TECHNOLOGY BRIEF

PCI DSS COMPLIANCE WITH THE SOURCEFIRE 3D® SYSTEM

KNOW MORE NETWORK RISKS
NO MORE GUESSING

SOURCEfire®

EXECUTIVE SUMMARY

The Payment Card Industry Data Security Standard, or PCI DSS, is globally accepted across the payment industry. With the potential results of non-compliance being severe damage to the financial health and reputation of a company, payment organizations want to protect themselves to the fullest extent while minimizing unnecessary staff and IT costs.

By using the Sourcefire 3D® System, payment card merchants and service providers can improve their security and demonstrate key aspects of PCI DSS compliance without significant increases in personnel and IT costs. This technology brief will provide an overview of PCI DSS and review the specific PCI DSS requirements where the components of the Sourcefire 3D System can help payment vendors demonstrate compliance.

> *"Without Sourcefire, we would have never passed the [PCI] audits, which could have led to regulatory fines or loss of business with our partners."*
>
> **Michael Morgan, Network Security Administrator, BankersBank**

OVERVIEW OF THE PCI DATA SECURITY STANDARD (PCI DSS)

The PCI DSS was developed by the founding payment brands of the PCI Security Standards Council (PCI SSC) to enhance cardholder data security and facilitate broad adoption of consistent data security measures on a global basis. The PCI DSS version 1.2 is a comprehensive, worldwide security standard comprised of six core principles and 12 specific requirements that provide a single approach to safeguarding sensitive data for all payment card brands.

The PCI DSS applies to all organizations that store, process, and/or transmit cardholder data. It covers technical and operational system components included in or connected to cardholder data. If a merchant accepts or processes payment cards, then he must comply with the PCI DSS.

Compliance with the PCI DSS also ensures compliance with the following mandated payment industry programs:

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

PCI DSS Core Principles and Requirements

The PCI DSS consists of common sense steps that mirror security best practices. Below is a high-level overview of the six core principles and 12 PCI DSS requirements from the PCI DSS Requirements and Security Assessment Procedures, version 1.2.

Build and Maintain a Secure Network

1. Install and maintain a firewall configuration to protect cardholder data
2. Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, 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

HOW THE SOURCEFIRE 3D SYSTEM SUPPORTS COMPLIANCE WITH PCI DSS

Payment card merchants and service providers can demonstrate key aspects of PCI DSS compliance without significantly increasing staff and IT costs by using the Sourcefire 3D System. The 3D System delivers multiple best practice technology controls to improve security and demonstrate PCI DSS compliance—more than any other vendor in the IPS industry. Sourcefire's patented combination of threat and network discovery and behavioral profiling with 24x7 network monitoring and security policy enforcement provides a comprehensive network security system that meets the six core PCI DSS principles. Sourcefire's intelligent 3D System can automate security policies and defenses without increasing IT staff to gain the highest possible network protection.

Components of the Sourcefire 3D System support compliance with the following PCI DSS requirements:

- 1.1. Documented list of ports and services required for business
- 2.2. Enforcement of configuration policy
- 6.5. Develop Web applications based on secure coding and identify coding vulnerabilities
- 6.6. Protect Web applications
- 10.1. Identify users
- 10.3. Record audit trail entries
- 11.2. Run network vulnerability scans
- 11.4. Use IDS and/or IPS technology to monitor all network traffic
- 12.5. Monitor and analyze security events
- 12.9. Incident response and reporting

In the remainder of this section, we will review the specific PCI DSS requirements where the components of the Sourcefire 3D System can help payment card industry vendors demonstrate compliance.

PCI DSS Requirements 1.1.5. and 2.2.2.

> *PCI DSS Requirement 1.1.5. Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.*

> *PCI DSS Requirement 2.2.2. Disable all unnecessary and insecure services and protocols (services and protocols not directly needed to perform the device's specified function).*

Sourcefire RNA® (Real-time Network Awareness) provides 24x7, passive network intelligence, storing a real-time inventory of operating systems (OSes), services, applications, protocols, and potential vulnerabilities that exist on your network. Administrators can work with this inventory to model and enforce acceptable-use policies with "compliance white lists." White lists specify the OSes, services, applications, and protocols that are approved for use on your network and can be applied to all hosts—or a select range of hosts—on a given network segment.

