

SOLUTION BRIEF

CONFIDENTIAL

PAYMENT CARD INDUSTRY (PCI) COMPLIANCE

**Top
Layer™**

perfecting the art of network security

Payment Card Industry (PCI) Data Security Standard and the Evolving Need for Intrusion Prevention System (IPS) Solutions



I. Introduction

On June 22, 2005, Jonathon Krim of The Washington Post called 2005 “the year of the data breach”, a phrase that, since then, has become common parlance for those observing the state of the fraud/security marketplace¹. 2005 saw high-profile breaches at payment processors, banks, retailers, and data brokers, breaches that compromised social security card numbers, credit card data, account numbers, and other important personal/financial data, of tens of millions of US citizens. In fact, as of January 18, 2006, Privacy Rights Clearinghouse estimates the number of people affected since February 15, 2005, calculated from public announcements, at over 52M².

One of the largest breaches so far, which occurred at CardSystems Solutions on June 16, 2005, a third-party processor of payment card data, compromised the data of 40M holders of credit cards of all types when CardSystems was hit by a computer virus that captured customer data for the express purpose of committing financial fraud. Congressional hearings on the matter were held in July, and Visa, MasterCard, American Express, and other payment card providers ceased allowing CardSystems to process payments³.

The CardSystems incident, combined with other significant data thefts from top enterprises such as TJX, ChoicePoint, DSW Shoe Warehouse, Polo Ralph Lauren, Bank of America, LexisNexis, Wachovia, and Sam’s Club, have made data security a top-of-mind issue for anyone handling sensitive consumer information, and have made calls for additional legislation more widespread and insistent.

Well before these events and subsequent calls for legislation occurred, all of the major credit card issuers had created detailed security programs in an effort to combat data theft and better ensure the protection of cardholder data.

Following are several of these programs:

- American Express Data Security Operating Policy (DSOP)
- Discover Information Security and Compliance (DISC) Program
- MasterCard Site Data Protection (SDP) Program
- Visa International Account Information Security (AIS) Program
- Visa USA Cardholder Information Security Program (CISP)

¹ “Ubiquitous Technology, Bad Practices Drive Up Data Theft,” Washington Post, June 22 2005.

² <http://www.privacyrights.org/ar/ChronDataBreaches.htm>

³ Litan, Avivah. “Congressional Hearing on CardSystems Exposes PCI Shortcomings,” Gartner, August 3, 2005.

II. Understanding the PCI Data Security Standard

In December 2004, Visa, MasterCard, American Express, Diner's Club, JCB and Discover joined together to merge their programs and develop the PCI (Payment Card Industry) DSS (Data Security Standard). **Compliance is mandatory for any business – including merchants, service providers, and issuing banks – that handle, store, transmit, or process any data related to the card companies. The program's purpose is to protect cardholder private information, decrease fraud, and spot security issues that could result in compromised or stolen data.**

PCI comprises twelve individual compliance requirements, each of which includes several sub-requirements, organized around six primary goal categories. These categories include the following:

- Build and maintain a secure network
- Protect cardholder data
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy

The individual requirements are listed below:

Rule 1: Install and maintain a firewall configuration to protect data

Rule 2: Do not use vendor-supplied defaults for passwords and other security

Rule 3: Protect stored data

Rule 4: Encrypt transmission of cardholder data and sensitive information across public networks

Rule 5: Use and regularly update anti-virus software

Rule 6: Develop and maintain secure systems and applications

Rule 7: Restrict access to data by business need-to-know

Rule 8: Assign a unique ID to each person with computer access

Rule 9: Restrict physical access to cardholder data

Rule 10: Track and monitor all access to network resources and cardholder data

Rule 11: Regularly test security systems and processes

Rule 12: Maintain a policy that addresses information security

PCI also contains ongoing validation requirements for merchants, enumerated here:

1. An on-site security audit
2. A self assessment questionnaire
3. A network scan

Specific requirements as to frequency and level of validation required depends upon the "Level" rating assigned to the merchant, based upon risk and transaction or account volume.

