



Cisco PCI Solution for Retail Addressing PCI Data Security

Helping Retailers Address Compliance while Strengthening Store Security

Executive Summary

Data security requirements are now a permanent feature of retailers' compliance obligations. The Payment Card Industry Data Security Standard was designed to protect the privacy of customers, as well as payment card and merchant data. However, meeting PCI requirements has proved to be a challenge for many retailers. To help address this, Cisco offers the Cisco PCI Solution for Retail—a set of audited architectures that support secure transport for point of sale traffic, such as credit card data, cardholder information, transaction logs, and database records. The Cisco PCI Solution for Retail helps retailers meet their PCI compliance requirements while minimizing infrastructure complexity and simplifying integration with retail applications.

Introduction

The Payment Card Industry (PCI) Data Security Standard (DSS) was designed to ensure the security of cardholder data and information—at the point of sale (POS), in transit, and at rest. The standard affects any company that stores, processes, or transmits credit card information. This means that the PCI standard affects all retailers.

The Risks of Noncompliance

Merchants who fail to comply with PCI security standards face serious consequences. They may be fined, and repeated noncompliance may result in the retailer losing its card processing privileges, which can cripple a business. Consequences are severe because of the high risk associated with compromised data. Security breaches have resulted in lawsuits, which can damage the company's brand and lead to financial losses. On the other hand, companies that can demonstrate compliance with the PCI standard and prove that they are good custodians of customer data have the opportunity to build solid customer loyalty.

The Challenge of Meeting Requirements

The standards for achieving PCI compliance are somewhat broad, but all retailers are required to audit their current networks, policies, and processes (Figure 1). Retailers can interpret PCI requirements in different ways, however, creating systems that are more complex and difficult to support.

Figure 1. PCI DSS Primary Requirements



PCI Data Security Standard	
Build and Maintain a Secure Network	<ol style="list-style-type: none">1. Install and maintain a firewall configuration to protect data2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	<ol style="list-style-type: none">3. Protect stored data4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	<ol style="list-style-type: none">5. Use and regularly update antivirus software6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	<ol style="list-style-type: none">7. Restrict access to data by business need to know8. Assign a unique ID to each person with computer access9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	<ol style="list-style-type: none">10. Track and monitor all access to network resources and cardholder data11. Regularly test security systems and processes
Maintain an Information Security Policy	<ol style="list-style-type: none">12. Maintain a policy that addresses information security

Most industry experts agree that the best way to achieve and maintain PCI compliance is to adopt a strategic, holistic approach to network security risk management and compliance that includes the network infrastructure, policies, and procedures. The ability to centrally manage systems, network services, and security is essential to a holistic solution. In addition to simplifying retailers' approach to PCI requirements, central management improves operational efficiency and potentially will accelerate delivery of future retail applications that will travel the network infrastructure. Cisco offers a network foundation that is an important step for retailers to achieve regulatory compliance requirements and implement data security best practices.

Cisco PCI Solution for Retail

Cisco has extensive experience working with wired and wireless networking technologies. Using its accumulated best practices, Cisco has developed a set of architectures in a lab environment with PCI requirements in mind. Cisco invited PCI auditors to evaluate these architectures, and the auditors found that the technology, if properly deployed and maintained, could help retailers achieve PCI compliance. Known as the Cisco PCI Solution for Retail, these network architectures support secure transport for POS traffic, such as credit card data, cardholder information, transaction logs, and database records.

Retailers can use these network architectures as a guideline for deploying their own network installations as they work toward PCI compliance. These architectures can be used throughout the range of retail environments—from small stores to large retail footprints.

The Elements of a Cisco PCI Solution for Retail

Cisco network configurations can be tailored for each retailer's specific store footprint and application needs. In addition, Cisco's labtested architectures may help minimize infrastructure complexity and simplify integration. These architectures incorporate Cisco products, such as:

- **Secure routers**—Cisco IOS Software-based routers integrate advanced communications and security capabilities that support wireless, voice, firewall, intrusion prevention, and traffic profiling applications, and virtual private networks (VPNs). Cisco routers help to satisfy PCI requirements 1, 2, 4, 6, 10, 11, and 12.
- **Adaptive security appliances**—The Cisco ASA 5500 Series Adaptive Security Appliances offer firewall, antiX, intrusion prevention, and VPN capabilities that thwart malicious attempts to steal identity and credit card information. Integrated IP Security (IPSec) and Secure Sockets Layer (SSL) VPN capabilities offer optimal encryption across public networks, when properly deployed and maintained. Cisco adaptive security appliances can help a retailer meet PCI requirements 1, 2, 4, 6, 11, and 12.
- **Cisco Security Agent**—Cisco Security Agent protects against worm and dayzero attacks, and offers sophisticated protection against theft of information for both servers and clients. See PCI requirements 1, 2, 3, 5, 6, 7, 10, 11, and 12.
- **Compliance reporting and management**—Cisco centralized management, monitoring, and remediation capabilities are provided by Cisco Secure Access Control Server, Cisco Security Manager, and Cisco Wireless ControlServer—as well as by other management products that support usage and event reporting, provisioning, policy and change management, and workflow tracking on wired and wireless networks. This information can be placed into compliance reports for auditing purposes. Cisco management products thus help reduce operational expenses and help a retailer address PCI requirements 10, 11, and 12.
- **Network Admission Control (NAC)**—NAC determines which client devices are granted network access and which devices are denied. Controlling network access reduces the threat of unauthorized access to credit card information. See PCI requirements 5, 6, 11, and 12.
- **Cisco Advanced Services**—Cisco is an approved PCI scanning vendor. Cisco PCI Compliance Assessment services can perform PCI vulnerability scans to help companies determine their PCI compliance readiness and areas in which improvement may be necessary.

