Cisco PCI Solution for Retail 2.0: Simplifying Compliance

Cisco PCI Solution for Retail 2.0: Simplifying Compliance

Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) Version 2.0 has been released, providing clarification and reinforcing the need for merchants and other organizations to identify all system components, people, and processes to be included in a PCI DSS assessment. Simply achieving device and system compliance is not enough to protect your retail business and your customers. Cisco® PCI Solution for Retail 2.0 helps you:

- Address current PCI compliance requirements
- Protect customer data in your data center, stores, Internet edge, contact center and between partners, such as payment processors
- Simplify compliance
- Offer guidance on security best practices

Introduction

Achieving PCI compliance is mandatory for organizations that accept payment cards and other forms of electronic payment. The Verizon 2010 Payment Card Industry Compliance Report is based on a sample of approximately 200 PCI DSS assessments performed by Verizon Qualified Security Assessors. Of the organizations assessed in the study, only 22 percent were validated compliant at the time of their Initial Report on Compliance (IROC). Interestingly, many of these organizations had been successfully validated as compliant during a previous assessment.

In addition to avoiding noncompliance fines, retailers also have brand integrity and network security at stake. Attempts at identity theft, malware, hacking, Structured Query Language (SQL) injection attacks, and exploitation of default credentials–all are increasingly common and vicious. With so much at stake, why is compliance still lagging? The answer: Achieving PCI compliance is not easy. For example, the Verizon report notes that organizations must pass approximately 250 testing procedures, many of which may not exist in a typical security program used by merchants.

Version 2.0 of the PCI Data Security Standard, effective January 1, 2011, included clarifications designed to make adoption easier for merchants. The most significant revisions in PCI Version 2.0 include:

- Clarifications reinforcing the need for merchants and other organizations to thoroughly scope their data storage and network infrastructure environments and to have a method for knowing where cardholder data resides
- Promotion of more effective log management in securing cardholder data
- Allowing organizations to adopt a risk-based approach that is appropriate to their specific business circumstances in order to assess and prioritize vulnerabilities
- Clarifications to better accommodate the unique environments of small merchants, helping to simplify their compliance efforts
- Clarifications that explain the allowed use of virtualization technology with cardholder data

Cisco PCI Solution for Retail 2.0: Simplifying Compliance

The primary goal of the PCI DSS standard is to secure cardholder data. Although technology advances deliver productive new capabilities, they also increase the difficulty of keeping pace with compliance changes. It is not surprising that most organizations struggle with protecting stored credit and debit card data, monitoring access to network resources and cardholder data, and regularly testing security systems and processes. In order to accurately assess their own risks, organizations must understand the increasingly complex path of data as it travels through the networks of card issuers, acquirers, and banks.

Unfortunately, there is no single "silver bullet" technology that can address a growing list of detailed standards and requirements. Technologies such as encryption, tokenization, and Europay, MasterCard, and Visa (EMV) smartcards address portions of your infrastructure, but none provide a single compliance solution.

For these reasons, your security strategy should employ best practices and an architecture that will support PCI compliance and other benefits. For example, it should 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 business services.

Breaches More Numerous, Sophisticated, and Costly

Threats are growing rapidly, and efforts to steal data are also becoming more sophisticated, using programmed techniques and hidden code to exploit vulnerabilities. According to the Ponemon Institute's 2009 study, the percentage of data breaches from malicious attacks and botnets doubled—from 12 percent to 24 percent—from 2008 to 2009, and cost substantially more than those caused by human negligence or IT system glitches. The average cost per compromised record across all causes has continued to increase each year, from $202 in 2008 to $204 in 2009. The Identity Theft Resource Center recorded 662 breaches on its 2010 ITRC Breach List, a slight increase over 2009.

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, email, 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 the Internet edge and payment processors.

Wireless Networks Considered to Be Public

Wireless environments are here to stay in retail. However, many merchants are unsure how to apply the PCI DSS to their wireless environments, especially when there may not be wireless technology deployed in their cardholder environments. Savvy cybercriminals can configure a server, laptop, printer, or other device to exploit weaknesses in point-of-sale (POS) terminals or other store systems, even if there is not a wireless network deployed. As a result, almost any environment is susceptible to attack.

The PCI standard recognizes wireless LANs as public networks, automatically assuming that they are exposed to public vulnerabilities and threats. Therefore, the best wireless security is based on a strategy that looks across the entire wireless spectrum for intrusion.

PCI DSS 2.0 guidelines address PCI compliance requirements specifically for wireless networks and prescribe two fundamental practices:

- Retailers 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.
- Retailers must implement a system to detect unauthorized wireless devices and attacks.