Under PCI, there is a web of responsibility that banks and merchants share. One Top Layer customer, for example, has its Web presence hosted by a third party. The Visa/MasterCard member bank, which is ultimately responsible for its merchants' compliance with PCI, is now responsible for PCI compliance at the Web hoster. The member bank has no relationship with the hoster, so it must rely upon the merchant to assure the compliance of the hosting vendor.

III. Why Comply?

All of this may sound oppressively difficult and expensive, but it is necessary. The risks of not complying with PCI requirements are considerable, and include aggressive defined financial penalties for non-compliant organizations. If a financial institution, service provider, or merchant is found non-compliant in the event of a breach, significant fines may accrue. Under the worst possible scenario, failure to meet PCI can end in suspension, and finally revocation, of an organization's right to accept or process credit card transactions, making it extremely challenging to continue doing business.

Soft costs, which can include tarnished reputation; lost market cap for public companies; desertion due to loss of trust by current and potential customers and partners; devalued brand; and other significant financial losses due to lost revenue, remediation expense, and liability lawsuits requiring reparations to injured parties. One Top Layer customer, a PCI "Tier One" merchant, states that "the lasting brand damage and associated damage to the business of allowing a successful data theft exponentially exceeds mere fines which, even at the mandated maximum, are limited."

Business organizations have the fundamental goal of gaining and maintaining customers' trust across all channels, from retail locations to telephone transactions to catalogs to the Internet. Users must have confidence in the overall reliability and confidentiality of private information in order to participate with a particular vendor. Customers, partners, and stakeholders are increasingly demanding a higher degree of accountability for security.

By complying with PCI requirements, merchants and service providers meet their obligations to the security programs of the six major credit card companies. In addition, meeting PCI requirements can help build a foundation to meet standards set by legal regulations such as the California Information Practices Act and Gramm-Leach-Bliley, as well as pending and future legislation, such as the Identity Theft Protection Act.

Security leaders at merchants can also use PCI compliance as a lever to enable the building of a sound security strategy. Management, when faced with potential significant fines, crippling negative publicity, and angry customers, will more likely listen to security proposals couched in terms of PCI.

Countering cyber-threats represents a central strategic issue for regulatory compliance, business development, revenue increase, and, where applicable, maintaining shareholder value.

IV. Why Network Intrusion Prevention Systems (IPS)?

When one examines the components of PCI, one finds an explicit requirement for network IPS in one place, subsection 11.4, which falls under Rule 11: Regularly test security systems and processes. It follows:

11.4. 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. Keep all intrusion detection and prevention engines up to date.

For strict compliance purposes, then, companies can fill the checkbox in a number of ways. If IDS or IPS tools are in place and maintained for monitoring purposes, the PCI contractual obligation is fulfilled. As one large high-end fashion retailer and Top Layer customer states, "One checkbox is IDS/IPS. IDS only detects problems without preventing them. There is nothing even implicit around what kind of bad traffic to look for, how to report intrusions, or what to do about them once they are detected. IPS offers the best protection."

Leading IPS solutions not only detect and provide forensics for all the bad traffic that attacks and traverses an organization's network; they stop it, providing a record of the events, without stopping an unacceptable amount of good traffic. A top-notch IPS solution can stop attacks in their tracks. This decreases the need both for scarce security staff to chase after attacks by wading through stacks of paper detailing events, and for the business to repair the damage successful data thievery wreaks. IPS is a must-have for PCI-affected business that wants to comply cost-effectively while mitigating against fallout from attacks that are detected but not prevented.

V. Why Deploy a Top Layer IPS for PCI Compliance?

"PCI data security guidelines stipulate stringent levels of security and requisite technology implementations to achieve compliance. Because we want our customers to feel absolutely safe doing business through all channels – mail, telephone, Internet – we deploy best-of-breed technology across our company to protect our policyholders. Top Layer Networks, with its unparalleled approach to protection, allows us to exceed PCI security requirements – blocking malicious attacks and potential fraudsters from accessing customer data and causing damage -- and go the extra mile that our customers deserve."

