



SecureWorks

Information Security Services

Achieving PCI compliance with
Dell SecureWorks' security services



Executive summary

In October 2010, the Payment Card Industry (PCI) issued the new Data Security Standard (DSS) version 2.0. The PCI DSS v2.0 outlines security requirements to protect payment account data. All companies who process, transmit or store cardholder data must implement these controls to avoid fines and/or penalties levied by the card brands (Visa, MasterCard, American Express, Discover and JCB International).

In addition to meeting the security requirements of the PCI DSS v2.0, merchants and service providers must also validate their compliance. All merchants and service providers with externally-facing IP addresses must undergo Quarterly Network Scanning performed by an Approved Scanning Vendor (ASV). Level 1 merchants (which process more than 6 million transactions per year) and Level 1 service providers (more than 300,000 transactions per year) must also undergo an Annual On-Site Data Security Assessment performed by a Qualified Security Assessor, or Internal Audit if signed by an officer of the company. Merchants and service providers, levels 2-4, must complete the appropriate PCI Self-Assessment Questionnaire (SAQ). Once completed, validation results must be submitted to your acquiring bank.

Dell SecureWorks is a PCI Qualified Security Assessor (QSA), Approved Scanning Vendor (ASV) and one of the leading providers of Security Services, with thousands of customers around the world. We offer a full breadth of services that will help your organization comply with the PCI DSS. Our services provide the effective controls necessary to protect cardholder information and demonstrate provable compliance with the PCI DSS v2.0.

PCI DSS compliance is addressed by security services

Build and maintain a secure network	
Requirement	How Dell SecureWorks helps
1. Install and maintain a firewall configuration to protect cardholder data.	<p>Security and Risk Consulting Managed Firewall Security Log Monitoring SIM On-Demand</p> <p>This requirement mandates the need to implement a sound firewall infrastructure to protect cardholder data from external access. Dell SecureWorks' Security and Risk Consulting team can perform an assessment to identify the state of your current firewall and network architecture, identify any gaps, recommend solutions to these gaps and implement the changes necessary.</p> <p>Dell SecureWorks' Managed Firewall service removes the burden of firewall management by providing you with a 24x7x365 team of experts. Our firewall experts will audit policies to ensure they align with PCI requirements, perform ongoing rule-set changes and monitor these devices for any signs of attack.</p> <p>Our Security Log Monitoring service provides real-time monitoring for known and unknown threats across your firewall infrastructure by our security experts, while our Security Information Management (SIM) service enables your team to perform this monitoring internally. All three of these services will deliver robust reporting through the secure, Web-based Customer Portal, enabling your team to easily demonstrate your compliance with this PCI DSS requirement.</p>



Build and maintain a secure network

Requirement	How Dell SecureWorks helps
2. Do not use vendor-supplied defaults for system passwords and other security parameters.	<p>Vulnerability Management</p> <p>This requirement dictates that organizations must use sound password policies, such as not using vendor-supplied passwords, and wireless and infrastructure configuration standards. Dell SecureWorks' Security & Risk Consulting Services can help you meet this requirement by conducting a Vulnerability Assessment of your environment to identify any weaknesses in your configuration practices including weak passwords, unnecessary services and rogue web servers. Our team of consultants can work with your organization to develop a secure configuration standard for all critical systems that is based on industry best practices.</p> <p>Additionally, you can utilize our Vulnerability Scanning service to perform ongoing internal and external vulnerability scans to ensure your infrastructure remains secure. Using the Dell SecureWorks Portal, you will be able to generate on-demand vulnerability reports that highlight any exposures and the actions your team has taken to eliminate them.</p> <p>This requirement also calls for your hosting providers to be secure as described in Appendix A of the PCI DSS. The services described in this document can apply to the hosting providers as well, to help them become PCI compliant. Also, with their permission, we can provide security visibility into their environment through the Dell SecureWorks Portal.</p>

