

MEETING PCI DATA SECURITY STANDARDS WITH JUNIPER NETWORKS STRM SERIES SECURITY THREAT RESPONSE MANAGERS

When it Comes to Monitoring and Validation it Takes More Than Just Collecting Logs

Table of Contents

Executive Summary	1
Data Theft On The Rise	1
Payment Card Industry Data Security Standard (PCI DSS) Synopsis	1
Log Collection Is Essential, but PCI DSS Demands More	2
Addressing the Key PCI Requirements with STRM Series	3
Build and Maintain a Secure Network	4
The STRM Series Approach:	4
Protect Cardholder Data	6
Maintain a VA Program	6
Regularly Monitor and Test Network	8
Maintain an Information Security Policy	9
Conclusion	9
About Juniper Networks	10

Executive Summary

PCI DSS stands for Payment Card Industry Data Security Standard. This standard was created by major credit card companies to ensure privacy and security of credit card holders. All organization small or large that deal with any credit card processing and transactions need to comply with these standards to avoid fees and penalties.

The PCI DSS standard outlines six relatively broad control objectives for network security:

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

This is not an easy task for IT administrators to implement these standards across their network. There is no one product that solves these standards. Many Security Information Management/Security Event Management (SIM/SEM) and log management products claim to answer all these concerns. However, PCI DSS standard calls for more than the collection and correlation of logs. Insight into the network from the passive monitoring of network communications must be put in place in conjunction with aggregation and correlation of logs from the security and network infrastructure.

The Juniper Networks® STRM Series Security Threat Response Managers combine log management, security event and information management, and network behavioral and anomaly detection (NBAD) into a single integrated end-to-end network security management solution. That allows administrators to get a complete picture of their network security posture. This whitepaper will show you how the STRM Series addresses these six main PCI DSS objectives

Data Theft On The Rise

Jan 9, 2000: 25,000 credit card numbers and addresses are stolen from the online music retailer CDUniverse.com and posted on the Internet for sale.

May 22, 2005: Master Card reports more than 40 Million credit cards were exposed to potential fraud because of a security breach by a hacker.

July 2005 through January 2007: TJX retailer announces 46.5 million credit cards were stolen by unknown hackers.

It does not require detailed analysis to see an increase in the frequency and intensity of credit card and identity theft targeting retailers, merchants and banks. A quick glance at major headlines reveals there are major blind spots in many organizations' security infrastructures that result in compromised customer and consumer data.

Payment Card Industry Data Security Standard (PCI DSS) Synopsis

Online retail revenue increased 25 percent from 2005 to 2006, reaching \$102 billion, and is projected to grow to \$300 billion by 2010. The rapid increase in online shopping transactions have forced retailers to quickly roll out new network infrastructure and technologies to streamline their business and meet customer demand.

Unfortunately, in the process of adapting to market trends, network security planning and policy has often been overlooked, highlighting the need for a common security standard.

PCI DSS was developed by VISA and is currently the standard for online credit card data security. PCI DSS is a set of data and network security requirements for companies that process credit card transactions—such as retail and insurance companies—for the purpose of protecting sensitive credit card information.

The PCI DSS standard outlines six relatively broad control objectives for network security:

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

These six control objectives are made up of 12 more detailed requirements.

The PCI DSS standard also includes objectives not found or highlighted in other regulatory compliance standards, such as an emphasis on monitoring the demilitarized zone (DMZ) and tracking which protocols and applications are traversing the network. This visibility into a broader set of monitoring inputs requires a security solution that provides in-depth analysis of the network, as well as the ability to monitor typical perimeter security devices and host system logs.

The cornerstone of the PCI DSS is the same as other regulatory compliance standards, which is to build and maintain a secure network. From a monitoring perspective, this means customers must be able to achieve fully compliant logging with best-in-class monitoring to manage threats and incidents. After all, how can a company meet any compliance standard if the network is not secure?

Log Collection Is Essential, but PCI DSS Demands More

There are an abundance of products that can and should be deployed to help meet PCI DSS requirements such as:

- Encryption products to ensure that cardholder data is being securely stored and transported over the Web
- Firewalls to ensure the protection of the DMZ or other sensitive areas of the network
- Vulnerability assessment tools that provide visibility into where risks are

These products are a critical part of the security infrastructure but they also raise other concerns at the forefront of security today:

- How do we unify products to provide the most efficient enterprise-wide security solution that meets PCI DSS requirements?
- How do we deal with the massive amounts of information (logs, events, alerts and flow data) created by these independent network and security devices?
- How do we get an accurate picture of what is going on in the network relative to PCI DSS and other regulatory compliance standards?

