

PCI DSS: Beating the Cardholder Data Blues

Using a Holistic Approach to Lower Total Cost of Ownership (TCO) by 50% or More

an eIQnetworks White Paper

by John Linkous
Security and Compliance Evangelist
eIQnetworks, Inc.



eIQnetworks
31 Nagog Park
Acton, MA 01720
t. +1 978.266.9933
f. +1 978.266.0004
www.eIQnetworks.com

© 2010, eIQnetworks, Inc. eIQnetworks, the eIQnetworks logo and SecureVue are registered trademarks of eIQnetworks, Inc. All other trademarks, servicemarks, registered trademarks or registered servicemarks are the property of their respective owners. All rights reserved.

Contents

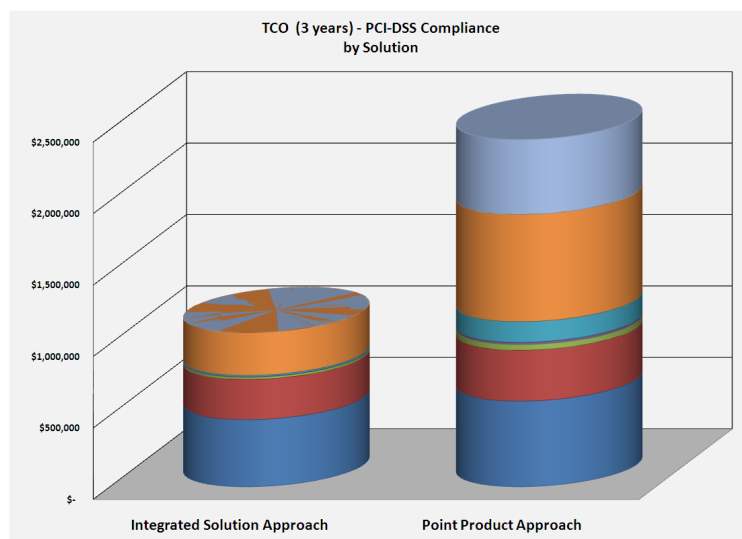
Abstract	3
The Business Problem	3
Meeting PCI DSS Audit Challenges	4
The Traditional Approach: Security Point Products	4
Product 1: SIEM and Log Management	5
Product 2: Configuration Auditing and Assessment	5
Product 3: Network Behavioral Analysis (NBA)	5
Product 4: File Integrity Monitoring (FIM)	5
Integrated Solution Approach: Unified Threat and Compliance (UTC)	6
Integrated Solution (SecureVue) Profile	6
Calculating Real TCO for PCI DSS Compliance	7
Assumptions	7
Product Procurement Costs	8
Annual Support and Maintenance Costs	9
Training Costs	10
Professional Services	10
Operations Personnel	11
Conclusion	12
Cost Comparison Table	12
Cost Comparison Charts	13
Appendix 'A': Detail of Security Data Type by PCI DSS Requirement	13

Abstract

As one of the most critical information security standards in use today, the PCI Data Security Standard (DSS) defines a comprehensive set of mandatory requirements that must be followed by every organization that stores or transmits credit or debit card data, including retailers of all sizes, payment processors, and financial institutions.

The traditional approach to PCI DSS compliance requires both technology-based tools to collect relevant PCI-related security data, as well as processes, oversight and management. While there is no such thing as fully-automated “turnkey” PCI DSS compliance, a large number of the PCI DSS requirements can be automated through security tools, reducing the amount of time required to manually address these requirements. Automating PCI DSS requires implementing key technologies that provide collection and analysis of PCI-related data, including log management (or SIEM), configuration auditing, vulnerability assessment, and network traffic analysis products. This traditional approach to PCI DSS compliance is usually adequate; **however, by taking a different approach based on a single, integrated platform that brings together all relevant PCI DSS technical data, the total cost of ownership for PCI DSS compliance can be reduced by 50% or more over a three-year period.**

In this white paper, eIQnetworks documents the true TCO associated with the traditional method of PCI DSS compliance, and compares this approach to one based on eIQnetworks’ SecureVue solution. Individual cost factors between both solutions are compared in a typical PCI DSS compliance scenario, and a comprehensive summary comparison identifies the real-world costs associated with both solutions.



Typical 3-Year PCI DSS Compliance Comparison Between Traditional Point Product Approach and Integrated Solution Approach

The Business Problem

The PCI DSS standard requires a combination of technology, people and processes, driven by proper governance. Under the rigorous standards defined by the PCI Security Standards Council (SSC) for Level 1 and Level 2 merchants, these organizations must address a broad set of data analysis, data retention and monitoring requirements by measuring, archiving, monitoring, analyzing, and reporting on a broad range of technical security data from across the PCI infrastructure, including asset data, configuration data, log and event data, known vulnerabilities, network flows, file integrity and removable media data, written security policies and manual procedures, and physical security audit results.

