

TippingPoint PCI-DSS Compliance Solution Brief

IPS-Secured Networks

SOLUTION BRIEF – PCI Compliance



Major retailers are experiencing unauthorized intrusions into their computer systems that process and store customer transaction information. This has resulted in the theft of millions of credit card numbers and other sensitive customer data. In addition, they must adhere to legislation specifying guidelines for the protection of networks and critical data against malicious threats. This growing burden of responsibility requires CIOs/CSOs and IT administrators to rethink their network security priorities or risk compromised data integrity, financial loss and potential criminal implications.

"We constantly struggled with inspecting traffic across all of our locations and protecting critical data centers. With TippingPoint's stability and high performance, we were able to cover critical network areas that were previously unprotected. Knowing that we can manage multiple TippingPoint devices centrally, we can now easily deploy more devices at key traffic aggregation points."

Large U.S. Retailer

"After evaluating several alternatives, we chose the TippingPoint IPS because it met our requirements for stability, performance and threat coverage. TippingPoint was part of our concerted internal PCI-DSS readiness initiative which enabled us to pass our PCI-DSS audit with flying colors."

Large U.S. Grocery Store Chain

TippingPoint Customer Base

- 3,500+ worldwide customers
- 10,000+ in-line IPS deployments
- 300+ Fortune 1000 customers

What Are Some of the Security Challenges facing the Payment Card Industry?

High Volume of Credit Card Transactions

As the volume of online and standard credit card transactions continues to grow, merchants, banks and service providers are collecting and storing more and more sensitive information. This presents an attractive target to would-be hackers and criminal organizations who continue to develop new attacks specifically targeting credit card data, and they do so not for notoriety, but to profit from the exploitation of credit card accounts.

Targeted Attacks and Financial Fraud

The 2007 Computer Security Institute (CSI) Report indicates that more than one fifth of those surveyed have been victimized by a targeted attack¹. The study also concluded that financial fraud overtook virus attacks for the first time in seven years as the number one cause of financial losses from an IT security breach. Finally, customer and proprietary information was the second worst cause of financial loss. These trends show that the payment card industry faces more data security threats than ever before. The Payment Card Industry Data Security Standard (PCI-DSS) was created to mitigate these threats.

What is PCI-DSS (Payment Card Industry Data Security Standard)?

- An information security standard required of all banks, merchants and service providers that store, process, or transmit cardholder data
- Created by American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International to safeguard consumer information, reduce financial fraud

and identity theft, and protect the reputation of the payment card industry

- Participants are required to comply with six key areas of PCI:
 1. Build and Maintain a Secure Network
 2. Protect Cardholder Data
 3. Maintain a Vulnerability Management Program
 4. Implement Strong Access Control Measures
 5. Regularly Monitor and Test Networks
 6. Maintain an Information Security Policy

Why is PCI-DSS Important?

- Failure to comply with PCI-DSS may result in fines of up to \$500,000, increases in fees per card transaction, or loss of credit card payment privileges altogether
- Fines for September 2007: \$5,000 per non-compliant merchant
- Fines for December 2007: \$25,000 per non-compliant merchant
- In addition to fines, non-compliance can result in a loss of tier status and an increase in per-transaction interchange rates, which for most organizations will have a greater monetary impact than the fines

Banks, merchants and processors are increasingly the target of malicious attacks: TJX Companies Inc. suffered a security breach resulting in compromise of over 40 million credit card accounts². Some estimates place the cost of this breach at \$1.6 billion³.

What are the challenges to becoming PCI-DSS compliant?

- Limited budgets and staff to implement and maintain a compliant network

TippingPoint®

TippingPoint PCI-DSS Compliance Solution Brief

- Traditional technologies such as firewalls and Intrusion Detection Systems (IDS) require higher staffing levels and lack in-line enforcement functions and performance to effectively protect against today's threats

What is the TippingPoint Solution?

The TippingPoint Intrusion Prevention System is purpose-built for in-line network protection and is specifically designed to deliver network security enforcement with:

- High availability
- Multi-gigabit throughput including 10Gbps solutions with the TippingPoint Core Controller
- Switch-like latency and support for millions of sessions
- Filter accuracy (no false positives)
- Broad filter coverage
 - Vulnerability, exploit and anomaly-based filters
- Timeliness of filter coverage
- Low-touch central management system (manage with current staff)

Filter accuracy, coverage and timeliness are made possible by the world-renowned DV Labs security research team.

