

---

# PCI DSS FUNCTIONALITY IN PRODUCTS

## THE VALUE OF INDEPENDENT PRODUCT VALIDATION

By Rick Moy, President

September, 2008

### *Contents*

<b>INTRODUCTION.....</b>	<b>2</b>
<b>COMPLIANCE QUESTIONS .....</b>	<b>2</b>
<b>INADEQUATE RESOURCES .....</b>	<b>3</b>
<b>PCI SUITABILITY REPORTS.....</b>	<b>5</b>
<b>APPLICABLE PRODUCT CATEGORIES.....</b>	<b>6</b>
<b>KEEPING UP-TO-DATE .....</b>	<b>7</b>
<b>INDUSTRY BENEFITS.....</b>	<b>7</b>
<b>CONCLUSION .....</b>	<b>7</b>
<b>ABOUT NSS LABS.....</b>	<b>9</b>
<b>ABOUT RICK MOY .....</b>	<b>9</b>

### *Summary*

The payment card industry has made great strides in security through the introduction of the PCI Data Security Standard (PCI DSS), which prescribes requirements for cardholder network architectures, policies & procedures, and even products. As a natural result, a number of clarifying questions surrounding products continue to arise, e.g. which products are required, when and where, and how should they be configured? Independent product validation of PCI DSS functionality offers much needed clarity and insight to assessors, banks, merchants and service providers. Such a standardized, independent certification process enables vendors to communicate product features more effectively and credibly to the payment card industry.

## INTRODUCTION

The payment card industry is driving merchants, banks and service providers to comply with the PCI Data Security Standard (PCI DSS). DSS specifies requirements for cardholder network architectures, policies & procedures, and even products. In preparing for a yearly assessment, merchants, banks and service providers must demonstrate compliance with all three aspects of their cardholder data network.

Despite PCI DSS being one of the most practical and prescriptive sets of regulatory requirements to date, many questions still remain for implementers and assessors alike. It is impossible to prescribe the perfectly compliant network for such a broad range of industries, technologies and business practices. Not surprisingly, the market place needs clarification when it comes to products and their configuration. This paper outlines how independent product evaluations for products used in cardholder data networks can solve this problem.

## COMPLIANCE QUESTIONS

Most organizations have co-existing security and compliance objectives. Moreover, many are faced with integrating new (and potentially multiple) compliance requirements with these existing security objectives. In many cases requirements such as DSS are helping to support security programs that couldn't otherwise get internal funding. On the other hand, some compliance requirements can be seen as unwelcome burdens.

Achieving validation of compliance is a process that involves analysis, research, testing, deployment and ongoing maintenance of products, practices and services. In building secure and compliant networks, merchants design network architectures, for which they buy, configure and deploy a wide range of security products; such as, firewalls, encryption, intrusion detection & prevention, vulnerability scanners, anti-malware, application security, wireless, etc.

This process requires significant research to determine which class of products is required or appropriate for a given environment; what is called for in the DSS? how should the products be configured; which vendor products and models are best suited for the task? Are my current products adequate? And are they configured properly?

Example:

*Does a UTM belong on the perimeter, in a level 4 retail storefront? Is WiFi acceptable? Where, and under what conditions? Is WEP permissible? Instead of a code review can an application firewall be deployed? Host or network? What threats beyond the OWASP top 10 should be mitigated? Which products go beyond the 'musts' to the 'shoulds'? Is an older version acceptable, or is an upgrade required?*

Merchants and assessors are currently lacking clear guidelines and standards for products. Information security professionals trying to comply with PCI need to architect a solution that meets the explicit and implicit requirements of the PCI DSS. These implied requirements can often align well with an organization's existing best practices security objectives. Thus, buyers must 'fill in the blanks' with their own interpretation of the requirements and best practices security guidelines in order to make product-level decisions.

How do you know what makes a good product? The complexity of today's products makes it difficult for information security professionals to cut through the marketing clutter and empirically evaluate the products before buying or deploying.<sup>1</sup> Few practitioners have the necessary breadth of knowledge of products, individual configurations, performance ratings, and security coverage effectiveness. Indeed, our research indicates that many vendors are struggling to accurately determine their product's effectiveness and performance capabilities in their own labs.

## INADEQUATE RESOURCES

Buyers need help. Where can they turn? QSAs, consultants, and ultimately the security standards council's technical working group. However, with over 6 million merchants and merely 1,000 Qualified Data Security Professionals (QDSPs), the 'consulting' model cannot scale quickly enough to meet the needs of either party. And quality and consistency issues are being addressed with a QA program.<sup>2</sup> However, when it comes to product suitability, there are simply too many products for QSAs to learn to do an effective job – unaided.