Table 1 identifies how each of these types of data map to individual requirements in the PCI DSS standard; for a detailed breakdown by PCI DSS requirement, see Appendix ‘A’ at the back of this document:

Requirement	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data	■	■	-	■	-	-	■	-
Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords	■	■	-	-	-	-	■	-
Requirement 3: Protect Stored Cardholder Data	■	■	■	-	-	■	■	■
Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks	■	■	■	■	■	-	-	-
Requirement 5: Use and Regularly Update Anti-Virus Software or Programs	■	■	-	■	-	■	-	-
Requirement 6: Develop and Maintain Secure Systems and Applications	■	■	■	■	■	■	■	-
Requirement 7: Restrict Access to Cardholder Data by Business Need to Know	■	■	■	■	-	■	■	-
Requirement 8: Assign a Unique ID to Each Person with Computer Access	■	■	■	■	-	-	■	-
Requirement 9: Restrict Physical Access to Cardholder Data	-	■	■	-	-	-	■	■
Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data	■	■	■	■	-	-	■	-
Requirement 11: Regularly Test Security Systems and Processes	■	■	-	■	■	■	■	-
Requirement 12: Maintain a Policy that Addresses Information Security for Employees	■	■	■	■	■	■	■	■

Table 1: Security Data Types Required Under PCI DSS 1.2

Meeting PCI DSS Audit Challenges

Merchants and other organizations that process, transmit or store cardholder data on their own infrastructure – especially those that are qualified as Level 1 or Level 2 under the PCI SSC categorization system – must implement technologies to collect and monitor the key types of information security data identified above. At a minimum, this includes four security functions:

- Security Information and Event Management
- Configuration Auditing
- Network Behavioral Analysis (NBA)
- File Integrity Monitoring (FIM)

Organizations that must address these security functions have adopted one of two approaches: a traditional point solution approach in which multiple security products are deployed, often as a “best of breed” set of tools; or, an integrated solution approach in which a multiple security functions are combined into a single platform. Below we provide an analysis of both methods.

The Traditional Approach: Security Point Products

In a traditional approach to PCI DSS compliance, organizations meet PCI audit challenges using point products address specific PCI DSS requirements, as illustrated in Figure 1, below:

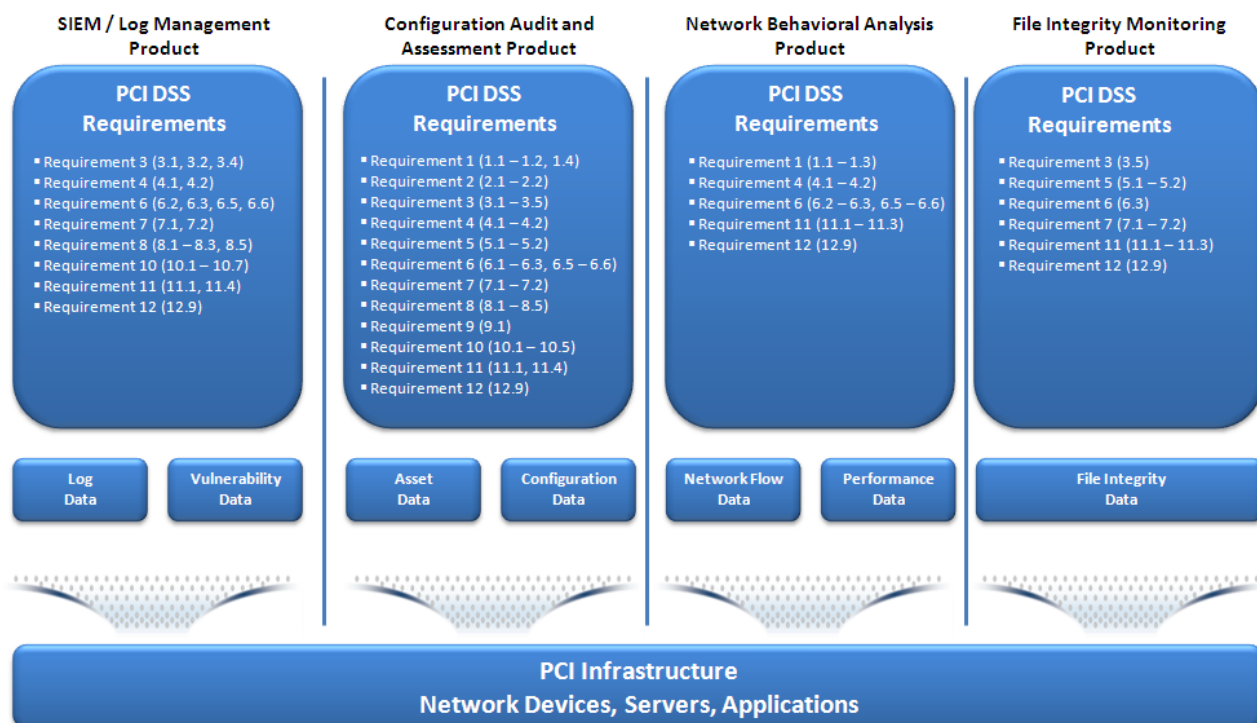


Figure 1: Traditional Approach to PCI DSS Compliance

Product 1: SIEM and Log Management

SIEM and log management solutions provide collection, aggregation, and analysis of log and event data from operating systems, network infrastructure devices, security devices, applications, and databases, as well as vulnerability data from third-party scanning products. Common tools that provide this point product functionality include: Arcsight ESM; Q1 Labs Radar; and RSA EnVision. These products fully address PCI DSS Requirement 10, and partially address PCI DSS Requirements 3-4, 6-9, and 11-12.