The Sourcefire Defense Center® management console can generate alerts if RNA sees changes that could indicate the violation of a compliance policy, such as the introduction of new network assets or new services. In addition, Sourcefire RUA™ (Real-time User Awareness) can identify by name the user who violated the policy. Defense Center alerts can be used to trigger a number of automated responses, including removal of assets from the network through integration with network infrastructures capable of performing network access control.

PCI DSS REQUIREMENTS	HOW THE SOURCEFIRE 3D SYSTEM SUPPORTS COMPLIANCE
1.1.5. Documented list of ports, services, and protocols needed for business	With RNA, customers have real-time discovery of the assets and changes on their network. Defense Center can set and automatically enforce software and network-use policies, and RUA can identify users that violate these policies.
2.2.2. Development and enforcement of configuration policy	
SUPPORTING SOURCEFIRE PRODUCTS	
Sourcefire Defense Center, Sourcefire RNA, Sourcefire RUA	

PCI DSS Requirement 6.5.

> *Develop all Web applications (internal and external, and including Web administrative access to application) based on secure coding guidelines such as the Open Web Application Security Project Guide. Cover prevention of common coding vulnerabilities in software development processes, to include the following:*

> *6.5.1. Cross-site scripting (XSS)*
> *6.5.2. Injection flaws, particularly SQL injection. Also consider LDAP and Xpath injection flaws as well as other injection flaws.*
> *6.5.3. Malicious file execution*
> *6.5.4. Insecure direct object references*
> *6.5.5. Cross-site request forgery (CSRF)*
> *6.5.6. Information leakage and improper error handling*

SNORT® is the de facto standard for intrusion detection and prevention with more than 3.7 million downloads and over 225,000 registered users, making it the most widely deployed IPS technology in the world. The robust Snort Rules language enables the industry's most comprehensive threat coverage, detecting cross-site scripting (XSS), injection flaws (specifically SQL, LDAP, and Xpath injections, as well as other injection flaws), malicious file execution, insecure direct object references, cross-site request forgery (CSRF), and information leakage and improper error handling.

PCI DSS REQUIREMENT	HOW THE SOURCEFIRE 3D SYSTEM SUPPORTS COMPLIANCE
6.5. Develop Web applications based on secure coding guidelines and identify coding vulnerabilities	Sourcefire VRT Rules detect XSS, injection flaws, malicious file execution, insecure direct object references, CSRF, information leakage, and improper error handling.
SUPPORTING SOURCEFIRE PRODUCT	
Sourcefire VRT Rules	

PCI DSS Requirement 6.6.

> *For public-facing Web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods:*

> *Reviewing public-facing Web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any change*

PCI DSS AUDIT GUIDANCE FOR REQUIREMENT 6.6	SOURCEFIRE 3D SYSTEM CAPABILITY
Detection of threats against relevant OWASP top 10 vulnerabilities	Yes – Sourcefire VRT Rules detect network attacks against OWASP top 10 vulnerabilities.
Inspect Web application input and respond (allow, block, and/or alert) based on active policy or rules, and log actions taken	Yes – Sourcefire 3D supports this through Sourcefire VRT Rules and the policy and response (P&R) subsystem.
Prevent data leakage	Non-standard – The 3D System is capable of supporting this requirement through custom Sourcefire VRT Rules.
Enforce both positive and negative security models	Yes – Sourcefire's Compliance White List supports the positive security model. The negative model is enforced through Sourcefire VRT Rules
Inspect both Web page content, such as HTML, DHTML, CSS, and the underlying protocols that deliver content, such as HTTP and HTTPS (SSL and TLS)	Partially – Sourcefire 3D inspects for HTML, DHTML, HTTP, and CSS. SSL and TLS require that traffic is decrypted prior to inspection.
Inspect Web services messages, if Web services are exposed to the public Internet	Non-standard – The 3D System is capable of inspecting Web services messages, however customization is required.
Inspect any protocol or data construct that is used to transmit data to or from a Web application	Yes – The 3D System is capable of inspecting any protocol. However, customization may be required to support custom, proprietary protocols.
Defend against threats that target the Web application firewall itself	Yes – The 3D System is capable of both defending itself from direct attacks or attempts at evasion.
Support SSL and/or TLS termination, or be positioned such that encrypted transmissions are decrypted before being inspected by the Web application firewall	Yes – Although the 3D System does not support SSL or TLS inspection, the IPS can be placed in a position to inspect traffic after SSL and/or TLS traffic has been decrypted.

