



PCI Solution for Retail: Addressing Compliance and Security Best Practices

Executive Summary

The Payment Card Industry (PCI) Data Security Standard has been revised to address an evolving risk environment and clarify compliance requirements. As the threat of security breaches grows, it is clear that simply achieving device and system compliance is not enough to protect retail businesses and their customers. Cisco® PCI Solution for Retail helps you:

- Address today's revised PCI compliance requirements
- Protect customer data in your data center, stores, across e-commerce sites, and to partners such as payment processors
- Build a foundation for ongoing compliance
- Create processes that reduce risk and cost

Introduction

As consumers use payment cards in growing numbers for their purchases, so does the risk associated with lost or stolen cards. According to industry and government experts, more credit cards are stolen in the United States than any other form of financial information. High volumes of personal and financial data transmitted through multiple devices and channels make it more challenging than ever to protect your customers, brand, and profitability. Vulnerability can occur at any interaction point where cardholder data and personal information is collected and transmitted. Data can be breached on point-of-sale devices in a store, on wireless or mobile devices, at call centers, on personal computers, and throughout the card processing system of service providers and financial institutions.

Version 1.2, of the PCI Data Security Standard, effective October 1, 2008, moves the PCI standard toward a risk-based approach to compliance. You now have more clearly stated requirements and a greater choice of acceptable ways to meet them. The three most significant changes in PCI version 1.2 include:

- **Network segmentation:** You can segment your network to limit risk exposure for customer and business data, which limits the scope of a PCI audit. A segmented network reduces the cost of achieving and monitoring compliance.
- **Wireless deadlines:** Wireless networks are widely used in stores and other retail operations, but not all are secured. No new Wired Equivalent Privacy (WEP) networks can be installed after March 31, 2009, and all existing WEP installations must be decommissioned by June 30, 2010.
- **More stringent requirements on auditors:** PCI auditors are required to test the effectiveness of your network segmentation, justify the sample size with documentation, and meet other new requirements.

The primary goal of PCI standards is to secure data. Therefore, your security strategy should employ best practices and an architecture that will not just enable you to be PCI compliant, but also help you secure the shopping environment, prevent identity theft, reliably protect brand image and assets, mitigate financial risk, and provide a secure foundation for adding new other business services.

Breaches More Numerous, Sophisticated, and Costly

Threats are growing, and efforts to steal data are also becoming more sophisticated, using programmed techniques and hidden code to exploit vulnerabilities. According to the Identity Theft Resource Center, reports of data breaches reached 656 instances at the end of 2008, an increase of 47 percent over 2007. Organizations that experienced a data breach in 2008 paid an average of \$6.6 million to rebuild their brand images and retain customers. Research firm Ponemon Institute found that approximately \$202 was spent on each consumer record compromised. And 84 percent of the companies surveyed had at least one data breach or loss prior to 2008.

Retail Environments Increasingly Complex

Data can be at risk in many places throughout your infrastructure, as well as outside of your organization. Mergers and acquisitions often result in inheriting different systems and policies. Sensitive data is used, transmitted, or stored across a wide range of locations, including stores, offices, and warehouses or distribution centers. Data streams into your organization in high volumes and through channels that may include stores, call centers, and websites. And new retail, database, or communications applications can create new vulnerabilities

Understanding and addressing PCI compliance across retail operations is a complex task. Data in use, at rest, and in motion must be secured at the data center, in all physical locations, across wired and wireless networks, and in transit and use between e-commerce sites and payment processors.



Wireless Networks Considered to Be Public

The PCI standard recognizes wireless LANs as public networks, automatically assuming that they are exposed to public vulnerabilities and threats. New guidelines address PCI compliance requirements specifically for wireless networks and prescribe two practices:

- You must have firewall segmentation between wireless networks and point-of-sale networks, or in front of any network that comes in contact with credit card information.
- You must implement wireless intrusion detection systems to detect unauthorized wireless devices and attacks.

Cisco PCI Solution for Retail

Maintaining compliance is an ongoing commitment because new threats emerge, business needs change, and the PCI specification evolves. The Cisco PCI Solution for Retail helps you secure cardholder data, customer privacy, and your business assets at every point across your business: from the data center, to storefronts, and across e-commerce sites and payment processors.

The Cisco PCI Solution for Retail is built on a Cisco Connected Retail Network platform, proven Cisco products, Cisco Services, and partner solutions that are validated for compatibility with Cisco PCI Solution for Retail architectures and meet Payment Application Best Practices standards.

Cisco Connected Retail Network

The Cisco Connected Retail Network provides a common platform for addressing regulatory requirements, delivering retail business applications, and supporting advanced network services such as security, unified communications, and storage. Network systems span your retail stores, enterprise data center, and the network edge where sensitive data is transported from online customers and to outside partners. Network services include a wide range of technologies that enable security, mobility, identity verification, storage, voice, and collaboration applications.

Retail Architecture Built on Validated Design

A critical element of the Cisco PCI Solution for Retail is Cisco network architecture and validated network designs. More than just printed diagrams, these designs were deployed and tested in Cisco labs. Cisco invited PCI auditors to evaluate them, and with their input developed designs that include end-to-end PCI security recommendations. You can use these design guidelines for your own network as you gain and maintain PCI compliance.

