CHAPTER 1

Solution Overview

The Payment Card Industry Data Security Standard (PCI DSS) is generally perceived to be a complicated means to secure sensitive information. As of 2010, according to the PCI Security Standards Council, 100 percent of all breached companies were not compliant at the time of the breach, regardless of whether they were compliant at the time of their audit. How did a company that took such pains to achieve compliance not take equal measures to maintain it? Is the standard really so complex that it is not capable of being sustained? Some pundits have argued that PCI is therefore an unrealistic goal and valueless.

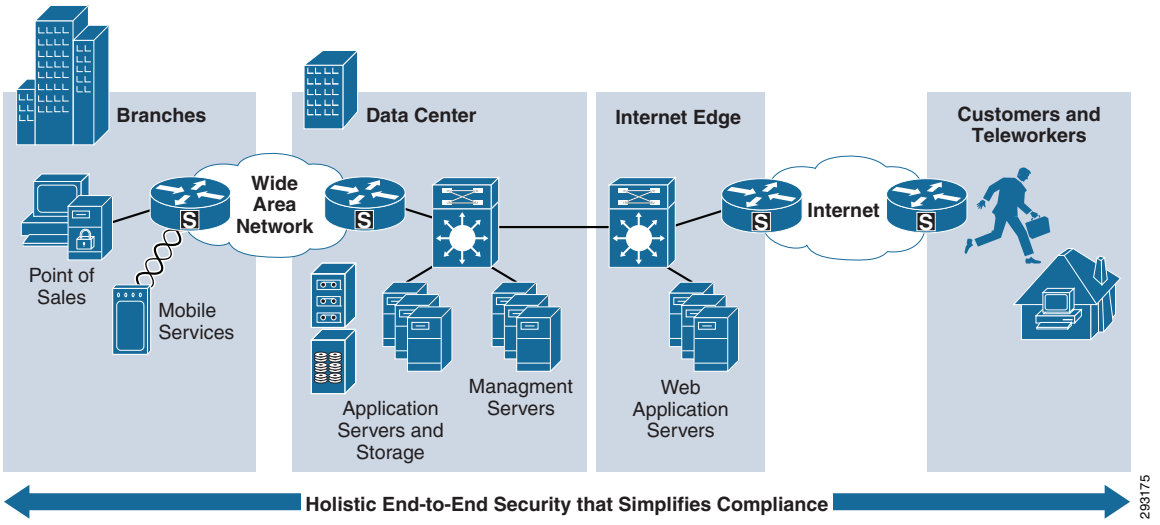
Cisco takes a more balanced stance. PCI is not overly stringent from a security perspective. In fact, Cisco sees the PCI security standard to be the *minimum* security any company should have when taking payments. PCI is a global attempt at setting a minimum bar. Some very large companies and some entire countries have not developed a security awareness that meets the evolved threats of cybersecurity today. From that perspective, PCI is the lowest common denominator that provides the minimum level of protection. Putting in a firewall, changing default passwords, locking the door to the wiring closet, and making sure that you have knowledge of who is configuring a device rather than leaving open a general admin account; these items are not complex.

Although the standard is indeed intricate, the real complexity challenge comes from managing an enterprise network. Enterprise companies do not arise overnight. Most companies that existed in the 1980s did not consider data security to be an ingredient that must be included at all levels. After IP became the de facto network protocol, enterprise companies have been struggling to integrate data with voice systems, video, wireless, digital media, administrative duties, and business processes; as well as holistically integrate protection of payment card information throughout. Each of these technologies was developed independently of each other. With the advent of IP, they have merged, in sometimes inefficient and complex fashion.

Therefore, the real struggle is to develop a simple, sustainable, and operationally efficient enterprise architecture. This foundation needs to have security integrated not only within its technical infrastructure but within its processes and policies as well. This manual is written to provide resources to address these issues and to help simplify compliance.

Figure 1-1 shows the enterprise architecture.

Figure 1-1 Enterprise Architecture



Executive Summary

The Cisco Compliance Solution for PCI DSS 2.0 was developed to help organizations simplify and maintain PCI compliance. The main feature of the solution is *segmentation*. The solution refines a company's compliance needs in the following ways:

- **Defining where sensitive payment information flows**

  This simply means putting sensitive data onto its own network. By segmenting your existing architecture, you can reduce audit costs and simplify maintenance.

