

Proofpoint Solution Brief for PCI DSS Compliance



Proofpoint Messaging Security, Data Loss Prevention and Encryption Solutions



The Payment Card Industry Data Security Standard (PCI DSS) was established in January 2005 to protect credit card data, which includes Primary Account Numbers (PAN), card verification values (CVV), and PIN numbers. The regulation incorporates twelve requirement categories for any company that handles credit card data, including merchants, banks, and payment service providers. The scope of PCI can extend well beyond these obvious target industries, given the wide use of credit cards for non-traditional retail transactions with entities such as online stores, medical providers and government agencies.

PCI DSS compliance challenges

Addressing both PCI compliance and email security creates a burden for compliance officers, internal auditors and IT administrators. Credit card data may exist on end-user systems and travel across the network via high-volume and mission-critical applications such as email. This creates data loss risks as critical information could end up with unauthorized users. These risks can result in non-compliance with PCI, leading to steep fines, increases in transaction fees paid to banks and damage to brand reputation. Data loss also has an adverse impact on IT operations due to ad-hoc remediation efforts and data collection for repeat audits. PCI compliance notwithstanding, businesses also have to contend with relentless spam and virus threats introduced via inbound email, which also impacts productivity and security.

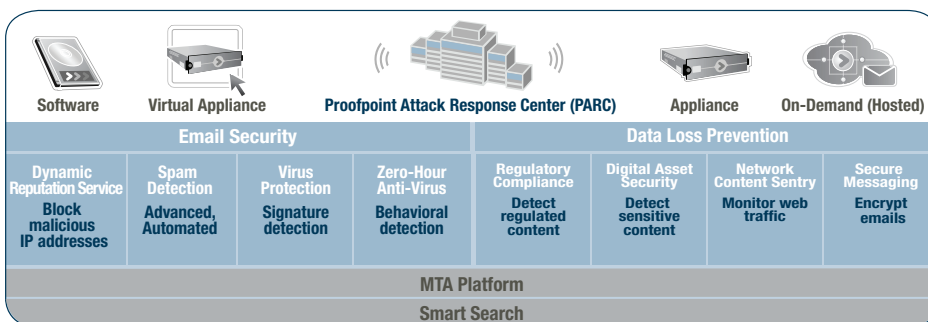
proofpoint solution

Proofpoint addresses PCI DSS challenges with a proven, single-platform solution:

- **Data Loss Prevention (DLP):** Outbound detection over email (SMTP), web (HTTP) and file transfer (FTP) channels
- **Email Security:** Inbound detection and blocking of spam and viruses over email

These solutions can be deployed in any of four form factors. Combined with Proofpoint Attack Response Center (PARC) research, the solution assures timely and accurate anti-spam and zero-hour anti-virus protection.

Proofpoint Solution Platform



Industries Impacted by PCI DSS

- Retail and any entity using credit cards
- Payment Service Providers
- Acquiring and Issuing Banks
- Cardholder Associations
- Credit Unions

Key Business Challenges

- Comply with PCI DSS to avoid penalties (up to \$500K), damage to reputation
- Accurately detect and protect credit card data for Data in Motion to:
 - Comply with PCI DSS Req. 4.2: No unencrypted PANs via email
 - Protect business-sensitive data related to credit card data
- Accurately and efficiently detect and block spam and viruses to:
 - Comply with PCI DSS Req. 5: Use and regularly update anti-virus (AV) (and anti-malware) programs
 - Enable safe, productive email use

Key Enforcement Options to Address PCI DSS Req. 4.2

- Automatically encrypt sensitive emails
- Quarantine and block email and configure workflow
- Educate users on PCI violations

Benefits of Proofpoint's Solution

- Simple and accurate PAN data detection over SMTP, HTTP and FTP
- Policy-based email encryption: automated or user-initiated
- High accuracy anti-spam, anti-virus and malware detection
- Automated blocking with built-in email gateway (MTA)
- Divert training to users responsible for most data loss incidents

Proofpoint Solution Brief for PCI DSS Compliance

Summary of DLP Process

- **Monitor** SMTP, HTTP and FTP
- **Detect** PCI data with pre-defined and customizable techniques
- **Prevent** via automated, policy-based encryption; quarantine to review, release
- **Inform** IT admins, users of violations
- **Report** top violators and trends

Proofpoint DLP Solution Modules

- **Regulatory Compliance:** Policies for industry regulated content
- **Secure Messaging:** Encrypt private data
- **Network Content Sentry:** Visibility across HTTP channels (webmail, blogs)
- **Digital Asset Security:** Policies for business-sensitive data