Many Security Information Management/Security Event Management (SIM/SEM) and log management products claim to answer all these concerns. However, PCI DSS standard calls for more than the collection and correlation of logs. In order to meet many of PCI DSS's requirements, insight into the network from the passive monitoring of network communications must be put in place in conjunction with aggregation and correlation of logs from the security and network infrastructure.

Through collection, aggregation, analysis and correlation of logs, a multitude of threats and violations can be detected. Yet relying on logs as the principle source of surveillance data leads to PCI DSS monitoring blind spots.

Building a secure network infrastructure and providing accountability, transparency and measurement to meet PCI DSS requirements requires a network-wide security monitoring solution that leverages more than logs. A successfully secure network combines important log data with vulnerability and flow data (network context) to provide an accurate assessment and prioritization of threats and violations relative to PCI DSS.

While being able to complement host, application and database logs, security event data and vulnerability information with network context allows for another layer of analysis and correlation to occur that significantly improves accuracy and prioritization of detected incidents. Logs from a large variety of security and network devices can be compared and correlated with what is occurring on the network for validation purposes.

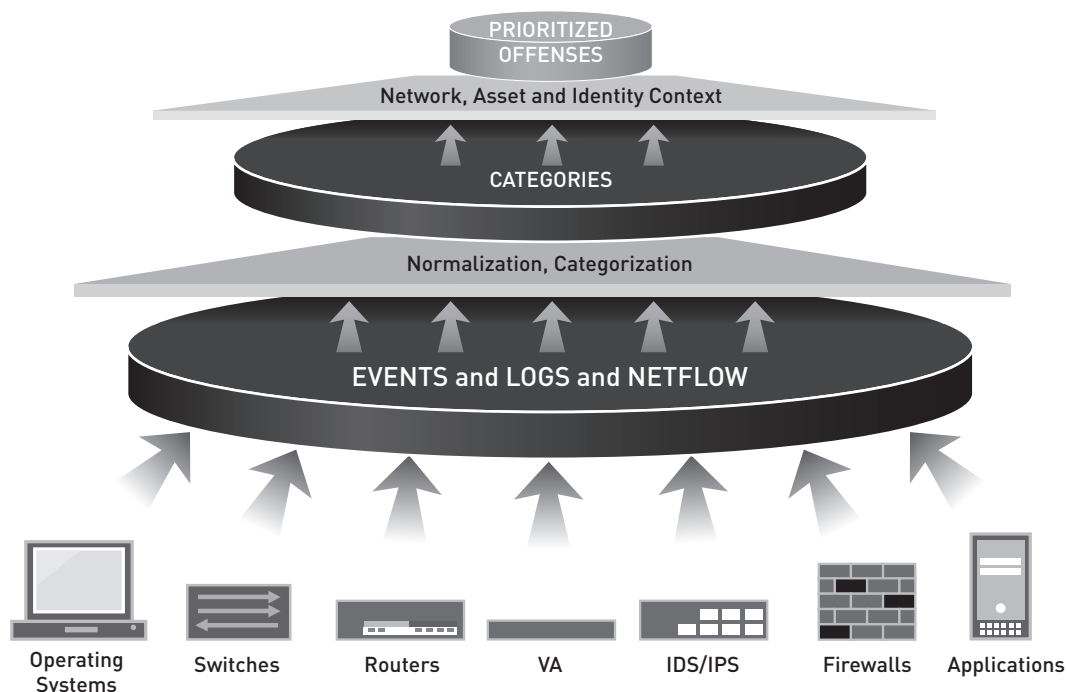
The STRM Series is a solution that combines log management, security event and information management, and network behavioral and anomaly detection (NBAD) into a single integrated end-to-end network security management solution.

For example: An anomalous file transfer not associated with normal in-policy backups occurs from a windows filer server. STRM Series detects and alerts this change in behavior that could be potential data theft. STRM Series can automatically start analyzing logs from the windows file servers to determine the user doing the transfer and what files are being accessed. All this evidence is accumulated and visible within a single offense.