Installing a Web-application firewall in front of public-facing Web applications

Given the cost and complexity of conducting code reviews, most organizations opt to use Web application firewalls to satisfy requirement 6.6. However, PCI DSS v1.2 does not define the required capabilities of an application firewall. Instead, it simply instructs the assessor to verify that the control is in place. To understand the required features of a control meeting the 6.6 requirement, organizations and assessors must review the supplemental guidance issued by the PCI SSC on April 15, 2008. This guidance is available at https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml.

According to the information supplement, the Sourcefire 3D System can be implemented and configured to satisfy 100% of the required capabilities for a Web application firewall as defined by the PCI SSC. The table above compares the required capabilities for compliance with PCI DSS requirement 6.6 with the capabilities of the 3D System.

PCI DSS Requirements 10.1. and 10.3.

PCI DSS Requirement 10.1. Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.

PCI DSS Requirement 10.3. Record at least the following audit trail entriets for all system components for each event:

10.3.1. User identification
10.3.2. Type of event
10.3.3. Date and time
10.3.6. Identity or name of affected data, system component, or resource

Sourcefire is the only IPS provider to link user identity to security and compliance events. Rather than sifting through Active Directory, LDAP, and DHCP log files to determine the owner of a host under attack, Sourcefire RUA links both Active Directory and LDAP usernames to IP addresses involved in security and compliance events. By clicking on the username, the security analyst is presented with the user's name, department, and contact information. RUA drastically reduces the time and effort to determine users affected by security and compliance events—a crucial capability when time is of the essence.

Sourcefire RUA provides:

- 24x7 passive user identity tracking
- Automated correlation of user identity with intrusion and policy compliance events
- Comprehensive user identity information, including first and last name, department, phone number, and e-mail address
- User connection with all currently assigned IP addresses and time stamps to support 24-hour analysis and forensics

PCI DSS REQUIREMENTS	HOW THE SOURCEFIRE 3D SYSTEM SUPPORTS COMPLIANCE
10.1. Identify user's access to system components	RUA detects AD and LDAP logins and pairs usernames with corresponding IP addresses. The user's full name, department, and contact information is provided.
10.3. Record audit trail entries for all system components	For security and compliance events, RUA provides user connection with currently assigned IP addresses and time stamps.
SUPPORTING SOURCEFIRE PRODUCT	
Sourcefire RUA	

PCI DSS Requirement 11.2.

> *Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).*

> *Note: Quarterly external vulnerability scans must be performed by an Approved Scanning Vendor (ASV) qualified by PCI SSC. Scans conducted after network changes may be performed by the company's internal staff.*

In order to fulfill requirement 11.2, quarterly external vulnerability scans must be performed by a qualified ASV and passing results are required. Scans conducted after network changes can be performed by the company's internal staff or by third parties. Although Sourcefire does not directly satisfy this requirement, Sourcefire RNA continuously discovers and monitors network assets and maintains an updated inventory of OSes, services, client applications, protocols, and potential vulnerabilities that exist on your network. In real time, RNA can make you aware of changes to the network baseline, such as when a new host appears on the network or when an existing host has changed its approved configuration. By prompting you to perform scans after RNA discovers changes in your network environment, Sourcefire can improve your probability of passing the required quarterly vulnerability scans performed by an ASV.