Key Policy Definition Features

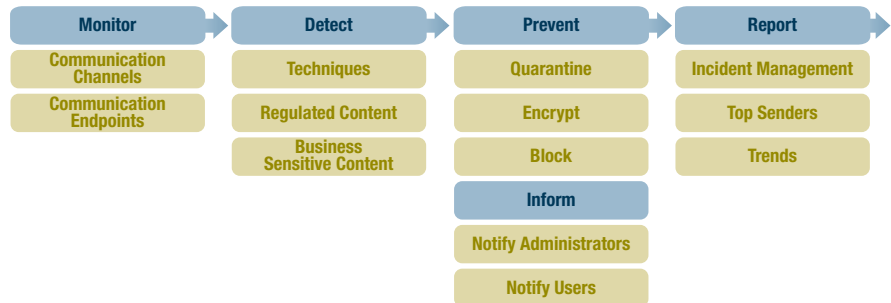
- Pre-defined checks
- Restrict policy to specific routes: sender/recipient, source/destination IP
- Multiple levels of conditions and checks
- Encrypt with one click
- Numerous quarantine options
- Customize user notification with pre-defined fields

Proofpoint Regulatory Compliance Module:

- 1 Simplified PCI rule definition using built-in 'Smart Identifier' and Managed Dictionaries
 - 2 Option to quarantine message with PCI data
 - 3 Quarantine options include discard and continue
 - 4 Single-click to encrypt
 - 5 Inform user with customized message using template fields
 - 6 Comprehensive discard options for emails with PCI data:
- Change subject
 - Change message headers
 - Reply to Sender
 - Send message
 - Notify compliance officer

data loss prevention

PCI Requirement 4.2 mandates that no PAN data be sent via unencrypted email. Proofpoint addresses data loss risks with a network-based solution for data loss prevention which can **monitor** communications; **detect** restricted content; **prevent** through quarantine, encryption or blocking; **inform** administrators and users of policy violations; and **report** on incidents, top violators and trends. The entire process is managed with the simple, easy-to-use Proofpoint unified policy interface.



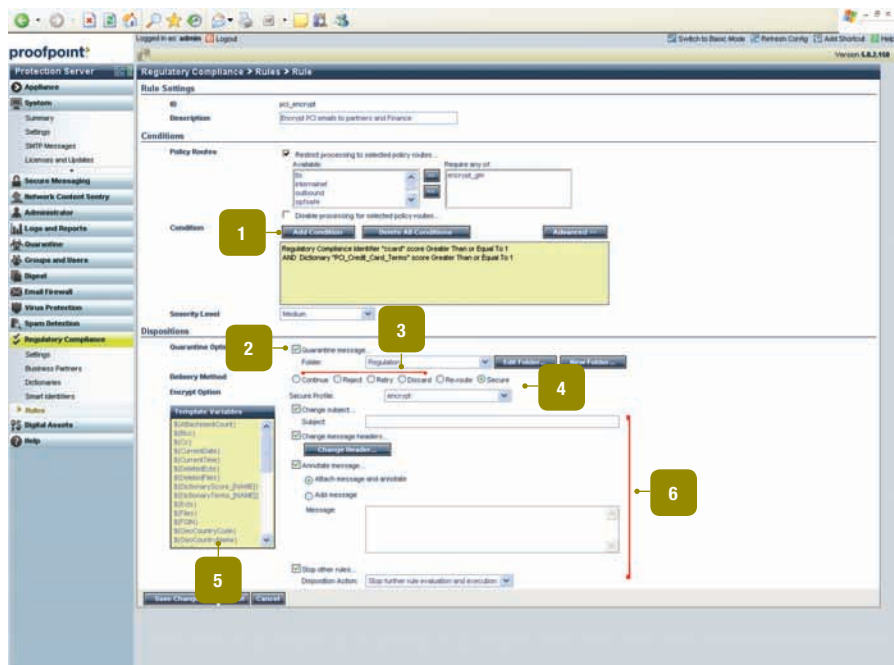
Monitor: Where to Look for PCI Violations

PCI DSS explicitly identifies email as a channel that requires monitoring for credit card data leaks. Proofpoint addresses this requirement, both in letter and spirit, by monitoring SMTP email and also inspecting content in HTTP (which includes webmail and blog posts) and FTP (common method for bulk file transfer). The solution also inspects a wide variety of email fields such as sender, recipient, attachments and country codes. The Network Content Sentry™ module provides built-in support for common webmail applications such as Yahoo!, Gmail and Hotmail. With the configuration of policy routes, end-to-end communication over these channels is further analyzed with knowledge of sender/recipient (for email), source/destination (IP addresses) and webmail sites.