The TippingPoint IPS also provides multiple enforcement functions:

- Blocks malicious traffic flows
- Quarantines non-compliant hosts
- Rate limits non-critical traffic
- Alerts staff of key events
- Redirects designated traffic
- Allows clean traffic to pass unimpeded

The function of the product is based on a simple concept: bad traffic goes in; only good traffic comes out. This provides real-time automatic protection for applications, operating systems, clients, servers, VoIP infrastructure, routers, switches and other assets.

The TippingPoint solution protects networks at the WAN perimeter and inside the network;

providing protection of critical Web infrastructure in the DMZ and key assets in the data center. TippingPoint provides security isolation in the core and for key network zones at the aggregation and access layers. By enabling strong protection between network zones, organizations can mitigate the propagation of threats within the network.

In addition, TippingPoint provides a Network Access Control (NAC) solution that enables organizations to classify users and devices on the network and to enforce network security policy based on this classification.

What areas of the PCI-DSS are addressed by the TippingPoint solution?

Build and Maintain a Secure Network / Protect Card Holder Data

- Comprehensive threat protection – above and beyond firewall capabilities
 - Total packet inspection through Layer 7 with low latency
 - Continually eliminates malicious traffic before damage occurs
 - No false positives contributes to low-touch management
- Attacks covered include: targeted server attacks, blended attacks, worms, viruses, Trojans, phishing, spyware and others
- Secure management protocols and traffic enforcement
- TippingPoint NAC compliance posture checks verify status of client-based protection tools such as client firewall and anti-virus software

Maintain a Vulnerability Management Program

- Provides Web, database and other application protections
 - Specific application vulnerability filters including Oracle, SQL, MySQL
 - Custom filter feature enables organizations to tailor filters to meet their custom applications
- Digital Vaccine protection is complimentary to existing client Anti-virus (AV)
 - Removes need for emergency and ad-hoc patching of AV

- TippingPoint's IPS protects infrastructure components from targeted attacks including:
 - Web and database applications
 - VoIP infrastructure
 - Routers
 - Switches
 - Application and DNS Servers
- Application filters specific to database and other application-specific threats, including:
 - SQL Injection attacks
 - Cross Site Scripting attacks
 - PHP program access and code injection
 - Denial of service attempts
 - Modified parameters in a URL request
 - Malicious code injection into Web application requests
 - Tampering with Web application forms
 - Cookie Hijacking within Web application
 - Brute force or dictionary password attacks
 - Data theft, anti-crawl and others

Implement Strong Access Control Measures

- TippingPoint NAC provides role-based user access coupled with detailed reporting and auditing
 - This includes the ability to classify users based on AD, LDAP, Radius...
- TippingPoint NAC provides granular user, device classification and strong access enforcement via IPS enforcement, an in-line NAC appliance, or 802.1X

How TippingPoint Can Help

Over 3,500 TippingPoint customers are already securing their networks with an in-line TippingPoint IPS, and passing their PCI-DSS audits with flying colors because of its automated in-line policy enforcement. Learn how our customers are protecting their networks with TippingPoint by visiting www.tippingpoint.com, or call TippingPoint directly to speak to a representative about our IPS evaluation program at (888) 878-3477.

¹ Richardson, Robert. "2007 CSI Computer Crime and Security Survey." October 2007 Computer Security Institute. http://www.gocsi.com/forms/csi_survey.jhtml

² Brenner, Bill. "PCI DSS Auditors See Lessons in TJX Data Breach." 01 March 2007. [SearchSecurity.com](http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci124572700.html). http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci124572700.html

³ Hack, Martin. "Inside Job? TJX Cost of Breach Estimated at \$1.6 Billion." 12 April 2007. [Hack Report](http://hackreport.net/2007/04/12/inside-job-tjx-cost-of-breach-estimated-at-16-billion/). <http://hackreport.net/2007/04/12/inside-job-tjx-cost-of-breach-estimated-at-16-billion/>

Corporate Headquarters:
7501B North Capital of Texas Hwy.
Austin, Texas 78731 USA
+1 512 681 8000
+1 888 TRUE IPS

European Headquarters:
Herengracht 466, 2nd Floor
1017 CA Amsterdam
The Netherlands
+31 20 521 0450

Asia Pacific Headquarters:
30, Cecil Street, #18-01
Prudential Tower
Singapore 049712
+65 6213 5999

TippingPoint®

www.tippingpoint.com