PCI DSS REQUIREMENT	HOW THE SOURCEFIRE 3D SYSTEM SUPPORTS COMPLIANCE
11.2. Quarterly vulnerability scans (passing scans required)	RNA improves your probability of passing external scans by prompting you to perform scans after RNA discovers network changes.
SUPPORTING SOURCEFIRE PRODUCT	
Sourcefire RNA	

PCI DSS Requirement 11.4.

> *Use intrusion-detection systems, and/or intrusion-prevention systems to monitor all traffic in the cardholder data environment and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines up-to-date.*

Built on the award-winning Snort detection engine, Sourcefire IPS™ (Intrusion Prevention System) uses a powerful combination of vulnerability- and anomaly-based inspection methods—at throughputs up to 10 Gbps—to analyze network traffic and prevent critical threats from affecting your network. Whether deployed at the perimeter, in the DMZ, in the core, or at critical network segments, and whether placed in inline or passive mode, Sourcefire's easy-to-use IPS appliances provide comprehensive threat protection. Sourcefire IPS excels with extensive analytics, powerful reporting, and unrivaled scalability.

For a third-party assessment of Sourcefire's PCI DSS product capability, please see the PCI DSS Product Capability Assurance report from ICSA Labs at http://www.icsalabs.com/icsa/docs/html/communities/nips/pcidss/v11/PCI_1.1_NIPS_SOURCF_3800.pdf. The report provides a detailed understanding of how the functionality of Sourcefire's 3D System products compares to the PCI DSS version 1.1. At the time of publication, Sourcefire is the only major IPS vendor to be issued the PCI DSS Product Capability Assurance report.

PCI DSS REQUIREMENT	HOW THE SOURCEFIRE 3D SYSTEM SUPPORTS COMPLIANCE
11.4. Use IDS and/or IPS to monitor network traffic, ensure the IPS is up-to-date	Sourcefire IPS satisfies PCI DSS requirements for IDS/IPS.
SUPPORTING SOURCEFIRE PRODUCT	
Sourcefire IPS	

"PCI compliance is critical in our industry. One of the many requirements of the PCI Data Security Standard is that all traffic be monitored by both network—and host-level—intrusion detection systems. Sourcefire replaces our previous solution for this requirement and adds considerable benefits."

John Abella, CISSP, Senior Network Engineer (Head of Global Security and Infrastructure), Retail Decisions

PCI DSS Requirement 12.5.2.

> *Monitor and analyze security alerts and information, and distribute to appropriate personnel.*

Sourcefire RNA provides 24x7, passive network intelligence, storing a real-time inventory of OSes, services, applications, protocols, and potential vulnerabilities that exist on your network. By incorporating RNA's real-time network intelligence into Sourcefire IPS, the ongoing process of IPS tuning and assessing the impact of security events can be fully automated. Sourcefire Defense Center automatically correlates RNA's threat intelligence against real-time target host intelligence to determine the relevance and impact of the attack, and prioritized Impact Flags are shown on the Defense Center dashboard. By determining the relevance and impact of each intrusion attack on your network, actionable security events can be reduced by up to 99%, and security analysts can focus their attention only on those events that matter most.

In addition, all IPS and RNA events on Defense Center can be forwarded via the eStreamer™ API to other applications, such as SIEM (Security Information & Event Management) and network management platforms. The eStreamer API includes a "reference client" that allows customers to format and integrate precisely the data from Sourcefire 3D that they need.

Sourcefire RUA links Active Directory and LDAP usernames to IP addresses involved in security and compliance events, drastically reducing the time and effort to determine the affected users. By clicking on the username, the security analyst is presented with the user's full name, department, e-mail address, and phone number.

PCI DSS REQUIREMENT	HOW THE SOURCEFIRE 3D SYSTEM SUPPORTS COMPLIANCE
12.5.2. Monitor and analyze events	Impact Flags make it possible to analyze events based on the relative risk of any event, enabling immediate response to high-priority alerts. The eStreamer API offloads host and event data to third-party applications. RUA quickly correlates user identity with security and compliance events.
SUPPORTING SOURCEFIRE PRODUCTS	
Sourcefire Defense Center, Sourcefire IPS, Sourcefire RNA, Sourcefire RUA	

PCI DSS Requirement 12.9.