This level of visibility and analysis is accomplished through a unique security architecture that collects security events, logs, network context, vulnerability and identity data to detect any type of threat or policy violation. The result is a list of actionable and highly prioritized offenses.

Addressing the Key PCI Requirements with STRM Series

STRM is a network security management platform that facilitates the comparison of data from the broadest set of devices and network traffic. This surveillance capability brings together all pertinent PCI DSS data for the purpose of executing and maintaining an organization's PCI DSS program.



STRM Series: Overview Technology Elements Related to PCI Requirements

	ACCOUNTABILITY	TRANSPARENCY	MEASUREMENT
Build and maintain a secure network	Monitor for risky/un-trusted protocols and out of policy applications	Layer 7 application analysis and automatic policy learning	Real time alerting and reporting
Protect card holder data	Monitor for proper secure protocols, encrypt card holder log data from devices to STRM	Layer 7 application analysis and encrypted transport of logs and flows across the network	Alerting and reporting on threats to critical systems
Maintain VA program	Utilize passive and active VA scanning to ensure up to date VA data for correlation, AV logs	Asset profiles and groups	Accurate correlation and analysis of threats, detect missed threats
Implement strong access control measures	Leverage logs and flows for identifying restricted access violations	User identity data correlated to asset profiles	STRM Series offenses associates actual users to offenses
Regularly monitor and test networks	Collect, store and analyze access and authentication log data	Correlation Rules: out of the box compliance intelligence	STRM Series offenses for failed login attempts followed by success
Maintain an information security policy	Develop strong security procedures and policies	Automated controls and enforcement	STRM Series offenses, reports, real-time views and dashboard

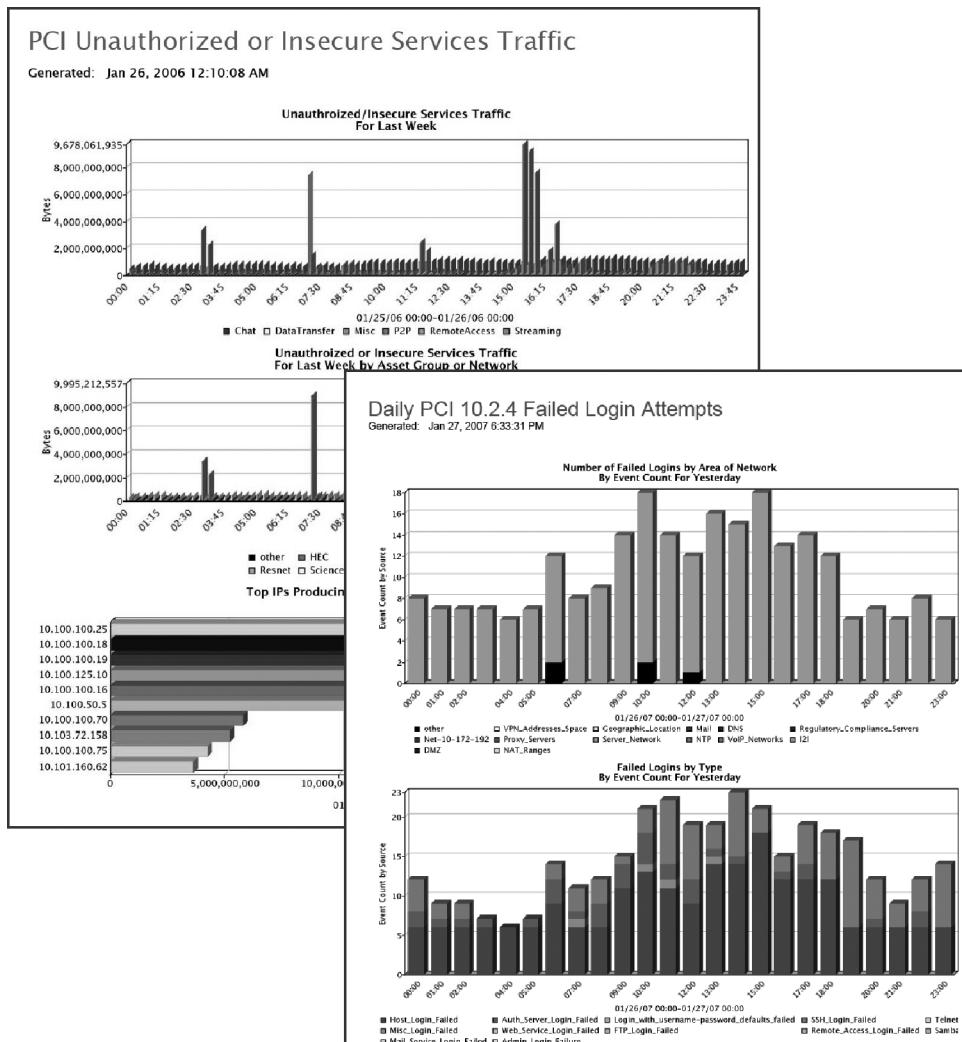
The following are the key PCI requirements and the role that STRM Series plays in addressing each of these.