Product 2: Configuration Auditing and Assessment

Configuration auditing and assessment products provide the ability to audit secure configurations for systems and applications, and continuously monitor these systems to ensure compliance with these secure baselines. These point solutions capture both what's on a system (such as hardware profile, installed applications, and running services/daemons) as well as how securely these components are configured (such as device settings, password standards, and access control lists). Common tools that provide this point product functionality include: Symantec CCS (formerly BindView); NetIQ Security Manager; and Tripwire Enterprise. These products partially address PCI DSS Requirements 1-8, and 10-12.

Product 3: Network Behavioral Analysis (NBA)

NBA security point solutions collect network flow data generated by routers, firewalls, and other network infrastructure devices, analyze this data to determine "normal" traffic patterns, and alert system administrators when normal abnormal network traffic is detected. These products also provide metrics on network data, such as sources and destinations of traffic, as well as network protocols, ports, and applications. Common tools that provide this point product functionality include: Lancope Stealthwatch; and Q1 Labs QRadar. These products partially address PCI DSS Requirements 1, 4, 6, and 10.

Product 4: File Integrity Monitoring (FIM)

FIM products continuously monitor critical files – such as operating system files, files containing sensitive data, and others – using checksum-based data, and immediately notify appropriate personnel when unauthorized or unexpected changes to files and directories occur. Common tools that provide this point product functionality include: TripWire Enterprise; Symantec CCS; and nCircle FIM. These products partially address PCI Requirements 3, 5, 6, 7, and 11.

Integrated Solution Approach: Unified Threat and Compliance (UTC)

An alternative approach to PCI DSS compliance provides the same comprehensive coverage of all security data and capabilities (such as alerting and real-time monitoring) as a traditional approach, but provides a significantly lower TCO through both “hard” capitalized costs, as well as operational efficiency. The approach – defined as unified threat and compliance (UTC) – provides a single platform that brings together both the operational security requirements and compliance reporting requirements of PCI DSS into a single product. SecureVue from eIQnetworks is a unified threat and compliance solution that meets this more cost-effective alternative approach to PCI DSS compliance.

Integrated Solution: SecureVue from eIQnetworks

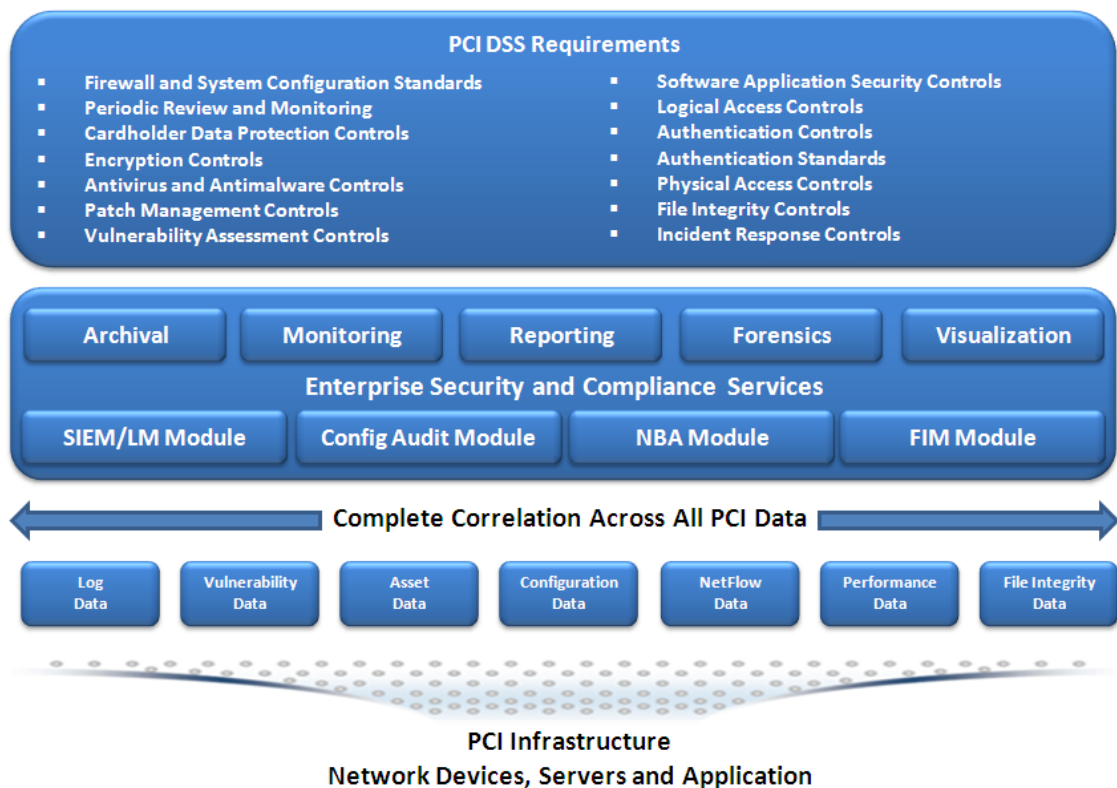


Figure 2: Unified Threat and Compliance (UTC) Approach to PCI DSS Compliance

The above diagram illustrates the breadth of collected security data, as well as the depth of security and compliance functions, provided by the SecureVue platform. Using an integrated solution such as SecureVue, organizations can address the broadest set of PCI compliance capabilities using a single product, without the need to generate piecemeal PCI compliance reports from different tools or master multiple point products that each provide only a “wedge” of PCI DSS compliance capability.