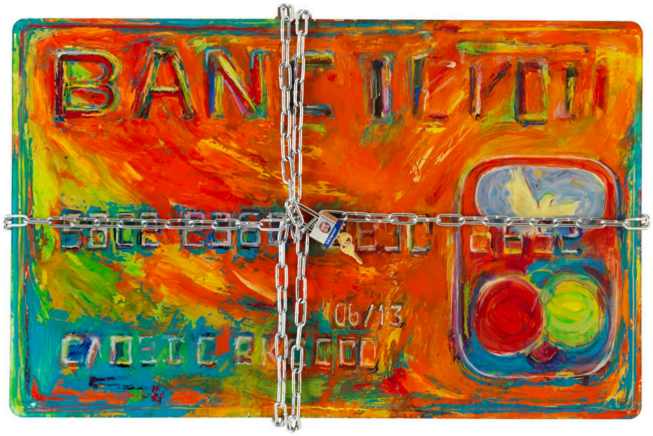
Cisco PCI Solution for Retail 2.0

Maintaining compliance is an ongoing commitment because new threats emerge, business needs change, and the PCI specification evolves. The Cisco PCI Solution for Retail 2.0 helps you secure cardholder data, customer privacy, and your business assets at every point across your business: from the data center, to storefronts and contact centers, the Internet edge and payment processors.

The Cisco PCI Solution for Retail 2.0 is built on network security best practices, the Cisco Connected Retail Network platform, proven Cisco products, Cisco services, and partner technologies that are validated for compatibility with Cisco PCI solution architectures and meet PCI DSS requirements.

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, video surveillance, and storage. Network systems span your retail stores, enterprise data center, contact 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, video, and collaboration applications.



Retail Architecture Built on Validated Design

A critical element of the PCI solution is Cisco's network architecture and validated network designs. More than just printed diagrams, the underlying products were deployed and tested in Cisco labs. Verizon Business, a Cisco partner, reviewed the products and network designs and issued an assessment report. With Verizon Business, Cisco developed designs that include end-to-end PCI security best practices and recommendations. You can use these design guidelines for your own network as you achieve and maintain PCI compliance.

Cisco network architectures have been designed for stores, enterprise data centers, contact centers, and the Internet edge to support e-commerce operations, store employees, customers, and teleworkers. Cisco PCI Solution for Retail 2.0 also supports wireless 3G technology deployments and multiple store formats, including pop-up stores, convenience stores, in addition to typical small, medium, and large stores. Cisco network architectures include products for both wired and wireless deployments, helping you effectively address PCI requirements across all users and environments.

Cisco and Partner Products with PCI Intelligence

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

- **Routing:** Cisco Integrated Services Routers (ISR, ISR G2), Cisco Aggregation Services Routers (ASR)
- **Switching:** Cisco Catalyst® compact switches, Cisco Catalyst access switches, and Cisco Catalyst data center switches, Cisco Nexus® 1000V Series Switches, Cisco Nexus 5000 and 7000 Series Switches, Cisco Application Control Engine (ACE), Cisco Multilayer Director Switch (MDS) with Storage Media Encryption module

- **Network Security:** Cisco Adaptive Security Appliance (ASA), Cisco IronPort® Email Security Appliance, Cisco Network Admission Control (NAC) Appliance, Cisco AnyConnect™ VPN, Cisco Firewall Services Modules (FWSM), Cisco Intrusion Detection System Services Modules (IDSM), Cisco Intrusion Prevention System Appliances (IPS), Cisco Nexus Virtual Security Gateway (VSG), Cisco IOS® Firewall, Cisco IOS IPS, Cisco Secure Access Control Server (ACS)
- **Wireless:** Cisco Aironet® Access Points, Cisco Wireless LAN Controllers, Cisco Mobility Services Engine with enhanced local mode (ELM), Cisco Adaptive Wireless IPS
- **Physical Security:** Cisco Video Surveillance Operations Manager (VSOM), Cisco Video Surveillance IP Cameras, Cisco Physical Security Multiservices Platform (MSP), Cisco Physical Access Manager, Cisco Physical Access Gateways
- **Compute Systems and Storage:** Cisco Unified Computing System™ (UCS), Cisco UCS Express
- **Management:** Cisco Security Manager, Cisco Wireless Control System (WCS), CiscoWorks LAN Management Solution (LMS)
- **Voice:** Cisco Unified Communications Manager, Cisco Unified Contact Center Enterprise, Cisco Unified Intelligent Contact Management, Cisco Unified Customer Voice Portal, Cisco Unified IP Phones
- **WAN Optimization:** Cisco Wide Area Application Engine (WAE), Cisco Wide Area Application Services (WAAS)