Simplified PCI Policy Definition for PAN Detection and Enforcement

The Proofpoint Regulatory Compliance™ module provides an easy-to-use interface with pre-defined policies for PAN detection while offering advanced features that make it easy to create customized policies.

Proofpoint Regulatory Compliance Module



Proofpoint Solution Brief for PCI DSS Compliance

data loss prevention (continued)

Prevent - Detect PCI Data

The Proofpoint Regulatory Compliance™ module provides pre-built and customizable checks for structured data containing PCI content:

- **Smart identifiers:** Pre-defined checks, including valid credit card numbers
- **Managed Dictionaries:** Pre-defined, customizable using keywords, regex
- **Proximity detection:** Find credit card number near cardholder name in email

The Digital Asset Security™ module can detect PCI data in unstructured formats such as drawings, legal documents and source code:

- **Digital Fingerprinting:** Create hash of text and images containing PCI data
- **Content Matching:** Detect whole or subset of fingerprinted content
- **File Types:** Detect .xls, .doc, .ppt and others even if file extensions are changed

Automated, Policy-based Encryption

Proofpoint Secure Messaging™ provides automated, policy-enforced email encryption at the gateway or the desktop. Advantages over user-enforced encryption include:

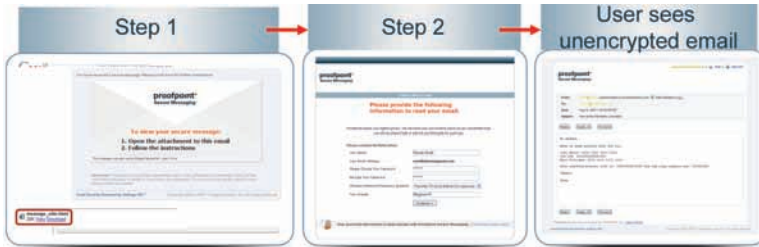
- Does not require users to assess when/how to encrypt their emails
- Supports encryption of corporate email from ANY device (such as Blackberry)
- Identity Based Encryption™ (IBE) for gateway to user
- TLS (included in platform) for gateway to gateway

Encryption Made Easy for PCI DSS

Secure Messaging makes encryption easy for recipients with a two-step process:

Step 1: User receives email with link to encrypted message.

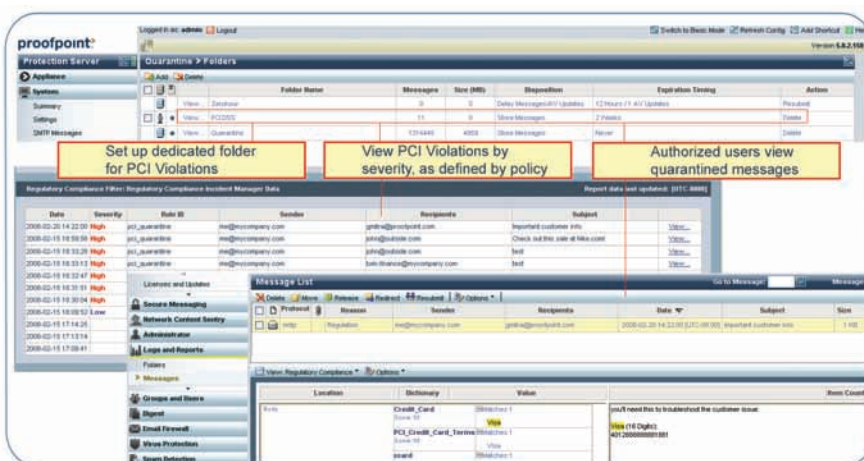
Step 2: User provides email address, password and question/answer.



Quarantine Sensitive Email for Further Review

A business may address PCI Req. 4.2 with email quarantine for review, before releasing for encryption. Proofpoint's built-in MTA blocks delivery.

