



Are you **really** PCI compliant?

FORTINET.





THE PAYMENT CARD INDUSTRY MANDATES PROTECTION OF CUSTOMER DATA

Over the past few years there has been an unprecedented attack on personal financial data that customers have entrusted to retailers, banks and credit card companies. Credit card data in particular has been compromised so frequently that calls for government intervention and regulation became widespread.

However, it was MasterCard and Visa who originally took up the challenge, which has now emerged as the Payment Card Industry Data Security Standard, or PCI as it is almost universally known.

PCI is a comprehensive security standard that establishes common processes and precautions for handling, processing, storing and transmitting credit card data.

So, how compliant are *you*?

PCI PRINCIPLES AND REQUIREMENTS

Build and maintain a secure network

- Install and maintain a firewall configuration to protect cardholder data**
- Do not use vendor-supplied defaults for system passwords and other security parameters**

Protect cardholder data

- Protect stored cardholder data**
- Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

- Use and regularly update anti-virus software**
- Develop and maintain secure systems and applications**

Implement strong access control measures

- Restrict access to cardholder data by business need-to-know**
- Assign a unique ID to each person with computer access**
- Restrict physical access to cardholder data

Regularly monitor and test networks

- Track and monitor all access to network resources and cardholder data**
- Regularly test security systems and processes**

Maintain an information security policy

- Maintain a policy that addresses information security
- Appendix B*
- Compensating controls**

PCI requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data.

Fortinet's focus is highlighted in bold on the table above.





CONSTANTLY CHECKING YOUR HEALTH

Do not use vendor-supplied defaults for system passwords and other security parameters

- We detect default passwords
- We verify system security settings
- We detect unwanted services
- We recommend optional configurations

Protect stored cardholder data

- We deliver processor-efficient data monitoring
- We provide insider threat protection
- We validate compensating controls
- We examine transactions and data selection

Use and regularly update anti-virus software or programs

- We carry out vulnerability assessment
- We discover vulnerabilities
- We detect and recommend patch levels

Develop and maintain secure systems and applications

- We discover vulnerabilities
- We detect and recommend patch levels
- We detect unwanted accounts
- We carry out penetration testing
- We document impact



WATCHING FOR THE ODD ONE OUT

Restrict access to data by business need-to-know

- We verify that business and security rules regarding data access are being followed
- We provide an activity trail on data access
- We identify the user, application and location associated with access
- We deliver near real-time analysis and threat detection

Unique user IDs

- We verify user identity
- We verify password settings
- We map network identity to database
- We enforce access rules with rule chaining

Monitor all access to cardholder data

- We record all access and transactions
- We store the audit trail independently
- We see all activity in the cardholder database

Regularly test security systems and processes

- We validate controls through audit analysis
- We perform penetration tests
- We test vulnerabilities periodically
- We monitor data and structural integrity, as well as privilege change
- We detect anomalous behavior

Appendix B

- We provide compensating controls



KEEPING DATA SAFE

Pro-active

Advanced event-based scripting enables complex, active decisions to be made on critical issues in real-time by Security Officers, DBAs and Compliance Officers.

CLI, SNMP and SMTP allow integration with existing patch management solutions, trouble ticketing systems, systems and network management platforms, etc.

Continuous

Once enabled, policies remain active until disabled. In addition, policies may be enabled or disabled for specified periods, for example, end of quarter. Unlike network monitors, audit data can be recovered and policies executed after accidental down-time.

Independent from DBAs

The Fortinet solution can create and apply policies independent of DBAs. Furthermore, auditors can review policies and reports independent form DBAs and Fortinet administrators.

Auto-discovery

Fortinet can automatically discover all of the databases within your organization and provide a complete inventory. Once you have automatically identified all of your databases Fortinet can then check to see if they hold any credit card data that requires protection.

Configuration Management

Configuration management is a key element of enterprise security. Fortinet has a large number of policies to assess configuration settings and to provide remediation advise. By utilizing periodic scans it is also possible to keep track of configuration changes. Integration with other configuration management tools can be achieved by utilizing Fortinet's export capabilities.

A graphic of a green clipboard with a white checklist titled "FORTINET CHECKLIST". The checklist has four items, each with a red checkmark in a blue box: "Pre-packaged policies", "Consistent, safe and easy", "IT and Business Unit reports", and "Unburden DBAs".

FORTINET CHECKLIST

- ✓ Pre-packaged policies
- ✓ Consistent, safe and easy
- ✓ IT and Business Unit reports
- ✓ Unburden DBAs

RELIABLE, PAINLESS CONTROLS

Pre-packaged policies

Out-of-the-box policies and reports accelerate productivity, allowing you to be up-and-running quickly with customized procedures. Out-of-the-box policies can be easily edited to adjust risk level, criticality, action and remediation advice. New policies can be created to capture best practices or compliance requirements.

Consistent, safe and easy

Automation mitigates the risk of human error. Unlike humans, Fortinet does not get tired, bored or interrupted by fellow workers. No application changes are required meaning no new points of failure.

IT and Business Unit reports

Reports designed by auditors improve confidence and trust. They are also structured to business needs, which serve to bridge the gap between IT and users.

Unburden DBAs

Policy review and reports can be done by auditors without the need for DBA involvement. Fortinet manages the audit trail, freeing DBAs to focus on other issues. Manpower costs can be reduced by eliminating complex administrative scripts and manual reporting.

Compensating Controls

Many organizations find that compensating controls are more effective in implementing security over credit card data, and address limitations in database encryption.



KEY COMPONENTS TO PCI COMPLIANCE

Easy, safe deployment

- Non-invasive and does not affect database performance
- Non-invasive and does not affect application performance
- Non-invasive and does not provide an additional point of failure for applications
- Non-invasive and does not introduce a new security risk

Central policy management

- Single policy repository allows for consistent policy application
- Web-based interface provides 'manage anywhere' capability
- Maintains history of policy violations

Full database coverage

- Support of current production and legacy database versions
- Consistently apply policies to different database types
- Maintains audit data for forensic analysis

Encapsulates best practices

- Years of industry best security practices pre-bundled
- Expert level policies pre-defined
- Custom policy capability
- Lowers risk of human error

Automated alerting and reporting

- Scans and reports can be scheduled to ensure timeliness
- All alerts can be individually provided to email, paging and control centers
- All reports can be placed into different formats, such as PDF, HTML and text files

Auto-discovery

- Finds all databases in your organization
- Finds all credit card information within the database(s)



**YOUR TIME COULD BE
RUNNING OUT.
CONTACT FORTINET AND
KEEP YOUR DATA SAFE.**

ABOUT FORTINET

Fortinet, Inc.'s award-winning software is **Keeping Data Safe** for companies around the world. From hardening databases against attacks to real-time activity monitoring, Fortinet is the solution to enterprise compliance and database security needs.

For more information please call

AMER +1-408-235-7700

EMEA +33-4-8987-0510

APAC +65-6549-7050

click www.fortinet.com

or visit 1090 Kifer Road, Sunnyvale, CA 94086, USA

Fortinet and the Fortinet logo are trademarks of Fortinet, Inc.
All rights reserved. Any unauthorized use or reproduction of the
Fortinet logo is prohibited.
© 2008 Fortinet, Inc.

FORTINET.

Design by www.rightangle.co.uk