Integrated Solution (SecureVue) Profile

SecureVue from eIQnetworks capture, monitor, correlate, analyze, and reports on all technical data required to address PCI DSS compliance, including: log and event data; asset data; configuration data; vulnerability data; performance data; network flow data. SecureVue captures a broad range of data, including:

- **Log data** from Servers, network devices, and applications
- **Vulnerability data** (via a third-party vulnerability scanner) from servers, network devices and applications
- **Asset data**, such as installed applications and patches, and device/host hardware information, from servers and network devices. SecureVue collects this data without the need for an agent.
- **Security configuration data**, such as password properties and Windows registry settings, from servers and network devices. SecureVue collects this data without the need for an agent.
- **Network flow protocols**, including NetFlow, C-Flow, J-Flow, and others, from network infrastructure and security devices that generate flow data
- **File integrity data** based on both checksums and properties of files and directories
- **Performance data** from multiple sources, including SNMP and a variety of other protocols

Together, this broad set of data coupled with SecureVue's extensive analysis capabilities provide organizations with the most complete solution available to provide automation across all twelve requirements of the PCI DSS standard.

Calculating Real TCO for PCI DSS Compliance

Comparing a traditional security point product approach for PCI DSS compliance to an approach based on an integrated solution, it's clear that an approach encompassing multiple tools is inefficient. Using the point product approach, collecting all of the data and achieving all of the security functions required for PCI DSS compliance requires the purchase of multiple security point products.

In this section of the white paper, we will analyze the specific costs associated with both approaches by comparing traditional PCI DSS security point products against an integrated solution such as eIQnetworks' SecureVue. These specific cost categories include: product procurement costs; support and maintenance costs; training costs; professional services; and operations personnel.

Assumptions

Calculating TCO for a PCI DSS compliance solution is, of course, a relative process; specific assumptions must be made about the size and scope of the environment, personnel costs, and other highly variable factors. For the TCO analysis presented below, the following assumptions are made that are typical of a mid-to-large size enterprise with PCI DSS applicability:

- **Sample PCI-DSS Environment.** The organization maintains a total of 1,000 nodes as part of its PCI DSS-applicable infrastructure. This includes 300 network devices (routers, switches, firewalls, UTM, IDP, DLP, etc.), and 700 servers (Windows, UNIX, Linux, and others).
- **Solution Deployment Hardware.** This paper does not include hardware costs due to the significant range of pricing that is affected dedicated vs. shared hardware, virtualization, and other factors. However, it is safe to assume that it is likely more computing power is required for multiple point solutions, than a single, integrated solution.

- **Software Pricing.** SecureVue pricing is based on the list price of SecureVue, delivered as an appliance (one of several delivery methods for the software). SIEM point solution pricing, configuration auditing product pricing, NBA product pricing, and FIM product pricing are based on the average list price of multiple tools in their respective categories.
- **Maintenance Agreements.** Full maintenance agreements are purchased up-front on software for three (3) years.
- **Maintenance Support Level.** All software updates are included, and live vendor support is provided at least 8x5, with 7x24x365 access to on-line support options provided by the vendor.
- **Maintenance Pricing.** Maintenance costs are assumed to be 20% of the product base license, per year. This is in line with maintenance and assurance agreements throughout the IT industry.
- **Personnel for Product Training.** Two (2) personnel are assumed to be trained on each product.
- **Product Training Pricing.** Pricing for training is based on a typical rate of \$2,500 per day, per trained employee. Training is assumed to take two (2) days per product, and is assumed to take place on-site at the organization (i.e., no additional costs for travel and expenses are assumed).
- **Professional Services Personnel.** The organization uses vendor-provided resources for both deployment architecture design, and implementation services. It is assumed that one (1) vendor-provided resource conducts professional services at a time.
- **Professional Services Pricing.** Pricing for professional services is based on an assumed five (5) days of total professional services required per product: one (1) day for deployment architecture design; and (4) days for implementation services. The baseline daily rate (excluding travel and expenses) for a professional services resource is \$2,500 per day.
- **Operations Personnel Costs.** The fully-loaded cost of the organization's full-time personnel is \$100,000 per year. This value may vary based on factors such as geographic location and the overall experience of the personnel.
- **Operations Personnel Allocation for Administration.** Based on typical real-world use, this paper assumes that SIEM and integrated solution products each product require one (1) FTE for annual administration and maintenance, while configuration auditing, NBA, and FIM products require a one-half (.5) FTE for the same.
- **Operations Personnel Allocation for DBA.** For products that are back-ended by a commercial relational database management system (RDBMS), this paper assumes that SIEM products require one (1) FTE for annual database administration, while configuration auditing, NBA, and FIM products require a one-half (.5) FTE for the same.

Product Procurement Costs

The most obvious cost factor when calculating TCO is the cost of the product itself. For a traditional PCI DSS compliance approach, multiple product licenses are required for each product category (SIEM and log management, configuration auditing, network behavioral analysis, and file integrity monitoring). Using eIQnetworks' SecureVue, only one product license is required; the ability to address all four functional areas – SIEM, configuration auditing, NBA, and FIM – is included out-of-box.