Implement an incident response plan. Be prepared to respond immediately to a system breach.

PCI DSS Requirement 12.9.5. Include alerts from intrusion-detection, intrusion-prevention, and file integrity monitoring systems.

Sourcefire Defense Center's custom workflows enable you to match the Sourcefire 3D technology to your incident response plan. Sourcefire RNA continuously discovers and monitors network assets and maintains an updated inventory of OSes, services, client applications, protocols, and potential vulnerabilities that exist on your network. Defense Center can generate alerts in the form of e-mail messages or SNMP alerts if RNA sees changes that could indicate the violation of a compliance policy, such as the introduction of new network assets or new services. Security analysts can also receive alerts through a third-party SIEM using the Sourcefire eStreamer capability. These real-time alerts can be used to trigger a number of automated responses, including removal of assets from the network through integration with network infrastructures capable of performing network access control.

With RNA's change management capability and powerful policy and response (P&R) engine, Information Security or Network Operations can be notified the moment a new host appears on the network and/or when an existing host has changed its approved configuration (e.g., OS upgrade, new service). In addition, Sourcefire's Remediation API enables the 3D System to direct external devices and systems to help enforce policies and/or take corrective actions, such as quarantining connections at the firewall or router.

Customers can leverage a variety of Defense Center's pre-defined report templates or create custom reports to meet the needs of any organization. Reports can be created in PDF, HTML, and CSV formats, which can be automatically e-mailed for easy distribution.

PCI DSS REQUIREMENT	HOW THE SOURCEFIRE 3D SYSTEM SUPPORTS COMPLIANCE
12.9. Incident response and reporting	Policy options, including use of the Remediation API, enable you to automate the response of alert-on incidents. Security analysts can receive alerts via e-mail, SNMP, or through a third-party SIEM using the eStreamer API. Reports are available on security events and policy violations.
SUPPORTING SOURCEFIRE PRODUCTS	
Sourcefire Defense Center, Sourcefire IPS, Sourcefire RNA, Sourcefire RUA	

TAKE THE NEXT STEP TO PROTECT YOUR NETWORK AND DEMONSTRATE PCI DSS COMPLIANCE

Payment card organizations can improve their security and demonstrate PCI DSS compliance by using the Sourcefire 3D System. The 3D System supports compliance with the PCI DSS requirements by:

- Real-time discovery of all hosts on the network
- Incident response
- Intrusion detection and prevention
- User identity tracking
- Configuration policy and acceptable-use monitoring and enforcement
- Ad-hoc and scheduled reports for examiners
- Compensating control for Web application firewalls

The following table illustrates the components of the Sourcefire 3D System that satisfy various requirements of the PCI DSS.

PCI DSS REQUIREMENT	SOURCEFIRE 3D SYSTEM COMPONENT			
	DC	IPS	RNA	RUA
1.1. Documented list of ports, services, and protocols needed for business - standard router configuration			✔	
2.2. Development and enforcement of configuration policy	✔		✔	✔
6.5. Develop Web applications based on secure coding guidelines and identify coding vulnerabilities		✔		
6.6. Ensure all public Web-facing applications are protected against known attacks		✔	✔	
10.1. Establish a process for linking all system access to individual users				✔
10.3. Record audit trail entries for all system components				✔
11.2. Quarterly vulnerability scans (passing scans required)			✔	
11.4. Use IDS and/or IPS to monitor network traffic, ensure the IPS is up to date		✔		
12.5.2. Monitor and analyze events	✔	✔	✔	✔
12.9. Incident response and reporting	✔	✔	✔	✔

For more information about the Sourcefire 3D System, visit Sourcefire's website at www.sourcefire.com or contact Sourcefire or a member of the Sourcefire Solutions Network™ today.