Cisco network architectures have been designed for small, medium-sized, and large retail stores, for enterprise data centers, and for the Internet edge to support e-commerce operations, customers, and teleworkers. They include solutions for both wired and wireless deployments, helping you effectively address PCI requirements across all users and environments.

Cisco Products with PCI Intelligence

Many Cisco products already include features and the specific intelligence needed to help meet PCI requirements:

- **Secure routers:** Integrate advanced communications and security capabilities of Cisco IOS® Software-based routers
- **LAN switches:** Include network-connectivity and integrated service-aggregation products
- **Storage area network switches:** Provide highly secure storage connectivity and encryption of stored payment transaction data
- **Adaptive security appliances:** Deliver encryption, firewall, antiX, intrusion prevention, and VPN capabilities.
- **Wireless access points and controllers:** Provide secure wireless connectivity to retail devices.
- **Cisco Security Agent:** Includes PCI policies and rule sets to automatically help protect servers and clients against threats and information theft
- **Compliance reporting and management:** Offers centralized management, monitoring, and remediation
- **Network Admission Control:** Provides access control for wired and wireless networks

Validated Technology Partners

Solutions from Cisco technology partners have been validated for compatibility with Cisco PCI Solution for Retail network designs and products, and they meet Payment Application Best Practices standards. Solutions for retail include:

- **Point of sale:** Terminals and mobile computing systems, software applications, management and wireless monitoring solutions
- **Payment:** Payment equipment and wireless payment devices for payment validation authorization
- **Encryption:** Industry-standard encryption for data at rest, remote and two-factor authentication, key management, and server log management
- **Audit, scanning, and remediation:** Audit, design, and comprehensive PCI lifecycle services

Cisco Advanced and Advisory Services

Cisco Advanced and Advisory Services help make networks, applications, and the people who use them work better together. Using a Lifecycle Services approach, Cisco provides fixed-price planning, design, and optimization services to help increase business value and return on investment. Several of our services help you address PCI compliance concerns:

- **Gap Analysis and Remediation Planning Service:** Detects system, policy, and process gaps and creates a customized remediation plan
- **Design and Implementation Service:** Helps you develop or refine compliance goals, procedures, and rules; provides design review; and helps implement your solution on time and on budget

- **Asset Monitoring Service, Support for Configuration and Change Management:** Helps you maintain compliance through critical device monitoring, identification of events or anomalies, and providing consistent change management
- **Quarterly Security Gap Analysis:** Assesses your network for changes that might affect compliance, provides periodic reporting, and recommends improvement or remediation as needed

Business Benefits

Protect Mobile Applications and Data

Cisco Unified Wireless solutions can be deployed on a Cisco Connected Retail Network to protect the wired network from wireless threats and to help ensure secure, private communications over authorized wireless LANs. Built-in security capabilities support:

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

Cisco Unified Wireless solutions support industry standards, such as Wi-Fi Protected Access (WPA) and WPA2, as well as integrated radio frequency (RF) scanning and monitoring capabilities. Support for industry standards enables you to secure sensitive cardholder information in both wired and wireless network environments and protect wireless networks and mobile applications from unauthorized use or attack. Cisco Unified Wireless solutions can also identify and prevent rogue access points and unmonitored networks from gaining access to your network. 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 Ongoing Compliance

Cisco architecture and validated network designs encompass the entire range of your operations to help you address PCI requirements across all users and environments. When built on a Cisco Connected Retail Network with proven Cisco products, the infrastructure includes built-in security capabilities and specific intelligence, such as PCI rule sets, needed for helping to meet PCI requirements.

Enhance Company Security and Risk Management

While adaptive security technologies help address PCI requirements, the Cisco Connected Retail Network can also strengthen your company's overall security posture by:

- Supporting and helping enforce security best practices
- Helping protect brand image and assets
- Mitigating the risk of noncompliance fines, penalties, and lost revenue

Enable New Business Initiatives

Investing in a network with advanced capabilities enables you to take advantage of new opportunities. You can add capabilities, such as wireless or voice services, without redesigning the network. The same security capabilities that facilitate PCI compliance can also support new initiatives such as interactive kiosks, unified communications, and wireless applications. In addition, an advanced network facilitates highly secure access for partners and helps control sensitive data from leaking outside of enterprise boundaries.

Strengthen Shopping Security

Investing in security best practices is also an investment in your retail business. The same Cisco Connected Retail Network and proven products that protect store, employee, and customer data can be confidently used for programs that enhance merchandising, improve the shopping experience, and build brand loyalty.

Why Cisco?

Whether you have two stores across town or 2,000 around the globe, Cisco has the solutions, experience, and expertise to help improve your effectiveness and operational capacity. The Cisco Connected Retail Network and Cisco PCI Solution for Retail help you pull everything together to effectively address the PCI data security standard.

Learn More Today

Using the PCI standard as the foundation of a strong security architecture and blueprint benefits more than just customer credit card information; it improves your organization's entire security posture. Cisco retail solutions help you achieve your compliance goals while simultaneously enabling new strategic business initiatives. Call your local Cisco account representative to learn how Cisco retail solutions tailored for meeting PCI requirements can help you.

For more information, visit www.cisco.com/go/retailsolutions.



Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

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.

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco Stackpower, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks, and Access Registrar, Aronnet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo 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. (0903R)