PCI DSS Compliance Solution Cost Category: Product License					
Category	Integrated Solution	Point Product Approach			
	SecureVue	All Are Required for PCI DSS Compliance			
		SIEM/LM	Config Audit	NBA	FIM
Product License	\$ 469,995	\$ 260,000	\$ 200,000	\$ 80,000	\$ 60,000
TOTAL COST	\$ 469,995	\$ 600,000			
Integrated Solution Cost Savings (\$)	\$ 130,005				
Integrated Solution Cost Savings (%)	21.67%				

Table 2: Product License Cost Comparison for PCI DSS Compliance Solutions

A traditional multiple-tool approach can lead to significant issues that can incur additional costs related to vendor management that are not calculated in this scenario, such as:

- Disparate License Models.** Different license models require the organization to carefully estimate initial licenses to ensure that personnel, assets, and data are clearly quantified.
- License Scalability.** Multiple license models also make scalability difficult. In many cases, adding personnel or assets to vendor solutions “resets” maintenance and other agreements, adding further complexity to the vendor management process.

In this typical, conservatively-priced model, an integrated security approach will save the organization at least \$130,000 in initial product license costs, an almost 22% savings over a traditional multiple point security solution approach. This excludes additional cost savings in FTE personnel required to address potential vendor management issues identified above.

Annual Support and Maintenance Costs

For enterprise products such as PCI DSS compliance solutions, maintenance is a critical component to the solution lifecycle. In a traditional PCI DSS compliance approach, multiple maintenance agreements must be maintained for each product; on the other hand using an integrated solution such as eIQnetworks’ SecureVue, there is only a single maintenance license that needs to be purchased.

PCI DSS Compliance Solution Cost Category: Support and Maintenance (3 Years)					
Category	Integrated Solution	Point Product Approach			
	SecureVue	All Are Required for PCI DSS Compliance			
		SIEM/LM	Config Audit	NBA	FIM
Support and Maintenance	\$ 281,997	\$ 156,000	\$ 120,000	\$ 48,000	\$ 32,000
TOTAL COST	\$ 281,997	\$ 356,000			
Integrated Solution Cost Savings (\$)	\$ 74,003				
Integrated Solution Cost Savings (%)	20.79%				

Table 3: Product Support and Maintenance Comparison for PCI DSS Compliance Solutions

Vendor management becomes a critical requirement using a traditional point solution approach, since significant issues can arise related to juggling multiple contracts, such as:

- **Multiple Termination Points.** With multiple maintenance agreements in place, organizations may run into inconsistent termination points for support, which can be exacerbated by scaling the vendors’ product to support additional users, assets, and/or data volumes.
- **Inconsistent Term and Condition Requirements.** Working with multiple vendors means having multiple sets of product use terms and conditions, which might include significant clauses related to product usability and scope, as well as different legal remedies.

In the standard scenario presented in this paper, an integrated PCI DSS compliance approach will save the organization at least \$74,000 in aggregate support and maintenance costs over the initial three years of the solution. This represents an almost 21% savings over a traditional point solution-based approach, and excludes any additional costs associated with a traditional approach due to potential support and maintenance concerns identified above.

Training Costs

Training is critical to the operation security and compliance products. Inefficient use of security and compliance software can lead to ineffective implementation of security controls, and significant lapses in compliance reporting capability.

PCI DSS Compliance Solution Cost Category: Training							
Category	Integrated Solution		Point Product Approach				
	SecureVue		All Are Required for PCI DSS Compliance				
			SIEM/LM	Config Audit	NBA	FIM	
Training	\$	15,000	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	
TOTAL COST		\$ 15,000	\$ 40,000				
Integrated Solution Cost Savings (\$)		\$ 25,000					
Integrated Solution Cost Savings (%)		62.50%					

Table 4: Product Training Comparison for PCI DSS Compliance Solutions

In a traditional PCI DSS compliance approach, additional “hidden” costs can be incurred due to potential issues such as:

- **Inconsistent Training Quality.** With multiple vendors, initial product training quality and training consistency between vendors may vary greatly.
- **Inconsistent Training Delivery Methods.** If a uniform training delivery method is not available – and specifically, a training method that is preferred by the customer – significant gaps in product operational knowledge may surface.
- **Extended Time to Comprehensive Training.** Training personnel on multiple security point solutions will require multiple training periods, regardless of the delivery method of the training materials.

In the standard scenario presented in this paper, an integrated PCI DSS compliance approach will save the organization at least \$25,000 over the initial three years of the solution, a 62.5% savings over a traditional point solution-based approach. This excludes additional costs related to potential training issues identified above.

Professional Services

“Professional services” is a broad cost category that may include: product deployment architecture; hands-on implementation; and product customization. Some products, such as most SIEM and log management tools, may also require significant software development time for the purpose of developing “connectors,” “adapters” and other interfacing components.