Validated Technology Partners

Products from Cisco technology partners have been validated for compatibility with Cisco PCI Solution for Retail 2.0 network designs and products. Technology partners include:

- **RSA:** Authentication, security, and compliance technology for data centers and stores. Products include:
  - **RSA Archer eGRC Platform**: An integrated governance, risk, and compliance platform that helps retailers assess security, identify areas of concern, prepare for a PCI audit and manage the reporting process.
  - **RSA enVision®**: Tightly integrated with RSA Archer, RSA enVision offers an effective security and information event management (SIEM) and log management system, capable of collecting and analyzing large amounts of log and event data in real-time.
  - **RSA SecurID®**: Two-factor authentication based on something you know (a password or PIN) and something you have (an authenticator); provides a much more reliable level of user authentication to cardholder data than reusable passwords.
  - **RSA Data Loss Prevention (DLP) Suite**: Enables organizations to discover and classify cardholder data, educate end users and ensure cardholder data is handled appropriately, and report on risk reduction and progress towards policy objectives.
  - **RSA Data Protection Manager**: Enterprise tokenization and encryption controls further strengthen PCI compliance by protecting cardholder data at rest and in transit across public networks.
- **VCE:** Next-generation virtualized converged infrastructure and private cloud technology
  - **Vblock™ Infrastructure Platforms:** Preintegrated, best-in-class datacenter infrastructure and rapid deployment private cloud platforms. Built with industry-leading VMware virtualization; Cisco networking and computing; and EMC storage, security, and management technologies
- **HyTrust:** Virtualization infrastructure security and logging
  - **HyTrust Appliance:** Policy management, access control, logging, and logical infrastructure segmentation for virtual infrastructures
- **EMC:** Storage and storage management technology. Products include:
  - **EMC CLARiiON® CX4 Series Storage Area Network (SAN):** Scalable networked storage optimized for virtualized environments
  - **EMC Ionix™ Unified Infrastructure Manager (UIM):** Simplified, integrated provisioning, configuration, change, and compliance management across network, storage, and compute resources for Vblock Infrastructure Platforms
  - **EMC Ionix™ Network Configuration Manager (NCM):** Model-based and automated compliance, change, and configuration management for networks
- **Verizon Business:** Consulting Services
  - **Qualified Security Assessor:** PCI audit, PCI readiness assessments, PCI Compliance Management Program, penetration testing, vulnerability scanning, and PCI consulting and remediation services

Cisco PCI Solution for Retail 2.0: Simplifying Compliance

Cisco Advanced and Advisory Services

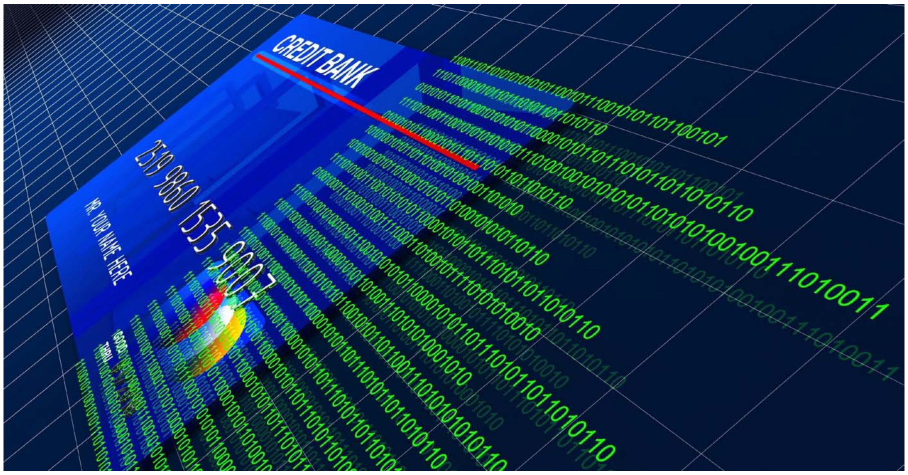
Cisco Advanced Services and Cisco Advisory Services help make networks, applications, and the people who use them work better together. Using a Lifecycle Services approach, Cisco Services provides planning, design, and optimization services to help increase business value and return on investment. Several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

