



A Websense® Research Brief

Prevent Data Loss and Comply with PCI

Standards for Credit Card Security

More than a decade after the commercialization of the Internet, many remain afraid to shop online. A plethora of responses have emerged, with 63% of online retailers requiring Card Verification Value (CVV) at checkout and 47% displaying logos such as “Hacker Safe” on their home pages.¹ In addition to these individual measures, the credit card industry adopted almost universally the Payment Card Industry Data Security Standards (PCI DSS). PCI DSS provides for the secure payment and processing of merchants and shoppers, and demonstrates a commitment to data security from the industry.

PCI DSS consists of six categories:

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

In an age of phishing scams, under-encryption, and hackers’ pursuit of profits, PCI DSS is usually interpreted as the mitigation of an external threat. SSL, TLS, IPSEC, and other measures are recommended, emphasizing anti-theft and anti-intrusion measures. However, the risk of data loss is barely acknowledged, despite clear implications under PCI DSS. Compliance with PCI DSS inherently requires the implementation of rigorous data loss prevention (DLP) measures.

Information leaks are much more common than external breaches. Most often caused by error or accident, erroneous data leaks account for 81% of information loss, according to a recent survey by the Ponemon Institute², with the average incident costing \$4.8 million. In a payment processing and storage environment, however, the costs can be even higher, because of the nature of the data. While the need to prevent intrusion is widely accepted, data loss prevention may actually prove more important in the near future. A single leak can lead to high remediation costs, damage to an organization’s reputation, and loss of market share.

PCI DSS Equals DLP

It’s virtually impossible to fully comply with PCI DSS without implementing a data loss prevention solution. Data must be protected from the risk of fraud, wherever that risk lies. The standard 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. Malice factors into only 6% of data loss³, while negligence and error are more common causes, a majority of which is preventable.

The causes of data loss are many and seemingly mundane. Simple mistakes, however, can have catastrophic results. Data loss often results from:

- Emailing sensitive data using personal accounts (e.g., Yahoo! Mail, Gmail, or Hotmail)
- Copying data to the wrong drive
- Sending information to a person you think is authorized to receive it
- Emailing data to the wrong person inside or outside your organization

Whether erroneous or intentional, the outcome is equally damaging. Customer credit card information reaches the public, at which point you surrender all control.

Restoring customer confidence following a leak is not easy. The damage to customers and the company can last for years. Often, a payment card breach can require credit monitoring services for affected customers, payment of legal settlements, and lost business. Internally, you have to reengineer business processes, invest in restoring your brand, and pay for information control audits for up to five years. In the end, your business may never be the same.

A data loss prevention solution, consisting of 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. Data loss prevention 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 and Websense Data Security Suite

The Websense® Data Security Suite takes a unique approach to data loss prevention and information control. Websense uses “Deep Content Control” technology (DCC), which entails a contextual approach to leak prevention. Instead of looking only at data, Websense applies contextual indicators including data source, related data elements (e.g., corresponding data points), the number of records being sent, and end-user

information in order to decide whether a communication is a potential leak or simply the normal business. Context-sensitive data evaluation reduces the number of false negatives (actual data leaks not caught by the solution) and false positives (innocuous data flagged as a leak). In addition to yielding more accurate results, DCC reduces the leak-related workload of business unit leaders and other staff members.

Websense Data Security Suite ships with PCI DSS-related templates that can be modified to align with specific information security policies. For example, you can configure Websense Data Security Suite to alert stakeholders only if an email (for example) has at least five instances of records containing a credit card number and the associating 3-digit or 4-digit CVV. The reason for this threshold may be that an email with only one credit card record may indicate a personal transaction. Of course, 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.

In order to achieve PCI DSS compliance the solution employed must be effective. Byzantine policies and inaccurate solutions can slow the business and increase operating and compliance costs. Using Websense, you can comply with PCI DSS, lower costs, and achieve a higher level of information security.

For a free evaluation of all Websense products or to view our online demos, visit www.websense.com/evaluations.

