Cisco PCI Solution for Healthcare

At-A-Glance

Why Payment Card Industry Standard?

The Payment Card Industry (PCI) Data Security Standard, introduced in 2005, applies to all businesses worldwide, public and private, that process, transmit, or store credit card transactions, including the healthcare industry. The goal of PCI is to increase protection of customer credit card information.

PCI Deadlines and Effect

The U.S. Level 1 merchant deadline was September 30, 2007 (with some extensions to September 30, 2008), and the Level 2 merchant deadline was December 31, 2007 (with some extensions to December 31, 2008). The Level 3 merchant deadline is expected to be December 31, 2008. If a healthcare organization does not achieve PCI compliance by this date, acquiring banks will issue monthly fines until that organization becomes compliant. These monthly fines can range from US$5,000 to $25,000, and can increase further over time. These fines are for noncompliance—not for security breaches. European merchants (non-Level 1 merchants) have until December 31, 2008. Dates for other countries range from November 2008 through December 2009. Visa can provide specific deadline dates for each country and merchant level.

The PCI standard provides 12 security requirements that companies must adhere to:

1. Install and maintain a firewall configuration to protect data.
2. Do not use vendor-supplied defaults for system passwords and other security parameters.
3. Protect stored data.
4. Encrypt transmission of cardholder data and sensitive information across public networks.
5. Use and regularly update antivirus software.
6. Develop and maintain secure systems and applications.
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.
10. Track and monitor all access to network resources and cardholder data.
11. Regularly test security systems and processes.
12. Maintain a policy that addresses information security.

Table 1 gives validation requirements for Levels 1 through 4 for the United States and Europe.

Table 1 Merchant Levels 1–4 for the United States and Europe (other countries have some differences)

PCI Level	Transaction Volume	Validation Requirements
Level 1 (~360)	• Process more than 6 million Visa (or MasterCard, AMEX, JCB, or Discover) transactions annually **Note:** Any company that has suffered a credit card breach in the last 12 months	• Annual onsite audit by Qualified Security Assessor (QSA) • Quarterly network scan by Approved Scan Vendor (ASV) • Self-assessment questionnaire signed by officer of company
Level 2 (~1000)	• Process 1 million to 6 million transactions annually	• Quarterly network scan by ASV • Self-assessment questionnaire signed by officer of company
Level 3 (~2600)	• Process 20,000 to 1 million e-commerce transactions annually	• Quarterly network scan by ASV • Self-assessment questionnaire signed by officer of company
Level 4	• Process fewer than 20,000 e-commerce transactions annually	• Quarterly network scan by ASV (recommended) • Self-assessment questionnaire signed by officer of company

Cisco PCI Solution for Healthcare

Cisco® PCI Solution for Healthcare is a set of architectures (including remote locations, main hospital campus, the Internet edge, and the data center) in a lab environment to address PCI requirements, and complementary professional services to help healthcare organizations achieve and maintain PCI compliance.