Protect cardholder data

Requirement	How Dell SecureWorks helps
3. Protect stored cardholder data.	<p>Security and Risk Consulting Managed Intrusion Prevention and Detection</p> <p>This requirement mandates rendering stored cardholder data unreadable, if possible, or implementing other compensating controls, such as preventing Web application attacks, as outlined in Appendix B of the PCI DSS. Dell SecureWorks' Security and Risk Consulting experts can help you classify your assets and the data residing in them, and help formulate a data protection strategy appropriate to your infrastructure.</p> <p>Our Managed Intrusion Prevention and Detection service provides the prevention/detection controls identified in Appendix B to protect any data that cannot be encrypted. This service provides implementation of a commercial IPS/IDS technology or can be bundled with our award-winning iSensor IPS technology to deliver superior protection in a cost-effective manner. Once implemented, our Security Analysts will manage these devices, including ongoing tuning, and monitor them to identify and respond to any threats. The Dell SecureWorks Portal provides you with real-time visibility into your intrusion prevention and detection infrastructure, including any alerts and the actions we have taken against them, while also delivering on-demand reports to demonstrate PCI compliance.</p>



Protect cardholder data

Requirement	How Dell SecureWorks helps
4. Encrypt transmission of cardholder data across open, public networks.	<p>Security and Risk Consulting Managed Firewall Email Encryption</p> <p>This requirement calls for all cardholder data to be encrypted during transmission over public or untrusted networks. Dell SecureWorks' Security and Risk Consulting team can help you meet this requirement by assessing your current infrastructure to ensure all VPNs and wireless networks are configured properly to encrypt sensitive data, as well as identify any gaps in your data transmission flows that may leave sensitive information unencrypted.</p> <p>Dell SecureWorks' Managed Firewall service removes the burden of site-to-site VPN management by providing you with a team of security professionals to administer these devices. Our analysts will also monitor your VPNs for any signs of malicious activity, to respond before damage is done. All information is collected and presented to your team via the Dell SecureWorks Portal, providing your team with real-time visibility and on-demand reporting to demonstrate PCI compliance.</p> <p>Dell SecureWorks' Email Encryption service will ensure all cardholder data is transmitted via encrypted email. This solution uses lexicons to identify any cardholder data being sent in unencrypted emails and will automatically encrypt the message. The solution is easy-to-use and requires very little end-user training, making compliance with this requirement painless.</p>

Maintain a vulnerability management program

Requirement	How Dell SecureWorks helps
5. Use and regularly update anti-virus software or programs.	<p>Managed Intrusion Prevention and Detection Security Log Monitoring SIM On-Demand</p> <p>This requirement mandates the use of anti-malware solutions to prevent all known types of malicious software from impacting your critical systems. Dell SecureWorks' Network Intrusion Prevention and Detection service with our iSensor IPS appliance can provide an additional layer of defense against these types of attacks. iSensor contains advanced analysis and blocking techniques to protect against threats. Our security experts will provide full life-cycle management for iSensor appliances, from implementation to proactive administration and tuning, including monitoring, configuration, access management, backups, updates, patches, hardware expansion and replacement, and daily audits of existing signatures. If your organization has already invested in Network IPS/IDS equipment, Dell SecureWorks can deliver monitoring services in a co-managed fashion.</p> <p>Dell SecureWorks' Security Log Monitoring service provides a team of experts to monitor your infrastructure to identify attacks before damage is done. Should you prefer to monitor this activity in-house, Dell SecureWorks' SIM On-Demand service provides the same event aggregation and correlation technology used by our experts as a service, so that your team can analyze any threats that may occur. With both services, you will be provided with real-time security visibility and on-demand reports to demonstrate PCI compliance, through the Dell SecureWorks Portal.</p>