- CIO, Retail Insurance Provider

Top Layer Networks' IPS 5500 Intrusion Prevention System provides member banks, payment processors and merchants with the ability to comply with the letter of the specific PCI requirement, while helping them to reinforce other goals of the PCI program, such as "build and maintain a secure network", "protect cardholder data", "implement strong access control measures", and "regularly monitor and test networks". In addition, Top Layer Network's IPS Centralized Management Solution provides the reporting and logging capabilities for organizations to prove that PCI requirements and company security policies are being correctly followed.

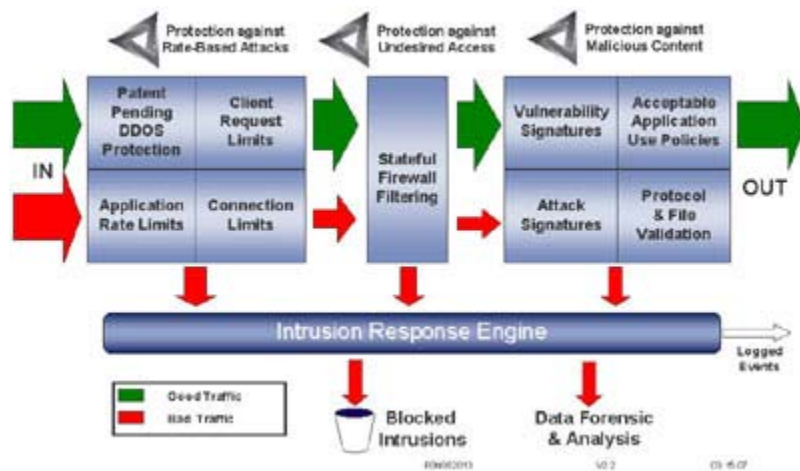
In order to support the stated goals of PCI and the overarching goals of the business, an organization should deploy solutions, like Top Layer's, that will proactively address important IT security concerns, such as the following:

- Undesired access to financial and confidential records
- Malicious content that may alter, damage, or contribute to theft of sensitive information
- Rate-based attacks that can render critical resources and information vulnerable

A. Three Dimensional Protection (3DP) - How The IPS 5500 Ensures Confidentiality and Privacy of Sensitive Data

In order to best combat the threats to sensitive data posed by undesired access, malicious content, and rate-based attacks (and complex hybrid attacks that use multiple elements of these to circumvent static, one-dimensional security tools), enterprises should select and deploy a network IPS solution that addresses all three in an integrated, mutually-reinforcing fashion – as Top Layer Networks does with its "Three Dimensional Protection" approach.

Figure 1: Top Layer Networks' 3DP Architecture



1) Protecting Against Undesired Access with Stateful Firewall Technology

In the first area of defense, Top Layer addresses the potential for undesired network and application access by adopting a stateful firewall stance. In the IPS 5500, Top Layer provides IP fragment abuse protection, Layer 2 and Layer 3 filtering, and stateful firewall filtering. Administrators can easily configure the IPS 5500's firewall filters to control who gets access to which servers and applications connected to the network, thereby preventing a malicious user from gaining entry to steal sensitive data. Top Layer's stateful firewall approach separates it from IPS competitors, who do not have this level of protection from undesired access throughout a network available.

2) Stopping Malicious Content

Top Layer protects against malicious content with a multi-pronged approach: Acceptable application use policies, protocol validation, attack/vulnerability signatures, antivirus signatures, and spyware protection modules. Top Layer stops traffic that does not conform to an enterprise's application use rule set, which is easily configurable Network transactions that pass through this initial gate are then sent through a protocol anomaly detection engine to determine whether the packets meet standard protocol implementations, an approach that defines what is good, allowable traffic.