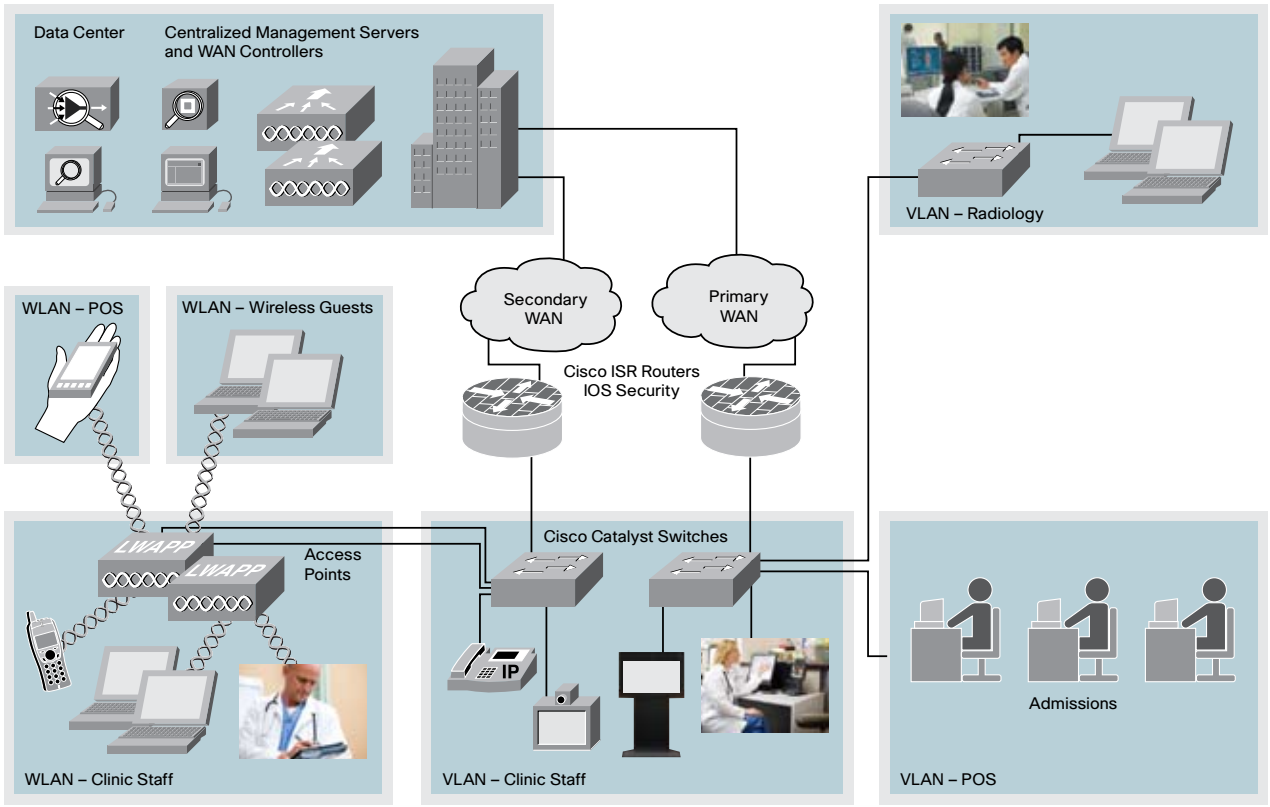
Cisco invited a global PCI Qualified Security Assessor (QSA), Verizon Business, to evaluate these test architectures. The auditors found that the technology—if properly deployed, maintained, and monitored—can help customers achieve PCI compliance. Customers can use these network architectures as a guideline as they work toward PCI compliance. Figure 1 shows the network architecture for a medical clinic.

What Are the Benefits of the Cisco PCI Solution for Healthcare?

The Cisco PCI Solution for Healthcare addresses many of the 12 PCI technology requirements and provides comprehensive best practices for securing sensitive information. The Cisco PCI Solution for Healthcare can strengthen your company's overall security posture and help you satisfy the PCI requirements cost-effectively and efficiently.

Cisco PCI Solution for Healthcare

Figure 1 Medical Clinic Deployment (25 to 100 devices)



Cisco PCI Compliance Services

Cisco PCI Compliance Services can help customers achieve PCI compliance, and then maintain a compliant state. Cisco PCI Compliance Services consist of four capabilities:

- **Cisco PCI Gap Analysis Service:** Assesses your network relative to the PCI Data Security Standard
- **Cisco PCI Remediation Service:** Addresses and closes compliance gaps as needed
- **Cisco PCI Remote Monitoring and Management Service:** Identifies threats rapidly
- **Cisco PCI Periodic Gap Analysis Service:** Identifies potential gaps and risks proactively

For More Information

For more information about the Cisco PCI Solution for Healthcare, please contact your local Cisco account manager or security product sales specialist, or go online to www.cisco.com/go/healthcare, or www.cisco.com/go/compliance, and www.cisco.com/go/services/security for more information about Cisco PCI Compliance Services.