Without a 'physician's desk reference' for security products, IT managers and assessors are compelled to make individual determinations on an ad-

---

<sup>1</sup> See the NSS Labs white paper: Product Testing Challenges for Enterprise Security Organizations

<sup>2</sup> At the PCI community meeting in September 2007, quality and consistency of assessments was a key topic, and the PCI council made 'quality control' a top priority for 2008. At the 2008 community meeting, a QA program was launched.

hoc, case by case basis. This introduces the potential for inconsistent and inaccurate determinations. In extreme cases, a merchant can always contest a Report on Compliance (ROC) with the PCI Security Standards Council.

Product vendors are currently utilizing a variety of vehicles to communicate their products' capabilities. These include a variety of data sheets, awards, magazine reviews, white papers, case studies, and 3<sup>rd</sup> party certifications. These provide partial informational at best. In general, they are either too limited in scope and detail, or extremely biased.

- “Achieving PCI compliance with product X” type of white papers have become quite common, and can provide a rudimentary ‘mapping’ of product functionality to a set of DSS requirements. Such approaches are informative, but generally incomplete.
- Magazine product reviews are a double-edged sword; they can help form an initial opinion or short list, but are generally too superficial technically to be conclusive. Reviews vary in the level of subjectivity, and the financial model has typically meant that proper methodologies (and accurate results) fall prey to the expediency of advertising.
- Vendor collateral, whether product documentation, implementation guides, data sheets, web content or presentations, is usually not sufficiently technical to quickly and clearly answer an assessor’s implementation questions. In addition, it is not an impartial source.
- Existing product certifications are too limited and do not address the explicit and implicit requirements of the payment card industry. E.g. ICSA Labs, as well as FIPS 140 and Common Criteria.

Furthermore, and perhaps most importantly from a security effectiveness perspective, none of the existing product standards programs today account for appropriate usage – the notion that products are becoming specialized for applications in specific areas of the network. For example, some IPS products focus solely on protecting the datacenter, while others are optimized for client protection at the network perimeter. For more information on appropriate usage, refer to the NSS Labs white paper: *Evaluating Products based on appropriate usage*.

## PCI SUITABILITY REPORTS

Right now there is a need and an opportunity for a more informative and scalable approach. Individual product validation reports tailored to specific PCI DSS requirements offer much needed clarity and insight to assessors, banks, merchants and service providers. Such a standardized, independent validation process enables vendors to communicate product features more effectively and credibly to the payment card industry. NSS Labs and its partners and advisors have developed PCI Suitability Reports for PCI-related products in the payment card industry.

PCI Suitability Reports should be comprehensive and informative, not merely a rubber stamp. They should help buyers and assessors make informed decisions about real-world implementations. This means they cannot simply be a magazine-style 4.5 star award. Rather, implementers and assessors must truly understand the specific capabilities of a product for the intended use.

Thus, PCI Suitability Reports include an analysis of each of the following areas for a tested product:

**1. Fulfillment of specific PCI DSS v1.1 requirements, including logging, administration & reporting**

The PSS contains a product-centric organization of all of the DSS requirements.

**2. Recommended product configurations for PCI environments**

No product works out of the box as needed. PSS Certified product reports include detailed recommended configurations. E.g. specific settings for vendor X's UTM product in a retail storefront.

These components of the NSS Labs PCI Suitability reports represent the most pragmatic, in-depth product analysis available to date for evaluating support for PCI DSS compliance requirements. However, for additional and equally important information about product effectiveness, performance and manageability, NSS Labs recommends consulting its standard certification reports.

**1. Fulfillment of additional 'must' and 'should' criteria according to best practices & standards**

Criteria in these reports have security as the primary objective and in many cases surpass compliance requirements in levels of stringency.

## 2. Indication of *Appropriate Usage* based on environment

NSS Labs recognizes that products are increasingly designed for specialized deployment. Thus, our assessments classify threats into the following categories in order to estimate the likelihood of specific types of threats in different environments: Datacenter, Perimeter, ROBO/SOHO, e-commerce, SCADA.

## 3. Security Effectiveness (Threat Mitigation)

Protective ratings are measured in raw percentages of attacks that were stopped for each attack category: System, Service, Fault, Reconnaissance, Denial of Service (DoS).

