



## PCI Compliance: Improve Payment Security

The latest Payment Card Industry (PCI) Data Security Standards (DSS) for customer data give you more ways to address an evolving risk environment and meet PCI compliance requirements. As the threat of security breaches grows, protecting your distribution network and customers goes beyond simply achieving device and system compliance. The Cisco® PCI Connected Payments solution serves insurance firms by helping you:

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

### Challenges

As more consumers use payment cards, the risk associated with lost or stolen cards increases. Growing 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. Threats are increasing, and efforts to steal data are also becoming more sophisticated.

Understanding and addressing PCI compliance across insurance operations is a complex task. Data can be breached on point-of-sale devices in an agency office, on wireless or mobile devices, at call centers, on personal computers, and throughout the card processing system of service providers and financial institutions. 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 between e-commerce sites and payment processors.

Mergers and acquisitions often result in inheriting different systems and policies. And new customer service, CRM, database, or communications applications can create new vulnerabilities.

Version 1.2 of the PCI Data Security Standard (DSS), effective October 1, 2008, moved 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 DSS version 1.2 include:

- **Network segmentation:** Networks can be segmented 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 networks:** All Wired Equivalent Privacy (WEP) networks must be decommissioned by June 30, 2010, and all wireless LANs must be treated as public networks, with intrusion detection systems as well as firewall segmentation in front of any network coming in contact with credit card information.
- **Audit requirements:** PCI auditors are required to test the effectiveness of your network segmentation, justify the sample size with documentation, and meet other new requirements.

### Cisco PCI Connected Payments Solution

The Cisco PCI Connected Payments solution is built on a Cisco Smart+Connected Insurance network platform, proven Cisco products, Cisco Services, and partner solutions that are validated for compatibility with Cisco architectures and meet Payment Application Best Practices standards.

#### Cisco Smart+Connected Insurance Network

The Cisco Smart+Connected Insurance network platform provides a common platform for addressing regulatory requirements, delivering insurance business applications, and supporting advanced network services such as security, unified communications, and storage. Network systems span your agency channel, 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.

#### Architecture Built on Validated Design

A critical element of the solution 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 agency offices, 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:

- **Routers:** Integrate advanced communications and security capabilities of Cisco IOS® Software
- **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 highly secure wireless connectivity to payment 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 network designs and products, and they meet Payment Application Best Practices standards. Solutions 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

### Business Benefits

Your security strategy should employ best practices and an architecture that will not just make you PCI compliant, but also help you secure your transaction environment, maintain PCI compliance, reliably protect your assets and mitigate financial risk, and be ready to add new business services. The Cisco® PCI Connected Payments solution helps you secure cardholder data and your business assets at every point across your business.

### Protect Mobile Applications and Data

The Cisco PCI Connected Payments solution helps you protect your wired network from wireless threats and 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

The solution supports industry standards such as Wi-Fi Protected Access (WPA) and WPA2, as well as integrated radio frequency (RF) scanning and monitoring capabilities. This enables you to secure sensitive cardholder information in both wired and wireless network environments and protect wireless networks and mobile applications from attack or unauthorized use. The solution can also identify and prevent rogue access points and unmonitored networks from gaining access to your network. Innovative air monitoring capabilities enable you to protect agency offices 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 Smart+Connected Insurance 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 as they evolve.

#### **Enhance Company Security and Risk Management**

While adaptive security technologies help address PCI requirements, the Cisco Smart+Connected Insurance network underlying Cisco PCI Connected Payments 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 video, unified communications, and wireless applications. In addition, an advanced network facilitates highly secure access for partners and helps control sensitive data from leaking outside your enterprise boundaries.

#### **Cisco Services**

Cisco Services help make your 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 with PCI standards, provides periodic reporting, and recommends improvement or remediation as needed

## Why Cisco?

- Cisco works closely with leading corporations and financial services organizations worldwide and has carefully built a collection of network, security, application, and management best practices that address the PCI Data Security Standard.
- Cisco has the deep understanding and architectural approach to support the underlying network as a platform that spans the enterprise and distributed agency/broker channel.
- Cisco is a participating member of the PCI Security Standards Council and was elected to its Board of Advisors in 2009.
- Cisco has formed partnerships with leading financial services partners across the insurance value chain to bring you solutions that address the unique functional, security, and compliance requirements of insurance companies.
- Cisco is recognized as one of the top five companies in the Fintech 100 top 25 Enterprise Companies list, and non-life (property and casualty) insurance carriers voted Cisco tops in customer care in the Insurer's Choice Technology Ranking 2009.
- Cisco offers a strong financial foundation as an industry leader, providing you with a technology partner that will continue to support your business and meet your needs in the long term.

## For More Information

To learn more about how the Cisco PCI Connected Payments solution can benefit your organization, contact your account manager or visit:

<http://www.cisco.com/go/financialservices>



**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](http://www.cisco.com/go/offices).

CCDE, CCENT, CCSI, Cisco Eos, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco Nurse Connect, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flip Video, Flip Video (Design), Flipshare (Design), Flip Ultra, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Store, and Flip Gift Card are service marks; and Access Registrar, Aironet, 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. (0907R)