Maintain a vulnerability management program

Requirement	How Dell SecureWorks helps
6. Develop and maintain secure systems and applications.	<p>Security and Risk Consulting Vulnerability Scanning Counter Threat Unit Intelligence</p> <p>This requirement mandates the need to ensure that your environment maintains current patch levels, you adhere to secure coding practices and that all Web applications undergo periodic Web application assessments. Dell SecureWorks' Security and Risk Consulting team can help you meet this requirement by conducting periodic vulnerability assessments to ensure the security of your environment, perform Web application testing to identify any areas of concern across your Web-facing infrastructure, including vulnerabilities that may lead to Cross-site scripting attacks, buffer overflows, etc., and work with your team to align your application development with secure coding best practices.</p> <p>Dell SecureWorks' Vulnerability Scanning service provides you with the ability to conduct periodic scans of your infrastructure to identify any potential vulnerabilities or out-of-date systems. Through the Dell SecureWorks Portal, customers can schedule recurring PCI Compliance Scans and Web Application Scans, or they can conduct them at any time on demand.</p> <p>Dell SecureWorks' Counter Threat Unit Intelligence Services provides you with new vulnerability and threat alerts tailored to your environment, which keeps your team on top of any new patches relevant to your systems. With both the Scanning and Intelligence services you will gain access to the Dell SecureWorks Portal to generate on-demand reports to demonstrate PCI compliance.</p>

Implement strong access control measures

Requirement	How Dell SecureWorks helps
7. Restrict access to cardholder data by business need to know.	<p>Security and Risk Consulting Security Log Monitoring SIM On-Demand</p> <p>This requirement mandates the need for organizations to implement proper identity and access management across systems that house cardholder information. Dell SecureWorks' Security and Risk Consulting Services can help you meet this requirement by working with your team to classify your systems and identify those that house cardholder information. Our consultants can then help your organization design an appropriate identity and access management strategy. The Security and Risk Consulting team can also assess your infrastructure to ensure the proper access controls have been implemented in accordance with this PCI requirement.</p> <p>Dell SecureWorks' Security Log Monitoring service provides real-time monitoring of these systems by true security experts to ensure only authorized personnel gain access. Dell SecureWorks' SIM On-Demand delivers the technology you need to perform monitoring of these systems as a service, should you choose to keep this function in-house. Both services provide you with access to the Dell SecureWorks Portal where you will receive real-time visibility into the activity occurring on the systems housing cardholder information and on-demand reporting to demonstrate PCI compliance.</p>



Implement strong access control measures

Requirement	How Dell SecureWorks helps
8. Assign a unique ID to each person with computer access.	<p>Security and Risk Consulting Security Log Monitoring SIM On-Demand</p> <p>This requirement mandates the need to ensure that actions taken by known and authorized individuals with computer access can be monitored and traced. Dell SecureWorks' Security and Risk Consulting can help you meet this requirement by working with your team to develop and implement proper policies and procedures for assigning unique IDs and authentication measures. The Security and Risk Consulting team can also assess your identification and authentication measures to ensure their effectiveness in protecting cardholder data and complying with PCI requirements for password management and authentication.</p> <p>Dell SecureWorks' Security Log Monitoring service provides real-time monitoring of access to systems in your environment. Dell SecureWorks' SIM On-Demand delivers the technology you need to monitor access to these systems as a service, should you choose to keep this function in-house. Both services provide you with access to the Dell SecureWorks Portal, where you will receive real-time visibility into the actions being taken by known and authorized individuals in your cardholder data environment, as well as on-demand reporting to demonstrate PCI compliance.</p>
9. Restrict physical access to cardholder data	<p>Security and Risk Consulting</p> <p>This requirement dictates that organizations implement appropriate physical security controls to limit access to critical systems, ensure proper visitor handling procedures and that organizations have proper procedures when moving or destroying physical media where cardholder information is stored. Dell SecureWorks' Security and Risk Consulting can help you address this requirement by working with your team to identify areas where physical security controls must be implemented and testing controls to ensure compliance through social engineering and other tactics. The Security and Risk Consulting team can also help you develop physical data handling and destruction procedures that align with industry best practices, such as those from the Department of Defense.</p>

Regularly monitor and test networks

Requirement	How Dell SecureWorks helps
10. Track and monitor all access to network resources and cardholder data.	<p>Security Log Monitoring SIM On-Demand</p> <p>This requirement calls for companies to implement logging mechanisms across all network, security and server infrastructure that houses or handles cardholder information, and monitor the logs for any violations. Dell SecureWorks' Security Log Monitoring service provides real-time log aggregation, correlation and analysis across any security device or critical information asset. All logs and alerts are monitored in real-time, 24x7x365 by true security experts to identify known and unknown threats, or unusual user behavior. Any malicious activity identified is immediately responded to before damage is done. Our SIM On-Demand provides your team with the same aggregation and correlation technology used by our analysts, as a service, to enable your team to monitor your environment in-house. With both services, log information is stored indefinitely with the previous two years accessible via the Dell SecureWorks Portal. Also with both services, you will gain access to the Portal to gain real-time security visibility and generate on-demand reports to demonstrate PCI compliance.</p>