Proofpoint Quarantine Options and Review Capabilities for PAN Data



Proofpoint Encryption Benefits

- Send messages to anyone
- No client required for sender or recipient
- No Javascript or ActiveX
- Supports encrypted attachments
- No keys or message store required
- Recipient clicks on link in email to authenticate and view decrypted email
- Powered by IBE technology from Voltage Security
- Interoperable with any standard gateway encryption solution

Flexible User Authentication

- Username/password
- Question/answer
- Email answerback
- LDAP, Active Directory
- PKI smart cards
- RSA SecurID

Effective DLP policies

“Proofpoint email quarantine provides unprecedented grouping, drill-down and review capabilities, necessary to develop the most effective email DLP policies.”

Barry Johnson
VP of Risk Mitigation
lgxglobal

Inform - Policy Violations:

- **IT admins:** Alerts via email, syslog, log viewer and published reports
- **Users:** Automated, customizable email response educates user on policy violation as it occurs

Built-in Reports

Proofpoint 'Logs and Reports' provide pre-defined reports for security events and trends including: Top Regulatory Senders, Violation Trends, and Incident Manager.

These reports can be leveraged to divert training resources to where they are most needed – to specific users or to develop additional training content. More advanced reporting and analysis is offered by the Proofpoint Smart Search™ module.

Proofpoint Solution Brief for PCI DSS Compliance

email security

PCI DSS also mandates the use of anti-virus and anti-malware programs, per Req. 5. Highest accuracy in anti-spam combined with anti-virus features from Proofpoint provides customers with safe and efficient email services. For more information on Proofpoint email security solutions, please visit <http://proofpoint.com/products>.

proofpoint platform can also be audited under PCI DSS

Email security solutions may be ‘in-scope’ for a PCI audit since the solution may store, transmit or process PAN data. The following table highlights other PCI requirements that need to be considered as part of an audit of Proofpoint’s solution.

Summary: Email Security Solution

- Anti-spam: automated updates, based on machine learning, PARC research
- Signature-based anti-virus: Technology from industry-leading vendors
- Behavioral: Zero-Hour anti-virus
- 99%+ anti-spam effectiveness

PCI Requirement	Proofpoint Solution Modules						
	Secure Messaging	Regulatory Compliance	Digital Asset Security	Network Content Sentry	Anti-Virus	Anti-Spam	Proofpoint Solution
! Req 4.2: Never send unencrypted PANs by e-mail (SMTP, HTTP, FTP; structured, unstructured data; encryption)	➤	➤	➤	➤			
Scope of Assessment: - PCI Security Audit Procedures: “Adequate network segmentation, which isolates systems that store, process, or transmit cardholder data..., may reduce the scope of the cardholder data environment.”							➤
Req A.1: Hosting providers protect cardholder data environment (restrict company access, logging, auditing).							➤
Req 1: Install and maintain a firewall configuration ...							➤
Req 2.1: ...change vendor-supplied defaults before installing a system...							➤
Req 2.2.2: Disable all unnecessary, insecure services, protocols...							➤
Req 2.2.3: Configure system security parameters to prevent misuse							
Req 2.2.4: Remove all unnecessary functionality....							
Req 2.3: Encrypt all non-console administrative access							➤
Req 4.1: Use strong cryptography and security protocols such as ...transport layer security (TLS)...							➤
Req 5: Use and regularly update anti-virus software or programs [...including malicious software...]					➤	➤	
Req 6.1: Ensure that all system components and software have the latest vendor-supplied security patches installed							➤
Req 6.2: ...process to identify newly discovered security vulnerabilities							➤
Req 7: Restrict access to cardholder data by business need-to-know							➤
Req 8.4: Encrypt all passwords during transmission and storage...							➤
Req 8.5: Ensure proper user authentication and password management							➤
Req 10: Track...monitor...access to network resources and cardholder data							➤

Our customers say it best

Don’t just take our word for it. See what our customers have to say about how Proofpoint solved their toughest email security and data loss prevention challenges. Visit our Resource Center and browse through our case studies:

<http://www.proofpoint.com/resource-center/>

See for yourself

Take the next step to learning more by viewing our free online demo which presents the key features and benefits of Proofpoint’s unified email security and data loss prevention solutions:

<http://www.proofpoint.com/demo>

©2008 Proofpoint, Inc. Proofpoint Protection Server, Proofpoint Messaging Security Gateway, Proofpoint Spam Detection, Proofpoint Virus Protection, Proofpoint Digital Asset Security, Proofpoint Regulatory Compliance, Proofpoint MLX, Proofpoint Dynamic Reputation, and Proofpoint on Demand are trademarks or registered trademarks of Proofpoint, Inc. in the United States and other countries. All other trademarks contained herein are the property of their respective owners. 04/08