PCI DSS Requirement	Requirement Satisfaction
<p>PCI DSS 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/or regulatory purposes, as documented in the data retention policy.</p>	<p>Websense Data Security Suite can automatically discover cardholder data stored throughout the enterprise—on desktops, laptops, file servers, and in databases—that is in violation of the PCI data retention and disposal policy. Once discovered, the solution can automatically enact pre-defined actions, including file quarantining, encryption, transfer, and removal. With Websense Data Security Suite organizations can ensure that copies or cardholder data are not stored in violation of corporate and regulatory policy.</p>
<p>PCI DSS 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.</p>	<p>Websense Data Security Suite can 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, administrators can any number of pre-defined or custom actions, including file quarantining, encryption, transfer, and removal.</p>
<p>PCI DSS 3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).</p>	<p>Websense Data Security Suite provides detailed forensics of PCI violations while masking the primary account number (PAN) to comply with PCI DSS 3.3. Additionally, forensics and other details can be configured with role-based access and control to limit administrator/auditor views of incident details.</p>
<p>PCI DSS 3.4 Render PAN, at minimum, unreadable anywhere it is stored.</p>	<p>Websense Data Security Suite can identify and report on the location of primary account numbers stored throughout the enterprise. Armed with this information, administrators can use built-in policy controls to automatically launch file encryption and other, custom actions to remediate the violation.</p>
<p>PCI DSS 3.5 Protect encryption keys used for encryption of cardholder data against both disclosure and misuse.</p>	<p>Websense Data Security Suite 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.</p>

PCI DSS Requirement	Requirement Satisfaction
<p>PCI DSS 3.6 Fully document and implement all key management processes and procedures for keys used for encryption of cardholder data.</p>	<p>Websense Data Security Suite enables implementation of key management processes and procedures for encryption keys and cardholder data through automated discovery, monitoring, and control processes as described for PCI DSS 3.1-3.5.</p>
<p>PCI DSS 4.2 Never send unencrypted PANs by email.</p>	<p>Websense Data Security Suite 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.</p>
<p>PCI DSS 6.3.4 Production data (live PANs) are not used for testing and development.</p>	<p>Websense Data Security Suite can discover live PANs resident on test systems and automatically enforce a preset or manual action to secure the data. It can also monitor communications from test systems to ensure cardholder information is not in use, including over email, the web, FTP, print, or transfer to removable media.</p>
<p>PCI DSS 7.1 Limit access to computing resources and cardholder information only to those individuals whose job requires such access.</p>	<p>Websense Data Security Suite can identify cardholder information stored in inappropriate locations and/or with inappropriate access permissions and, with integration with rights management technologies, automatically apply the appropriate access rights to secure its use.</p>
<p>PCI DSS 7.2 Establish a mechanism for systems with multiple users that restricts access based on a user’s need to know and is set to “deny all” unless specifically allowed.</p>	<p>Websense Data Security Suite can restrict file access to specified users based on the type of information they’re 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).</p>
<p>PCI DSS 8.4 Encrypt all passwords during transmission and storage on all system components.</p>	<p>Websense Data Security Suite can accurately identify cardholder data transmitted over business communication channels and force encryption (with integration with an encryption gateway). It can also apply file level encryption (with integration) upon discovering PCI data stored throughout the enterprise.</p>

PCI DSS Requirement	Requirement Satisfaction
<p>PCI DSS 10 Track and monitor all access to network resources and cardholder data.</p>	<p>Websense Data Security Suite can passively monitor or actively enforce (depending on preferred policy) file access to documents containing cardholder data, as well as actions taking 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.</p>
<p>PCI DSS 12.2 Develop daily operational security procedures that are consistent with requirements in this specification.</p>	<p>Websense Data Security Suite includes built-in, automated workflow to increase awareness of the sensitivity of cardholder data and advise employees and contractors of their responsibility for protecting it. Notification and confirmations provide real-time user education and policy enforcement, and integration with security information management solutions provides insight into data use.</p>
<p>PCI DSS 12.3 Develop usage policies for critical employee-facing technologies to define proper use of these technologies for all employees and contractors.</p>	<p>Websense Data Security Suite provides automated notifications and confirmations of policy and policy violations for employees and contractors. It includes alerts for users and managers, including message quarantining, which require manager approval for release (PCI DSS 12.3.1). The system is configurable for autonomous operation, utilizing existing messaging tools to permit remediation from the business unit.</p>
<p>PCI DSS 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>

PCI DSS Requirement

Requirement Satisfaction

PCI DSS 12.6

Implement a formal security awareness program to make all employees aware of the importance of cardholder data security.

Websense Data Security Suite includes 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.

PCI DSS 12.9

Implement an incident response plan. Be prepared to respond immediately to a system breach.

Websense Data Security Suite is a fully integrated DLP solution that provides both passive monitoring and automated enforcement. Centralized management and reporting permits administrators to quickly identify and respond to policy violations for data at rest, in use, and in motion. The solution includes built-in trend analysis and reporting to provide visibility and help create, implement, and evaluate the effectiveness of incident response.