



SOLUTION OVERVIEW



Enterprise Compliance Solutions for the Payment Card Industry



Where it all comes together.™



CONTENTS

+ Who Must Comply?	3
+ PCI Data Security Standards	4
+ VeriSign® PCI Compliance Solutions: Leveraging Expertise, Intelligence, Trust	4
VeriSign® Global Security Consulting	4
Annual PCI Audits	4
Application Best Practice Certification	5
Incident Response and Forensics	5
VeriSign® Managed Security Services	5
PCI Scanning and Testing Services	5
VeriSign® Firewall Management Service	5
VeriSign® Intrusion Detection Management and VeriSign® Intrusion Prevention Management Service	6
VeriSign® Log Monitoring Service	6
VeriSign® iDefense Security Intelligence Services	6
VeriSign® Unified Authentication Services	6
+ Summary	7
+ Learn More	7
+ About VeriSign	7
+ PCI Data Security Standard and Related Information	7





Enterprise Compliance Solutions for the Payment Card Industry

Theft of cardholder data is a growing threat that carries potentially enormous liability—both from fines charged by credit card associations and from loss of public confidence in your enterprise. The Payment Card Industry (PCI)—with Visa, MasterCard, American Express, and others—has come together to establish the PCI Data Security Standard, which mandates that merchants and service providers meet minimum standards of security. If you are a service provider or a merchant, you need to protect your critical digital data now. If you are an acquirer, you not only have to protect your own data; you also must ensure that your affiliated merchants and service providers are implementing necessary security measures.

VeriSign offers a complete suite of compliance solutions for the Payment Card Industry. The suite includes consulting, managed security, strong authentication, and messaging security services. VeriSign was one of the first assessors to conduct PCI onsite audit and scanning services under the Visa Cardholder Information Security Program (CISP) and MasterCard Site Data Protection (SDP) program. As a trusted provider of intelligent infrastructure services, VeriSign possesses the proven technology, hands-on expertise, and global intelligence to help companies appropriately and cost-effectively address PCI requirements.

+ Who Must Comply?

Any company that processes, stores, or transmits credit card data must comply with the PCI Data Security Standard. PCI has grouped companies by their types as well as how many transactions they process. Using these groupings, the PCI has assigned levels, from largest (Level I) to smallest (Level IV). (To determine your level, use the links provided at the end of this document.) Merchants are companies that conduct business, either online or in traditional “brick-and-mortar” fashion. Service providers (and payment gateways) are companies that facilitate transactions on behalf of merchants and acquiring banks. Based on its level, a company must perform a series of tasks to substantiate its compliance with the PCI. The following table indicates these tasks.

CATEGORY/LEVEL	MEET THE PCI DSS	ANNUAL AUDIT	ANNUAL SELF-ASSESSMENT	ANNUAL PENETRATION TEST	QUARTERLY SCANNING
Service Provider - Level I	X	X		X	X
Service Provider - Level II	X	X		X	X
Merchant - Level I	X	X		X	X
Merchant - Level II	X		X	X	X
Merchant Level III	X		X		X
Merchant - Level IV	X	*	*	*	*

* At the discretion of the acquiring banks.



+ PCI Data Security Standards

Regardless of transaction volume and the steps required to demonstrate compliance, all companies must adhere to the PCI Data Security Standard. The following table summarizes key provisions of these standards. A downloadable version of the entire text of the Data Security Standard is available on the Visa Web site (see the address at the end of this document).

PCI Data Security Standards	
Build and Maintain a Secure Network	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	3. Protect stored data 4. Encrypt transmission of cardholder data and sensitive information across public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	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	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

+ VeriSign® PCI Compliance Solutions: Leveraging Expertise, Intelligence, Trust

Although many vendors offer services to companies seeking PCI compliance and auditing solutions, few providers match VeriSign’s expertise, intelligence-gathering capabilities, commitment to open standards, or role as trusted advisor. VeriSign leverages regulatory knowledge, training, and experience; best-of-breed solutions; a global network of proven technology; and its history of stability and trust to deliver solutions that are not only effective, but also make the best use of existing in-house personnel, technology, and processes.

