

Cisco Self-Defending Network Solution for PCI Compliance in Healthcare

Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) was designed to protect customer privacy and their credit card information. However, meeting PCI requirements can be a challenge for many healthcare customers. The Cisco® Self-Defending Network PCI solution provides guidance for healthcare institutions working to reach PCI compliance. Cisco offers the Cisco PCI Validated Architectures—a set of PCI audited architectures for remote location, Internet edge, and data center networks—to help with the design and implementation of network security for PCI.

Introduction

PCI was designed to ensure the security of cardholder data and information while in transit or at rest. PCI applies to any company that stores, processes, or transmits credit card information. This means that the PCI standard impacts most industries, including healthcare. Healthcare institutions may process credit card information in several locations, including registration and admittance areas, pharmacies, gift shops, cafeterias, in-room services, and online billing and payment processes. And wherever credit card data is stored, those locations also are part of the PCI scope. Areas such as the data center, remote clinics, or different departments that may store credit card data, are all impacted by the PCI DSS.

The Risks of Noncompliance

In the United States, the deadline for merchants to become PCI-compliant was September 30, 2007 for Level 1 merchants and December 31, 2007 for Level 2 and Level 3 merchants. Companies that missed this deadline may receive fines between US\$5,000 and \$25,000 per month, with some companies receiving \$100,000 fine per month. European merchants (non-Level 1 merchants) have until December 31, 2008, and Level 1 merchants in Asia have until December 31, 2009.

Consequences are severe because of the high risk associated with compromised data. Security breaches have resulted in lawsuits, government investigations, expensive damage cleanup, reduced revenue, and damage to reputations. Some of the more expensive breaches have resulted in hundreds of millions of dollars in damage costs.

The Challenge of Meeting Requirements

PCI compliance requirements are comprehensive, but are built upon security best practices and provide more detailed information than most compliance regulations. Table 1 shows the 12 PCI requirements.

Table 1. PCI Requirements

PCI Data Security Standard Requirements	
Build and Maintain a Secure Network	<ol style="list-style-type: none"> 1. Install and maintain a firewall configuration to protect data 2. 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 data 4. 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 software 6. 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-know 8. Assign a unique ID to each person with computer access 9. 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 data 11. 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. Cisco offers a network foundation that is an important step for healthcare institutions to achieve regulatory compliance requirements and implement data security best practices.

Cisco Self-Defending Network Solution for PCI

Cisco has developed a set of architectures (including remote locations, the Internet edge, and the data center) in a lab environment to address PCI requirements. Cisco invited a global PCI Qualified Security Assessor (QSA) to evaluate these architectures. The auditors found that the technology, if properly deployed and maintained, helps customers achieve PCI compliance. Customers can use these network architectures as a guideline for deploying their own network installations as they work toward PCI compliance.

Learn More Today

Cisco PCI solutions can help healthcare customers achieve their compliance goals and simultaneously enable new strategic business initiatives. Call your local Cisco account executive to learn how Cisco healthcare solutions tailored for meeting PCI requirements can help you reach your compliance goals. For more information, visit <http://www.cisco.com/go/healthcare> and <http://www.cisco.com/go/compliance>.



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.

CCDF, CCENT, Cisco Eos, Cisco StadiumVision, the Cisco logo, DCE, and Welcome to the Human Network are trademarks. Changing the Way We Work, Live, Play, and Learn is a service mark and Access Register. 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, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IQ Experience, the IQ logo, IQ Net, Readiness Scorecard, iQuickStudy, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MEX, Newscenter, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SNA First, 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. (080239)