Protect cardholder data

Requirement	How Dell SecureWorks helps
11. Regularly test security systems and processes.	<p>Security and Risk Consulting Vulnerability Scanning Managed Intrusion Prevention and Detection Managed Host Intrusion Prevention Security Log Monitoring SIM On-Demand</p> <p>This requirement mandates that organizations periodically test their systems and protect them through vulnerability scans, penetration testing, intrusion prevention and detection, and file integrity software. Dell SecureWorks' Security and Risk Consulting can help you comply with this requirement by providing vulnerability assessments and penetration testing. Dell SecureWorks is an approved scanning vendor and our Vulnerability Scanning service can be utilized to comply with the quarterly external scan that is required for PCI compliance.</p> <p>Our Managed Intrusion Prevention and Detection service provides the prevention/detection controls identified in this requirement. This service provides implementation of a commercial IPS/IDS technology or can be bundled with our award winning iSensor IPS technology to deliver superior protection in a cost-effective manner. Once implemented, our experts will manage these devices, including ongoing tuning, and monitor them to identify and respond to any threats. Likewise, Dell SecureWorks' Managed Host Intrusion Prevention service provides you with the technology and a team of experts to manage and monitor this infrastructure in order to keep it operating at peak performance.</p> <p>Dell SecureWorks' Security Log Monitoring service provides real-time monitoring across your systems by true security experts to respond to any security events occurring. Dell SecureWorks' SIM On-Demand service delivers the technology you need to perform monitoring of these systems as a service, should you choose to keep this function in-house.</p> <p>The Scanning, Managed Intrusion Prevention and Detection, Log Monitoring and SIM On-Demand services provide you with access to the Dell SecureWorks Portal, where you will receive real-time visibility into the activity occurring on the systems housing cardholder information and on-demand reporting to demonstrate PCI compliance.</p>

Maintain an information security policy

Requirement	How Dell SecureWorks helps
12. Maintain a policy that addresses information security for employees and contractors.	<p>Security and Risk Consulting Security Log Monitoring</p> <p>This requirement dictates that organizations must create an information security policy that is kept up to date and addresses all the security requirements in the PCI DSS, as well as operational security, system usage, security management, security awareness and incident response. Dell SecureWorks' Security and Risk Consulting team can help you address this requirement by working with your team to create a robust, effective information security policy that addresses all the requirements of this section and the PCI DSS as a whole.</p> <p>Additionally, our Security Log Monitoring Service can provide you with the incident response plan and experts necessary to conduct effective response to stop threats before damage is done. With this service, you will be able to utilize the Dell SecureWorks Portal to gain real-time security visibility and on-demand reporting to demonstrate PCI compliance.</p>



SecureWorks

About Dell SecureWorks

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology and business solutions they trust and value. Recognized as an industry leader by top analysts, Dell SecureWorks provides world-class information security services to help organizations of all sizes protect their IT assets, comply with regulations and reduce security costs.

For more information, visit <http://www.secureworks.com>

THIS WHITE PAPER IS FOR INFORMATIONAL PURPOSES ONLY AND MAY CONTAIN TYPOGRAPHICAL ERRORS AND TECHNICAL INACCURACIES. THE CONTENT IS PROVIDED AS IS, WITHOUT EXPRESS OR IMPLIED WARRANTIES OF ANY KIND.

Availability varies by country. © 2011 Dell Inc. All rights reserved.

Dell and the Dell logo, SecureWorks, Counter Threat Unit (CTU), iSensor, iScanner, Sherlock, Inspector and LogVault are either registered trademarks or service marks, or other trademarks or service marks of Dell Inc. in the United States and in other countries. All other products and services mentioned are trademarks of their respective companies. This document is for illustration or marketing purposes only and is not intended to modify or supplement any Dell specifications or warranties relating to these products or services. February 2011.