The VeriSign suite of PCI compliance solutions includes VeriSign® Global Security Consulting, VeriSign® Managed Security Services, and VeriSign® Unified Authentication.

VeriSign® Global Security Consulting

The VeriSign Global Security Consulting team offers a range of comprehensive, customized PCI compliance solutions that objectively match each requirement to the best possible solution for your company. In addition, the consulting team provides assessment, certification, and incident response services that help companies address specific areas of PCI compliance and best practice.

Annual PCI Audits

The VeriSign Global Security Consulting practice was one of the first providers of onsite assessments for both Visa and MasterCard and is a Qualified Data Security Company (QDSC). Since the program’s inception, VeriSign has conducted several hundred assessments of some of the largest merchants and service providers. Onsite audits consist of interviews of key personnel; review of policies, procedures, and other key documents; architecture review; vulnerability testing; and review of key device configuration. The result of this effort is a Report of Compliance, which articulates the company’s adherence to the PCI Data Security Standard.

**Application Best Practice Certification**

Although currently not a PCI requirement, Visa and MasterCard encourage application development companies to certify their payment applications in accordance with the PCI Payment Application Best Practices program. Applications that meet these standards can be listed on the Visa Web site as PCI-approved payment applications. VeriSign is an approved assessor under this program and conducted some of the program's first application certifications.

Incident Response and Forensics

Even with a strong security architecture, incidents may occur. If so, a company may call on VeriSign's forensic personnel. VeriSign is an approved vendor under Visa's Compromise Entity Program and has investigated many of the large-scale incidents that have occurred over the past several years. VeriSign personnel are trained as computer forensic examiners and several have worked with law enforcement officials during credit card investigations. Should a company experience a compromise, VeriSign not only assists with the investigation and root cause analysis, but also can help remediate vulnerabilities and work with you to re-establish PCI compliance.

VeriSign® Managed Security Services

VeriSign offers several Managed Security Services (MSS) that help customers meet several requirements of the PCI Data Security Standard. While VeriSign® PCI Scanning Services help customers meet a core verification requirement, other services help reduce the cost and complexity of meeting the PCI Data Security Standard.

PCI Scanning and Testing Services

The PCI Data Security Standard has broadened the requirements for ongoing quarterly scanning. Scanning requirements that previously applied to network and operating systems have been expanded to include any externally facing e-commerce application. Application-level threats are highly sophisticated and typically cannot be identified by automated means alone.

VeriSign® PCI Quarterly Scanning Services (offered at either a Basic or Enhanced level) are delivered through the VeriSign® Vulnerability Management Service team. Manual testing by experienced professionals is combined with automated technology to help identify the breadth and depth of vulnerabilities. The result is a detailed report of vulnerabilities and recommendations along with the statement of compliance that is required by the PCI and the acquiring banks. Most important, this is not simply an automated scanning service. The VeriSign team communicates regularly with you to discuss findings and recommendations for further improvement, and to keep you up to date on the latest vulnerabilities and threats.

VeriSign® Firewall Management Service

To help you address PCI Data Security Standard requirement 1 to install and maintain a working firewall, VeriSign offers a complete firewall monitoring and management service. This service includes upgrades, configuration management, rule-set changes, and health monitoring. VeriSign also monitors firewalls for anomalous port activity that may indicate an attack in progress. Reports and statistics are available via the secure VeriSign Enterprise Security Portal. In short, VeriSign can manage your firewalls cost effectively while you focus on your core business.

**VeriSign® Intrusion Detection Management and VeriSign® Intrusion Prevention Management Service**

PCI Data Security Standard requirement 11.4 requires that companies “use network intrusion detection systems, host-based intrusion detection systems, and/or intrusion prevention systems to monitor all network traffic and alert personnel to suspected compromises.” VeriSign offers an open-source (i.e., Snort™) network intrusion detection installation for companies seeking to minimize capital investment. VeriSign handles signature updates and configuration management, and alerts you only to critical events that may threaten your infrastructure. You can view all events and reports through the secure Enterprise Security Portal.