## 4. Performance Profiling

The security functions of most products vary with different levels of throughput. Determining a product's effective security at a rated performance level is crucial to properly sizing a solution. NSS standard reports include accurate performance profiles for the products tested based on real-world application-layer traffic.

## 5. Product Stability against Attacks

Security products must be able to withstand attacks that designed to destabilize or compromise them. This section addresses a product's ability to withstand commonly available, custom and fuzzing attacks.

## APPLICABLE PRODUCT CATEGORIES

There are more than 30 different security product technologies that could be implemented in modern networks. It would be impossible for any single specification document to adequately cover all of these categories. Thus, Security Standards need to exist for each category of products. Below are just a few:

- Network Firewalls
- Host Firewalls
- Web Application Firewalls
- Unified Threat Management
- Wireless Security
- PKI/Encryption
- VPN (SSL & IPSec)
- Antimalware
- Network IPS
- Host IPS
- Network Access Control
- Vulnerability Scanning / Management
- Web App Vulnerability Scanning

## KEEPING UP-TO-DATE

The PCI DSS prescribes best practices for deployment and maintenance. Security products, such as antivirus and IDS/IPS, must be kept up-to-date to remain effective.

*Section 5: Use and regularly update anti-virus software or programs*

*Section 11.4: ... "Keep all intrusion detection and prevention engines up-to-date."*

NSS Labs' offers a security update monitoring service (SUM) that monitors a product's security effectiveness on a recurring monthly basis, more frequently than any other service in the world. Note: The SUM service is currently an active, private service with a number of leading security vendors' products.

## INDUSTRY BENEFITS

Every party involved in PCI compliance benefits from scientific analysis of security products against well-defined, published standards. Merchants, banks and service providers now have empirically-based tools and guidelines upon which to base critical decisions. Compliance and security objectives can be met in an expedient, cost-effective manner.

Assessors have more information with which to judge implementations. As a result, assessments will be faster, with fewer disagreements, and overall more cost effective. Because they are scientific, repeatable and independent, such product standards can be trusted.

Product Suitability reports help ensure vendor claims of PCI value are independently validated in an empirical, standardized fashion. For strong vendors, who assume a leadership position, this is a welcome opportunity to assist customers with a key business problem. Similarly, new entrants can gain credibility by avoiding the pitfalls of 'marketing fluff.'

## CONCLUSION

Payment card industry requirements are unique and will continue to evolve.<sup>3</sup> PCI Suitability Reports for network security products are a natural answer to this, and a natural evolution of the product evaluation model already widely accepted in the marketplace.

---

<sup>3</sup> PCI DSS 1.1 was introduced one year after v1.0. In December 2007, the PCI Security Standards Council announced intentions to make the Payment Application Best Practices (PABP) a standard (PA-DSS).

The PCI DSS Functionality Map and product configuration contents are exclusively unique to NSS Labs' PCI validation reports. This extra level of pragmatic detail will benefit both vendors and information security buyers, particularly in the proof of concept and product evaluation phases of the purchasing cycle.

The model for vendor product certification already exists for government and financial sector regulations. With its additional benefits and the rapid industry support, product suitability reports are quickly becoming the *lingua franca* between participants in the payment card industry.

## ABOUT NSS LABS

Founded in 1991, NSS Labs is the globally recognized leader in independent security & performance testing and certification. NSS Labs' comprehensive certifications already address a wide range of security products, including Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Secure Content Appliances (SCA), Content Monitoring and Filtering (CMF) and Data Leak Prevention (DLP) devices, Unified Threat Management (UTM) systems, firewalls, host malware protection, VPNs, Web Application firewalls, cryptographic devices and PKI products. NSS Labs also performs private testing.

NSS Labs has offices in Carlsbad, CA and Austin, TX. Our customers include almost every major security vendor across a broad range of categories. NSS Labs a participating organization in the PCI Security Standards Council.

## ABOUT RICK MOY

As president of NSS Labs, Rick Moy is responsible for all business and editorial aspects of the company's operations. He is a leading expert with over 15 years experience in the network security industry. His background spans software development, network administration, product management, business development, and sales & marketing for a variety of network security technologies, including intrusion prevention, anti-malware, content filtering and SIM. Rick is a noted speaker and has appeared in dozens of print, online and television media. Prior to joining NSS Labs, he served in a variety of key positions at leading technology upstarts, such as Websense, ESET, Protego Networks (Cisco), Preventsys (McAfee), Lucid Security (Trustwave), and HighTower. Rick holds a B.S. in Cognitive Science from UCSD and an MBA from SDSU.