- **Protecting the segmented area**

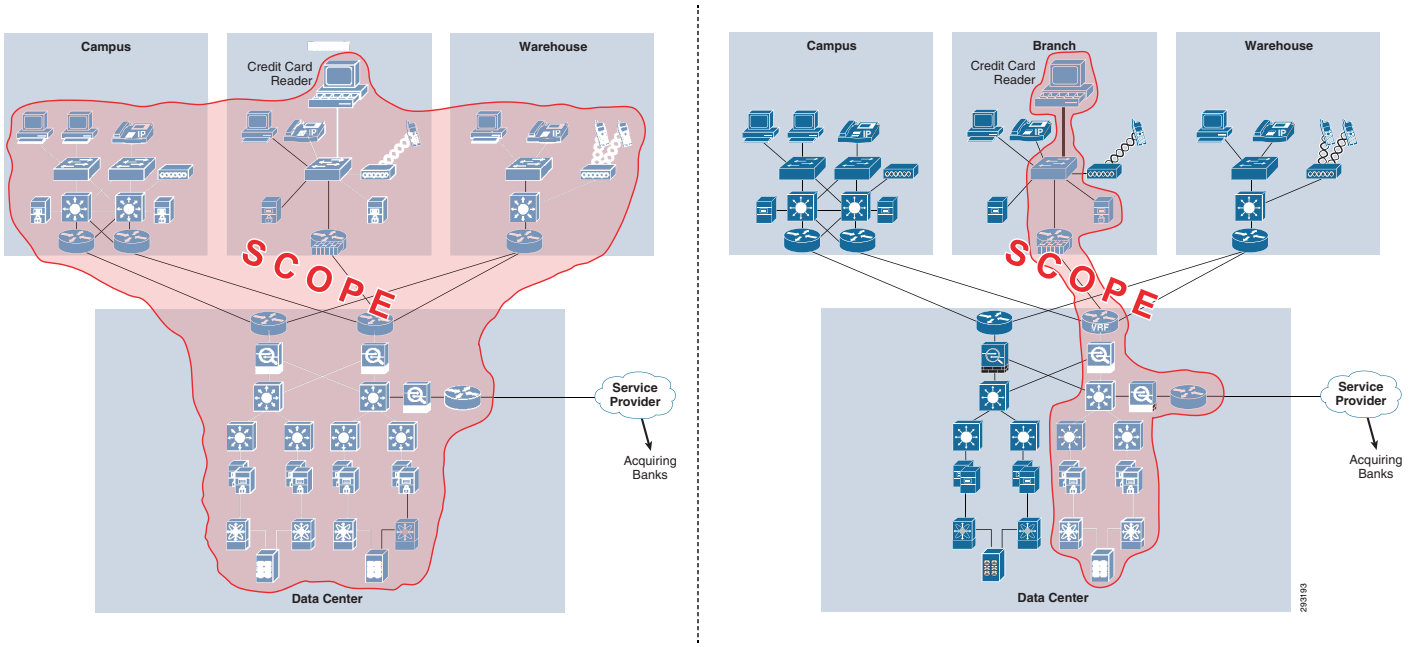
  With a clearly defined scope in which credit card data enters, flows, resides, and exits, you can easily identify the area's perimeter. Any boundary that touches public or untrusted networks must have firewall protection and intrusion detection capabilities.

- **Ensuring that you can effectively monitor the segmented environment**

  The Cisco Compliance Solution for PCI DSS 2.0 provides the ability to monitor the secured environment for threats, misconfiguration, and internal espionage. You must know the status of this sensitive area and the people that have access to it to maintain compliance.

Figure 1-2 shows an enterprise network that does not use segmentation and one that does.

Figure 1-2 Enterprise Architecture—Without and With Segmentation



The solution consists of strategic guidance as well as tactical implementation. Cisco is in the unique position to apply its enterprise-wide architecture experience to the requirements of PCI.