VeriSign® Log Monitoring Service

PCI Data Security Standard requirement 10.2 requires the implementation of automated audit trails. To help address this requirement, VeriSign offers its Log Monitoring Service. This managed service securely collects logs from most platforms and monitors for events, alerting you only when critical events arise. Customers can access logs and reports via the secure Enterprise Security Portal.

VeriSign® iDefense Security Intelligence Services

Threats to companies that handle and process credit cards are becoming increasingly complex. To defend itself appropriately, a company must know what the latest and greatest threats are in the wild. VeriSign iDefense Security Intelligence Services help companies proactively protect critical data and infrastructure from attacks by delivering comprehensive, actionable intelligence regarding network-based security threats and vulnerabilities. VeriSign’s experienced team of security experts diligently search the Internet for potential cyber threats including new malicious code, zero-day exploits, and hacker groups committing or threatening cyber crime. The team combines its findings with technical and traditional intelligence to deliver advanced warning and analysis of these threats, allowing your organization to protect critical infrastructure.

VeriSign® Unified Authentication Services

PCI Data Security Standard requirement 8.3 requires companies to “implement 2-factor authentication for remote access to the network by employees, administrators, and third parties, [and] use technologies such as RADIUS or TACACS with tokens, or VPN with individual certificates.” VeriSign is a leading provider of strong (two-factor) authentication. Digital certificates and public key infrastructure (PKI) were the first managed services provided by VeriSign, which now provides best-of-breed two-factor authentication solutions via VeriSign Unified Authentication Services. Whether your company needs one-time passwords, smart cards, or traditional PKI, VeriSign can help meet requirements cost effectively—and without deploying additional infrastructure. VeriSign leverages your existing architecture (e.g., Windows® Active Directory® or Lightweight Directory Access Protocol (LDAP)) and can also provide “in-the-cloud” authentication if required. Strong authentication is not just good practice for remote users. Merchants and service providers should also consider implementing this capability internally to protect access to sensitive data.



+ Summary

VeriSign has a complete suite of services for the Payment Card Industry—from assessment services that help validate compliance, to a comprehensive suite of Managed Security Services and Unified Authentication services that help you meet various parts of the PCI Data Security Standard. With VeriSign as your strategic partner, you can rapidly implement cost-effective compliance and auditing mechanisms that allow you to return focus to your core business.

+ Learn More

For more information about VeriSign® PCI Compliance Solutions, please call 650-426-5310 or email enterprise_security@verisign.com.

For more information about the VeriSign® Security Certification Program, please see <http://www.verisign.com/products-services/security-services/securityconsulting/services/security-certification-program/index.html>

+ About VeriSign

VeriSign, Inc. (Nasdaq: VRSN) operates intelligent infrastructure services that enable and protect billions of interactions everyday across the world's voice and data networks. Additional news and information about the company is available at www.verisign.com.

+ PCI Data Security Standard and Related Information

For more information for merchants, including the current transaction volumes/categories for each level, please see http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html?it=il/business/accepting_visa/ops_risk_management/cisp.html|Merchants

For more information for service providers, including the current transaction volumes/categories for each level, please see http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_service_providers.html?it=il/business/accepting_visa/ops_risk_management/cisp.html|Service%20Providers

For the full text of the Data Security Standard, please see http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_merchants.html

To review the standards for the PCI Payment Application Best Practices program, please see http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp_payment_applications.html

To review the Security Scanning Requirements for Vendors, please see https://sdp.mastercardintl.com/pdf/srv_entire_manual.pdf

Visit us at www.Verisign.com for more information.

©2006 VeriSign, Inc. All rights reserved. VeriSign, the VeriSign logo, "Where it all comes together," and other trademarks, service marks, and designs are registered or unregistered trademarks of VeriSign and its subsidiaries in the United States and in foreign countries. Windows and Active Directory are trademarks of Microsoft Corporation. Snort is a trademark of Sourcefire, Inc. All other trademarks are the properties of their respective owners.

00021331 05-25-06