PCI DSS Compliance Solution Cost Category: Professional Services						
Category	Integrated Solution	Point Product Approach				
	SecureVue	All Are Required for PCI DSS Compliance				
		SIEM/LM	Config Audit	NBA	FIM	
Deployment Architecture and Design	\$ 2,500	\$ 5,000	\$ 5,000	\$ 2,500	\$ 2,500	
Implementation/Customization Services	\$ 10,000	\$ 62,500	\$ 62,500	\$ 10,000	\$ 10,000	
TOTAL COST	\$ 12,500	\$ 160,000				
Integrated Solution Cost Savings (\$)	\$ 147,500					
Integrated Solution Cost Savings (%)	92.19%					

Table 5: Professional Services Comparison for PCI DSS Compliance Solutions

In addition to the fact that multiple point tools will likely require multiple professional services engagements, there are additional concerns related to the cost of professional services for a multiple security tool approach:

- Project Management Integration Issues.** Enterprise software such as a PCI DSS compliance solution does not get implemented overnight; it requires the organization to carefully plan, communicate, and deploy the solution over time. However, for traditional solutions based on multiple security point tools, these project management concerns can become exacerbated by the need to deploy multiple servers, databases, and other infrastructure necessary to implement each point product.
- Software Development Requirements.** Many security point solutions – and SIEM and log management products, in particular – are built around “connector” and “adapter” components that provide customers with the flexibility to collect data from non-standard sources that require extensive subject matter expertise to ensure successful development. This can often result in vendor “lock-in” as the customer is forced to utilize the limited professional services of the vendor in order to derive real value from their product.

In the standard scenario presented in this paper, an integrated PCI DSS compliance approach will save the organization at least \$147,500 in professional services over the initial three years of the solution, a significant 91% savings over a traditional point solution-based approach.

Operations Personnel

One of the most significant costs of ownership for information security and compliance software is the cost of personnel to operate and maintain the system. Operations personnel typically fall into two categories: product administrators who are responsible for all aspects of managing the product, and product database administrators who are responsible for maintaining the large databases that back-end most security and compliance products (usually relational database management systems).

PCI DSS Compliance Solution Cost Category: Operations Personnel					
Category	Integrated Solution	Point Product Approach			
	SecureVue	All Are Required for PCI DSS Compliance			
		SIEM/LM	Config Audit	NBA	FIM
Product Administrator (3 Years)	\$ 300,000	\$ 300,000	\$ 150,000	\$ 150,000	\$ 150,000
Database Administrator (3 Years)	\$ -	\$ 300,000	\$ 75,000	\$ 75,000	\$ 75,000
TOTAL COST	\$ 300,000	\$ 1,275,000			
Integrated Solution Cost Savings (\$)	\$ 975,000				
Integrated Solution Cost Savings (%)	76.47%				

Table 6: Operations Personnel Comparison for PCI DSS Compliance Solutions

Product administration costs are significantly lower for an integrated solution such as eIQnetworks' SecureVue, due to the fact that SecureVue uses a proprietary, self-maintaining database that is designed for scalability and performance.

From an operations perspective, there are additional risks to a traditional point product approach that are not captured in the above table, including:

- Single Point of Failure for Product Knowledge.** In a traditional PCI DSS compliance solution model involving multiple security products, each product typically has a limited number of users. This leaves a critical single point of failure for individual security products in the environment if a key employee with unique knowledge leaves the organization. The only alternative to mitigate this issue is to cross-train multiple employees on each solution – which adds significant cost to the overall solution.

In the standard scenario presented in this paper, an integrated PCI DSS compliance approach – and specifically, a solution which has no DBA requirements, such as SecureVue – will save the organization at least \$975,000 in fully-loaded operations personnel costs over the initial three years of the solution, a 76% savings over the operational costs of a traditional point solution-based approach.

Conclusion

Based on the cost analysis and typical assumptions presented above, it is clear that a traditional PCI DSS compliance approach based on multiple point products – while perhaps effective at meeting rudimentary PCI audit and compliance reporting – is a significantly more expensive approach than an integrated solution based on a single, enterprise product.

Cost Comparison Table

Collectively, the following table presents the total cost of ownership comparison of list pricing between the traditional multi-product approach, versus an integrated solution such as eIQnetworks' SecureVue:

PCI DSS Compliance Solution Cost Category: Overall TCO						
Category	Integrated Solution		Point Product Approach			
	SecureVue	All Are Required for PCI DSS Compliance				
		SIEM/LM	Config Audit	NBA	FIM	
Product License	\$ 469,995	\$ 260,000	\$ 200,000	\$ 80,000	\$ 60,000	
Support and Maintenance	\$ 281,997	\$ 156,000	\$ 120,000	\$ 48,000	\$ 32,000	
Training	\$ 15,000	\$ 10,000	\$ 10,000	\$ 10,000	\$ 10,000	
Deployment Architecture and Design	\$ 2,500	\$ 5,000	\$ 5,000	\$ 2,500	\$ 2,500	
Implementation/Customization Services	\$ 10,000	\$ 62,500	\$ 62,500	\$ 10,000	\$ 10,000	
Product Administrator (3 Years)	\$ 300,000	\$ 300,000	\$ 150,000	\$ 150,000	\$ 150,000	
Database Administrator (3 Years)	\$ -	\$ 300,000	\$ 75,000	\$ 75,000	\$ 75,000	
TOTAL COST	\$ 1,079,492	\$ 2,431,000				

Integrated Solution Cost Savings (\$)	\$ 1,351,508
Integrated Solution Cost Savings (%)	55.59%

Table 6: Overall TCO Comparison for PCI DSS Compliance Solutions

Based on the typical scenario and relatively conservative assumptions presented in this paper, an integrated PCI DSS approach based on a unified threat and compliance solution – such as SecureVue from eIQnetworks – will save a typical organization at least \$1,350,000 in acquisition and operating costs over the initial three years of the solution, an almost 56% cost savings versus a traditional point solution-based approach over a three-year period.