Build and Maintain a Secure Network

Requirement 1.1.6 and 1.1.7: Justification and documentation for any available protocols besides HTTP, SSL, SSH and VPN as well as for risky protocols such as FTP.

The STRM Series Approach:

- Detection and classification of protocols and applications within the network.
- Policy creation allows for detailed monitoring and alerting on protocols that have been documented as risky and not permitted on the network.
- Automatic policy creation through learning normal traffic behavior and acceptable protocols, alerting when traffic deviates from normal patterns, and alerting when new servers, databases, protocols or applications are discovered in the DMZ.
- Layer 7 visibility detects and alerts risky or secure protocols running over non-standard ports, which indicates suspicious behavior.
- Real time intuitive views of network traffic by protocol or application allow for in-depth analysis and troubleshooting.
- Storage of flows like NetFlow, SFlow, JFlow and QFlow (with content) allows for detailed forensic searching of network communications associated with risky or mistrusted protocols.
- Default PCI report templates and a flexible reporting wizard provide in-depth reports on PCI-related networks and services.

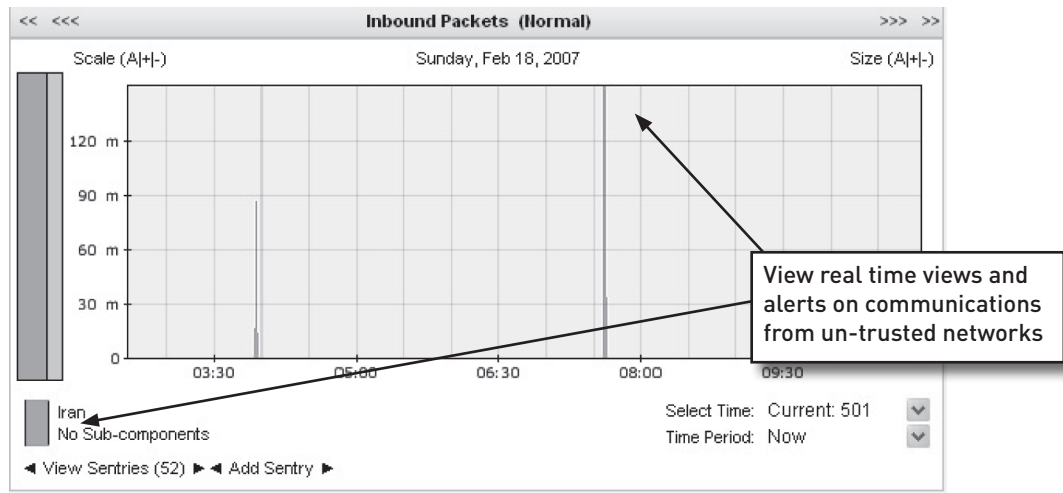


Requirement 1.2: Build a firewall configuration that denies all traffic from “un-trusted” networks and hosts, except for protocols necessary for the cardholder environment.

STRM Series:

- Correlation of network communications with geographical data to provide real time views and alerts about the source countries of network traffic. STRM Series provides real time views of traffic by geography, making it easy to identify and alert traffic originating from an un-trusted network. The definition of networks as objects also allows you to monitor inter-network communications.
- Reporting and alerting un-trusted networks and un-trusted protocols within the DMZ, or Internet traffic traversing the DMZ into secure areas of a network.
- Collection, correlation, analysis, alerting and reporting on firewall log data.