Because the IPS 5500 maintains more state, or context, than other IPS devices, it is better able to eliminate false positives by drawing more complex conclusions and detecting more subtle anomalies. Transactions that do not meet the acceptable protocol specifications (such as those containing buffer overflow attacks) are blocked and sent to a sophisticated identification and reporting engine for real-time reporting.

However, although this provides a powerful technique to detect and block many attacks, there are attacks that exhibit themselves as perfectly legitimate network traffic (such as some viruses, application logic attacks and reconnaissance methods). It is therefore important that seemingly legitimate traffic is subject to other protection mechanisms.

Packets that contain a file that may carry a malicious payload, such as a ZIP, JPEG, XML, or Microsoft Excel or Word files, are sent for further analysis of the body of the payload and matched against known exploits through attack signature pattern matching. This deep packet inspection and signature matching is performed without materially affecting network performance.

3) Denying Distributed Denial of Service (DDoS) and other Rate-Based Attacks

With the IPS 5500 and its patent-pending algorithms, Top Layer Networks builds upon its industry leadership position in protecting against network- and application-level flood attacks and other attacks using inappropriate rates. The IPS 5500 does so by applying DoS/DDoS mitigation techniques, policy-based rate limits, and other resource-consumption limits.

The IPS 5500 uses purpose-built flexible programmable hardware to maximize good, or legitimate, network transactions (by blocking rate-based attacks) and maintain a real-time threat-level assessment of 2 million IP addresses (increasing to 5 million when an attack is detected). In addition, it provides advanced contextual information about traffic flowing through the device and distinguishes legitimate traffic from seemingly legitimate DDoS attack traffic. The IPS 5500 is a purpose-built hardware platform, employing multiple high-performance ASICs and highly programmable FPGA. The system is optimized to be inline and keep sensitive data and mission critical systems safe from malicious activities.

Conclusion

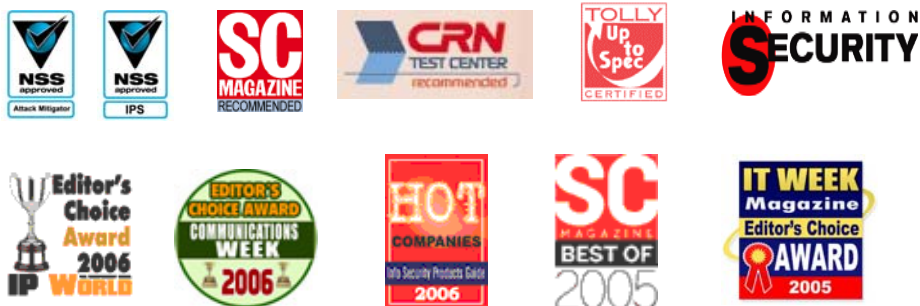
Considering the for-profit attackers who continue to make headlines stealing customer data and using it to generate revenue, today's PCI-affected enterprises must further enable fast and efficient access to account information and processing of financial transaction. They must also provide foolproof mechanisms for ensuring customer data security, maintaining good customer relations while staying out of the headlines.

Top Layer Networks has the best IPS solution for offering three-dimensional protection from undesired access, malicious content and rate-based attacks that target mission-critical servers and networks.

Top Layer's IPS 5500 does more than just "check a checkbox" – it provides enterprises that value their customers the peace of mind that comes with doing the right thing, not merely meeting a minimal compliance requirement. At the same time, it allows organizations to focus high value security resources on value-creating initiatives, not mere data correlation and attack remediation.

To find out more about how the IPS 5500 can help your business exceed PCI guidelines while securing your infrastructure against attacks in three dimensions, call Top Layer's sales at 508-870-1300.

The IPS 5500 has won the most awards:



Top Layer Networks, 2400 Computer Drive, Westborough, MA 01581

Phone: 508-870-1300, Fax: 508-870-9797, <http://www.TopLayer.com/>