Chapter 3, "Solution Architecture," discusses what organizations should consider when designing their posture for addressing PCI. It examines enterprise architecture and discusses the related controls within them. Chapter 4, "Component Assessment," then separates the solution architectures into their components. Each component is individually assessed for its capabilities, and configuration examples are given to demonstrate this utility. The solution shows how each component was assessed by Verizon Business and gives implementation examples and design considerations. The solution is designed to conform to PCI DSS 2.0.

The solution was built and tested using a holistic enterprise perspective including the following:

- Endpoint considerations—Point-of-sale (POS) systems and payment devices, including wireless payment devices
- Administrative concerns within scope of PCI
- Cisco, RSA, EMC, VCE, and HyTrust network infrastructure
- Assessment by Verizon Business, a qualified security assessor

The result is a set of branch, data center, and Internet edge architectures and designs that simplify the process of becoming PCI compliant, maintaining that posture and providing the capability of awareness when under attack. The Cisco PCI solution is part of the Cisco SecureX strategy, which allows you to establish and enforce security policies across the entire distributed network, not just at a single point in the data stream. By leveraging global and local security intelligence for dynamic, real-time threat protection, Cisco SecureX responds to the evolving security needs of today's borderless network environments. More information about Cisco SecureX can be found at www.cisco.com/go/securex.

Target Market/Audience

This solution is targeted toward the following audiences:

- Technical or compliance-focused individuals seeking guidance on how to holistically design and configure for PCI compliance
- Organizations that require a qualified security assessor to provide a Report of Compliance
- Organizations interested in preparing for growth that will someday require a Report of Compliance.

Although all organizations that take credit cards are required to be PCI compliant, this solution is designed to help the larger companies simplify the complexity of compliance. Smaller companies can benefit from the design and guidance as well, but should consult their acquiring banks for specifics if they do not currently require an onsite audit. Specific card programs are available at the following locations to determine their specific categorization process;

- American Express—http://www.americanexpress.com/datasecurity
- Discover Financial Services—http://www.discovernetwork.com/fraudsecurity/disc.html
- JCB International—http://www.jcb-global.com/english/pci/index.html
- MasterCard Worldwide—http://www.mastercard.com/sdp
- Visa, Inc.—http://www.visa.com/Cisp

Solution Benefits

This solution demonstrates how to design end-to-end systems that conform to PCI DSS 2.0 guidelines. Companies can simplify PCI compliance by building a similar network with the recommended configurations and best practices. In addition, this solution provides the following benefits:

- A reference set of architectural designs and the controls used to address PCI
- A detailed analysis of Cisco and Partner components and their relationship with PCI DSS sub-requirements
- A centralized management tool kit, which provides operational efficiency
- Insight into the PCI audit process by providing an assessment report from Verizon Business

PCI Solution Results

Table 1-1 provides a summary of the PCI assessment results.

Cisco Compliance Solution Components

This solution combines components to create an end-to-end solution conforming to the requirements of the PCI 2.0 guidelines. The result is a set of branch, data center, and Internet edge architectures and designs that simplify the process of achieving and maintaining compliance.

Endpoints	Primary PCI Function
Cisco IronPort Email Security	DLP
Cisco Physical Access Control	9.1
Cisco UCS and UCS Express	Servers
Cisco Unified CM and IP Phones	9.1.2
Cisco Video Surveillance	9.1.1

Administration	Primary PCI Function
Cisco ACS	7.1
Cisco Identity Services Engine	7.1, 11.1b, 11.1d
Cisco Prime LMS	1.2.2
Cisco Security Manager	1.2
Hytrust Appliance	10.5
RSA Authentication Manager	8.3
RSA Data Protection Manager	3.5
RSA enVision	10.5

Infrastructure	Primary PCI Function
Cisco ASA-Branch	1.3, 11.4
Cisco ASA-Data Center	1.3, 11.4
Cisco Branch Routers	1.3, 11.4
Cisco Branch Switches	Segmentation
Cisco Data Center Routers	1.2, 1.3
Cisco Data Center Switches	Segmentation
Cisco Data Center IDSM	11.4
Cisco MDS Switches	3.4
Cisco Nexus 1000V Series Switch	Segmentation
Cisco Nexus Data Center Switches	Segmentation
Cisco Nexus VSG	Virtual Firewall
Cisco Wireless	4.1, 11.1
EMC CLARiioN SAN	Storage