Cost Comparison Charts

Visualizing this data as an aggregate across both approaches, the following chart demonstrates the clearly lower TCO provided by an integrated solution such as SecureVue as compared to a traditional point-product approach, both in terms of overall solution cost, as well as by individual cost category:

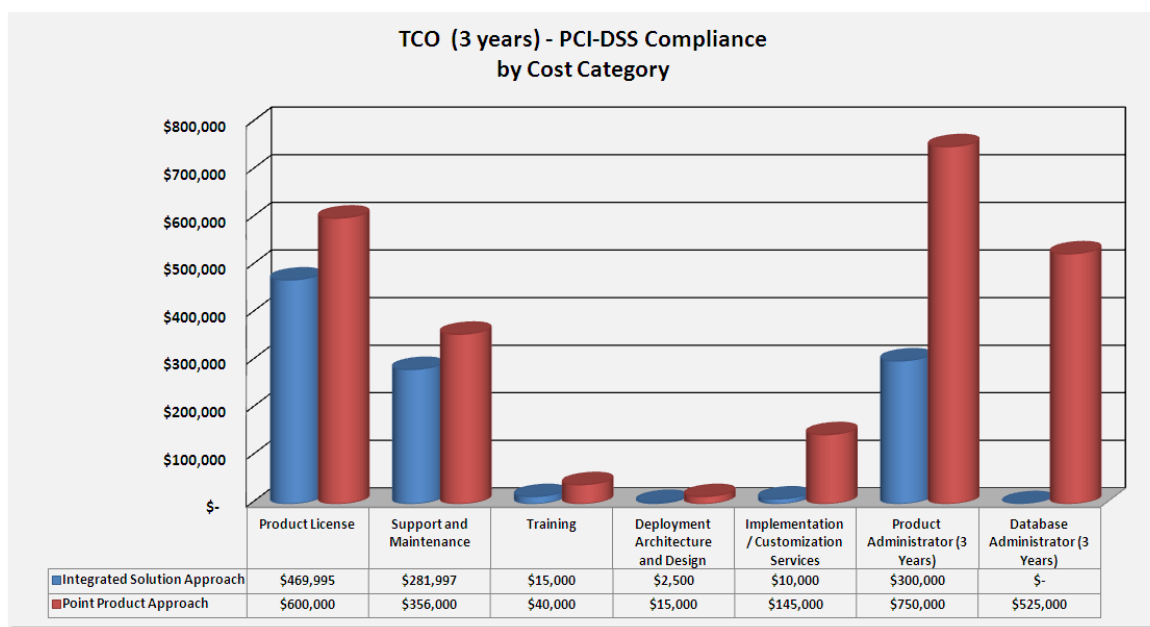


Figure 3: Three-Year TCO by Solution and Cost Category

Based on the TCO analysis presented in this paper, the following conclusions can be drawn:

- *A point solution approach to PCI DSS compliance, while it may be effective for PCI DSS compliance reporting and security operations, is highly cost-inefficient due to the need to replicate hardware, training, professional services, and other cost impacts across multiple products.*
- *An integrated solution that combines many aspects of PCI DSS compliance reporting and security operations yields a more cost-effective approach, while circumventing other issues that affect point solutions, such as scalability and the lack of situational awareness.*
- *Operational factors associated with an integrated solution provide additional value that goes beyond the cost calculations presented in this document: factors such as scalability, performance, faster return on investment, and other advantages of using an integrated solution will provide aggregate value above and beyond the “hard” costs presented here.*

Appendix 'A': Detail of Security Data Type by PCI DSS Requirement

The following table provides a detailed overview of the specific types of information security data required to address the PCI DSS standard, Version 1.2:

Requirement	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data								
1.1 – Firewall and Router Configuration Standards	■	■	-	■	-	-	■	-
1.2 – Firewall and Router Restrictions	-	■	-	■	-	-	-	-
1.3 – Prohibit Direct Access	-	-	-	■	-	-	-	-
1.4 – Install Personal Firewall Software	■	■	-	-	-	-	-	-
Requirement 2: Do Not Use Vendor-Supplied Defaults for System Passwords and Other Security Parameters								
2.1 – Change Vendor-Supplied Defaults	■	■	-	-	-	-	-	-
2.2 – Develop Configuration Standards for System Components	■	■	-	-	-	-	■	-
Requirement 3: Protect Stored Cardholder Data								
3.1 – Keep Cardholder Data Storage to a Minimum	■	-	■	-	-	-	-	-
3.2 – Do Not Store Sensitive Authentication Data	■	■	■	-	-	-	-	-
3.3 – Mask PAN When Displayed	-	■	-	-	-	-	-	-
3.4 – Render PAN Unreadable Anywhere It Is Stored	■	■	■	-	-	-	-	-
3.5 – Protect Cryptographic Keys	■	■	-	-	-	■	-	■
3.6 – Document and Implement Key-Management Procedures	-	-	-	-	-	-	■	-
Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks								
4.1 – Use Strong Cryptography	■	■	-	■	■	-	-	-
4.2 – Never Send Unencrypted PANs via Messaging Technologies	-	■	■	■	-	-	-	-
Requirement 5: Use and Regularly Update Anti-Virus Software or Programs								
5.1 – Deploy Anti-Virus Software	■	■	-	-	-	■	-	-
5.2 – Ensure Anti-Virus Capability	■	■	-	-	-	■	-	-
Requirement 6: Develop and Maintain Secure Systems and Applications								
6.1 – Install Vendor-Supplied Security Patches	■	■	-	-	-	-	-	-
6.2 – Establish a Process to Discover New Security Vulnerabilities	-	■	■	■	■	-	■	-
6.3 – Develop Secure Software Applications	■	■	■	■	■	■	■	-
6.4 – Follow Change Control Procedures	-	-	-	-	-	-	■	-
6.5 – Develop Secure Web-Based Applications	■	■	■	■	■	-	■	-
6.6 – Review Public-Facing Web Applications for Vulnerabilities	■	■	■	■	■	-	■	-
Requirement 7: Restrict Access to Cardholder Data by Business Need to Know								
7.1 – Limit Access to Cardholder Data Based on Need	■	■	■	■	-	■	-	-
7.2 – Establish an Access Control System Defaulted to “Deny All”	■	■	■	■	-	■	■	-

Requirement	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
Requirement 8: Assign a Unique ID to Each Person with Computer Access								
8.1 – Assign All Users a Unique ID Prior to Access	■	■	■	-	-	-	-	-
8.2 – Employ Authentication	■	■	■	■	-	-	-	-
8.3 – Employ Two-Factor Authentication for Remote Access	■	■	■	■	-	-	-	-
8.4 – Render Passwords Unreadable In-Transit and At-Rest	■	■	-	■	-	-	-	-
8.5 – Ensure Proper Authentication and Password Management	■	■	■	-	-	-	■	-
Requirement 9: Restrict Physical Access to Cardholder Data								
9.1 – Use Appropriate Facility Entry Controls	■	■	-	-	-	-	-	■
9.2 – Develop Physical Access Procedures	-	-	-	-	-	-	■	■
9.3 – Visitor Handling Procedures	-	-	-	-	-	-	■	■
9.4 – Use a Visitor Log	-	-	-	-	-	-	-	■
9.5 – Store Media Backups in a Secure Location	-	-	-	-	-	-	■	■
9.6 – Physically Secure Paper Media Containing Cardholder Data	-	-	-	-	-	-	■	■
9.7 – Maintain Control Over Media Distribution	-	-	-	-	-	-	-	■
9.8 – Ensure Management Approval for Data Removal	-	-	-	-	-	-	■	■
9.9 – Maintain Control Over Accessibility of Media	-	-	-	-	-	-	-	■
9.10 – Destroy Media When No Longer Needed	-	-	-	-	-	-	■	■
Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data								
10.1 – Link System Components to an Individual User	■	■	■	■	-	-	-	-
10.2 – Implement Automated Audit Trails	-	■	■	-	-	-	-	-
10.3 – Record Audit Trail Entries	-	-	■	■	-	-	-	-
10.4 – Synchronize All Critical System Clocks and Times	■	■	■	-	-	-	-	-
10.5 – Secure Audit Trail Entries	-	■	-	-	-	-	-	-
10.6 – Review Logs (At Least Daily)	-	-	■	-	-	-	■	-
10.7 – Retain Audit Trail History	-	-	■	-	-	-	■	-
Requirement 11: Regularly Test Security Systems and Processes								
11.1 – Test for Wireless Access Points	■	-	■	■	■	-	■	-
11.2 – Run Internal and External Vulnerability Scans	-	-	-	-	■	-	■	-
11.3 – Perform Internal and External Penetration Testing	-	-	-	-	■	-	■	-
11.4 – Use Intrusion-Detection Systems, and Keep Up-To-Date	■	■	■	-	-	-	-	-
11.5 – Deploy File Integrity-Monitoring Software	-	-	-	-	-	■	-	-

Requirement	Asset Data	Configuration Data	Log Data	Network Flow Data	Vulnerability Data	File Integrity Data	Policy or Procedure	Physical Security
Requirement 12: Maintain a Policy that Addresses Information Security for Employees and Contractors								
12.1 – Establish a Security Policy	-	-	-	-	-	-	■	-
12.2 – Develop Daily Operational Security Procedures	-	-	-	-	-	-	■	-
12.3 – Develop Usage Policies	-	-	-	-	-	-	■	-
12.4 – Ensure Scope of Applicability for Security Policy	-	-	-	-	-	-	■	-
12.5 – Assign Information Security Responsibilities	-	-	-	-	-	-	■	-
12.6 – Implement a Formal Security Awareness Program	-	-	-	-	-	-	■	-
12.7 – Screen Potential Employees Prior to Hiring	-	-	-	-	-	-	■	-
12.8 – Implement Policies and Procedures for Service Providers	-	-	-	-	-	-	■	-
12.9 – Implement and Test an Incident Response Plan	■	■	■	■	■	■	■	■