- **Cisco IT GRC Security Assessment Service:** The Cisco IT Governance, Risk Management, and Compliance (GRC) Security Assessment Service works with customers to assess effectiveness of their security programs and processes, establish benchmark metrics, and map security technical controls to PCI requirements and other standards.
- **Cisco IT GRC Strategy Planning Service:** This service helps organizations benchmark their security programs against industry standards and best practices. They also identify organizational inefficiencies, misalignments, and redundancies that may be undermining success.
- **Cisco Security Posture Assessment Service:** To directly address PCI Requirement 11 for penetration testing, the Cisco Security Posture Assessment Service performs vulnerability and penetration tests on the customer's perimeter and internal networks. The service discovers security weaknesses in the existing network by successfully gaining unauthorized access to the cardholder data environment and credit card information.
- **Cisco Design and Implementation Service:** This service develops or refines the security architecture so that it adheres to compliance regulations and industry-leading practices and can provide implementation engineering consulting and support.

Cisco Technical Services

Cisco Technical Services can cost-effectively maintain secure payment systems for customer-sensitive information while also improving operational efficiency. Based on best practices, Cisco Technical Services are designed to help accelerate your transition to an advanced payment architecture that optimizes performance, reliability, and security, and scales easily with growth in financial transactions.

- **Cisco SMARTnet® Service:** Your IT staff gains direct, anytime access to Cisco engineers and extensive Cisco.com resources to accelerate problem resolution, facilitate 24-hour business continuity, and improve operational efficiency.
- **Cisco Services for IPS:** This service protects your intrusion prevention system with the most up-to-date information to defend against attacks from local and global threats. Cisco Services for IPS not only helps reduce risk exposure, but also helps support the productivity of internal staff who are charged with maintaining security systems.
- **Cisco Remote Management Services for Security:** Cisco Remote Management Services (RMS) for Security provides 24/7/365 remote management, surveillance, monitoring, and remediation for networks to help protect against sophisticated attacks and new vulnerabilities.



Business Benefits

Secure Private Clouds, Virtualized Infrastructure and Applications

VCE Vblock Infrastructure Platforms and HyTrust Appliance technologies allow retailers to take advantage of the economic benefits of virtualization within their PCI infrastructures. Vblock Infrastructure Platforms deliver a completely integrated offering that combines best-in-class VMware virtualization, Cisco networking and computing, and EMC storage, security, and management technologies. This platform is designed for the high scalability, reliability, flexibility, and security needs in PCI environments.

Protect Mobile Applications and Data

Cisco Unified Wireless Network products 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
- User segmentation for access to appropriate resources
- Security strategies for client devices

Cisco Unified Wireless Network products 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 Network products can also identify and prevent rogue access points and unmonitored networks from gaining access to your network. For retail sites that do not have wireless LAN coverage, innovative air monitoring capabilities enable retailers to protect these sites from unauthorized wireless access.

Build a Foundation for Ongoing Compliance

Cisco architecture, validated network designs, and proven products from Cisco, RSA, EMC, VCE, and HyTrust encompass the entire range of your operations to help you address PCI requirements across all users and environments.

Enhance Company Security and Risk Management

While adaptive security technologies help address PCI requirements, the Cisco PCI Solution for Retail 2.0 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 flexible, PCI-ready network 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 keep 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 PCI Solution for Retail 2.0 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.

Cisco PCI Solution for Retail 2.0: Simplifying Compliance

Why Cisco?

Whether you have two stores across town or 2000 around the globe, Cisco and our technology partners have the technology, experience, and expertise to help improve your effectiveness and operational capacity. Cisco's PCI solution helps you pull everything together to effectively address the PCI Data Security Standard.

Cisco Capital

Through its knowledge of Cisco, Cisco Capital® is uniquely positioned to offer flexible financing options to help you obtain Cisco products, as well as products from Cisco PCI Solution for Retail 2.0 technology partners at competitive interest rates. You can address PCI compliance without a large upfront investment and preserve cash. We can help you match your expenses to technology benefits and revenue, to deliver increased business flexibility. We also provide flexible migration and upgrade options while enabling you to avoid having to dispose of equipment. Cisco Capital can help put your PCI compliance strategy into action faster.

The Cisco PCI Whole Offer

Cisco's PCI solution helps retailers simplify compliance. A PCI whole offer helps retailers simplify purchasing from Cisco. The offer includes Cisco PCI services, product financing, and incentives on specific products and services included in the design and validation of the Cisco PCI Solution for Retail 2.0.

Learn More Today

Using the PCI DSS standard as the foundation of a strong security architecture benefits more than just customer credit card information; it improves your organization's entire security posture. The Cisco PCI Solution for Retail 2.0 helps 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 to meet 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.**