Cisco also works with a wide range of vendors who provide solutions for antivirus, POS software, wireless POS, scan, audit, and remediation services, and payment applications.

Protect Mobile Applications and Data

Retailers can implement Cisco Unified Wireless capabilities on their Intelligent Retail Network to help address the requirements of the PCI Data Security Standard. Cisco Unified Wireless solutions protect the wired network from wireless threats and help ensure secure, private communications over authorized wireless LANs. Integrated support for industry standards, as well as integrated radio frequency (RF) scanning and monitoring capabilities, protect the wireless medium from unauthorized use or attack—a specific requirement of the PCI standard.

The inherent security capabilities of a Cisco Intelligent Retail Network with Unified Wireless capabilities support:

- Confidential communications
- Segmentation of users for access to appropriate resources
- Security strategies for client devices

To secure sensitive cardholder information—whether in a retail wired or wireless network environment—Cisco supports industry standards, such as WPA and WPA2. Cisco Unified Wireless solutions can also identify and prevent rogue access points and ad hoc networks from gaining access. Innovative air monitoring capabilities enable retailers to protect retail sites that do not have wireless LAN coverage from unauthorized wireless access.

Build a Foundation for Compliance

A Cisco Intelligent Retail Network builds in advanced security capabilities that help a retailer address many of the 12 PCI requirements and optimize security for sensitive information. It provides integrated, collaborative, and adaptive solutions that can help a retailer meet specific requirements of the PCI standard. For example, a Cisco Intelligent Retail Network protects against worm and dayzero attacks, and offers sophisticated protection against information theft for both servers and clients.

PCI compliance is just the beginning, however. Country, state/province, and local regulations may also require a company to safeguard data. A Cisco Intelligent Retail Network can support a company's efforts to meet current and future regulatory requirements, while also enabling a retailer to securely undertake new business initiatives and improve companywide risk management.

Enhance Company Security and Risk Management

While adaptive security technologies help address PCI compliance, the Cisco Intelligent Retail Network can also strengthen a company's overall security posture by:

- Supporting and helping enforce security best practices
- Helping protect brand image and assets
- Mitigating financial risk of noncompliance fines and penalties

Enable Secure New Business Initiatives

An investment in a network with advanced capabilities creates a foundation that allows retailers to take advantage of new opportunities. There is no need to redesign the network to add capabilities such as wireless or voice services. The same security capabilities that facilitate PCI compliance also permit new initiatives. This improves retailers' return on investment for new initiatives such as interactive kiosks, unified communications, and wireless applications. In addition, it facilitates highly secure access for partners and helps control sensitive data from leaking outside of enterprise boundaries.

Strengthen Shopping Security

With Cisco retail solutions, retailers can more easily meet PCI requirements while simultaneously providing a highly secure shopping environment—whether in a physical store or online. Investing in compliance best practices is an investment in a retailer's business—store, employee, and customer data can be confidently used for programs that enhance merchandising, improve the shopping experience, and build brand loyalty.

Cisco PCI Solution

Cisco Intelligent Retail Network

A Cisco Intelligent Retail Network can be tailored to meet a wide range of retail needs, such as complying with regulations, conducting video surveillance, or deploying wireless solutions. At the same time, the network plays a vital role in the company's longterm strategy for protecting customer, employee, and operational data. Designed on the Cisco Service-Oriented Network Architecture framework, the Intelligent Retail Network provides a common platform that is helpful for meeting regulatory requirements, delivering retail business applications, and supporting advanced network services such as wireless, security, and unified communications.

Learn More Today

Cisco retail solutions facilitate retailers' achieving their compliance goals and simultaneously enable new strategic business initiatives. Call your local Cisco account executive to learn how Cisco retail solutions tailored for meeting PCI requirements can help you reach your compliance goals. For more information, visit www.cisco.com/go/retailsolutions.



Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

©2007 Cisco Systems, Inc. All rights reserved. CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0701R)