit remediation from the business unit.	●	●	●	●

PCI DSS Requirement	Requirement Satisfaction	Websense Data Security Suite			
		Data Monitor	Data Protect	Data Discover	Data Endpoint
<p>12.5: Assign to an individual or team the following information security management responsibilities:</p> <p>12.5.1: Establish, document, and distribute security policies and procedures.</p> <p>12.5.2: Monitor and analyze security alerts and information, and distribute to appropriate personnel.</p> <p>12.5.3: Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.</p> <p>12.5.5: Monitor and control all access to data.</p>	<p>Websense Data Security Suite has automated incident alerting for users, their managers, and security administrators. Alerts can be customized and include incident details. The solution also includes advanced reporting that can be scheduled for automated distribution. Incidents related to specific policy violations can be disseminated on a daily, weekly, monthly or configurable schedule to anyone in the enterprise. An audit trail is kept within the system to provide details of incident response, and group managers can monitor and report on the progress of individual incident managers.</p> <p>All incident detail providing within the Websense Data Security Suite is secured based on user access privileges.</p>	●	●	●	●
<p>12.6: Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.</p>	<p>Automated, customizable notifications for data at rest, in use, and in motion. Notification templates communicate security policy to end users and their managers automatically at the time of the violation, and provide instruction on how to avoid similar incidents in the future.</p>	●	●	●	●
<p>12.9: Implement an incident response plan. Be prepared to respond immediately to a system breach.</p>	<p>Provides both passive monitoring and automated enforcement. Centralized management and reporting permits administrators to quickly identify and respond to policy violations for network communications, network storage services, and end-user systems. The solution includes built-in trend analysis and reporting to provide visibility and help create, implement, and evaluate the effectiveness of incident response.</p>	●	●	●	●