STRM Series Example: Monitoring and Alerting on Network Traffic From Un-Trusted Networks



STRM Series Example: Drill Down Into Traffic From Un-Trusted Protocols Reveals Communication With Internal Business Assets

The screenshot displays a "Results - Flow" table with columns for Local Address, Port, Remote Address, Port, Bytes (In/Out), Packets (In/Out), Protocol, Content, and Application. The following table represents the data shown in the screenshot:

Local Address	Port	Remote Address	Port	Bytes In	Bytes Out	Packets In	Packets Out	Protocol	Content	Application
205.174.165.4	rank6	87.107.58.204	64722	868	598	13	6	tcp_ip		
10.100.50		10.100.50	64722	530	1,340	7	14	tcp_ip		

A callout box points to the second row of the table, containing the text: "Network traffic displays exchange server communicating back to untrusted network". A secondary callout box points to the "Resolve" field for the second row, showing details for the IP 10.100.50.4:

- Target Magnitude: (177100)
- Offenses: 9
- Host Name: q1exch01.q1labs.inc
- Machine Name: 10.100.50.4
- User: Q1EXCH01\$
- Network: Net-10-172-192-Net_10_0_0_0

Requirement 1.3 and 1.4: Build a firewall configuration that restricts connections between publicly accessible servers and any system component storing cardholder data, including any connections from wireless networks.

STRM Series:

- Default DMZ monitoring of inbound and outbound traffic for validation of firewall configuration.
- Default compliance server objects allows for the grouping of systems with cardholder data for the purpose of monitoring communications with other networks and ensuring they are running trusted applications and protocols.
- The STRM Series intuitive rules engine allows for easily developed correlation rules that can be written specifically for the DMZ and cardholder systems, in order to correlate logs and alert for any unnecessary network communications.
- Collection, correlation, analysis, alerting and reporting on firewall log data.

Requirement 1.4: Inhibit direct public access between external networks and any system component that stores cardholder data (for example, databases, logs and trace files).

STRM Series:

- STRM provides layer 7 screening of traffic for accurate detection and classification of protocols and application in the DMZ or anywhere else in the network.
- Detection and reporting of outbound traffic from credit card applications into the DMZ.

Requirement 2.2.1 to 2.3: Do not use vendor-supplied system passwords and other security parameters.

STRM Series:

- Define alerts for detection of potentially insecure services and protocols running on web servers, databases and so on.
- Detection and alerting on non-encrypted user name, passwords and protocols.

Protect Cardholder Data

Requirement 3: Protect stored data.

STRM Series:

- Alert and notification of any suspicious attempts to sensitive data.

Requirement 4: Encrypt transmission of cardholder data across open and public networks.

STRM Series:

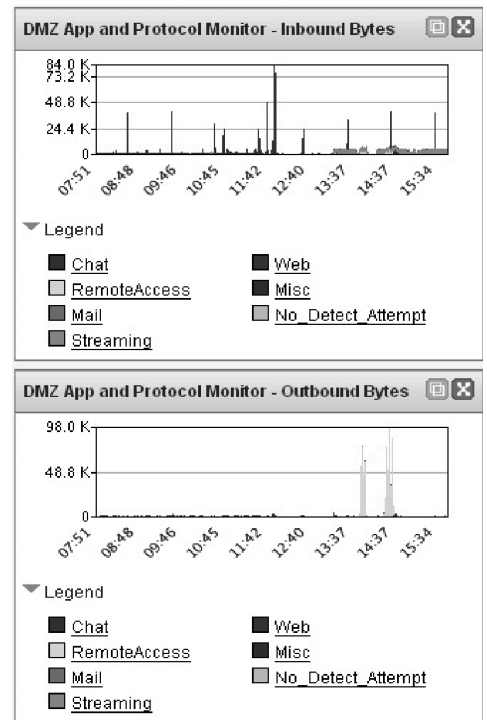
- Even in the absence of intrusion detection systems, STRM Series can detect unencrypted data.
- STRM Series stores the content from flows, which allows detection of unencrypted user name and passwords, or information on potential data theft.
- Logging from encryption technologies such as SNMP V3 devices.

Maintain a VA Program

Requirement 5: Use and regularly update antivirus software or programs.

STRM Series:

- Automatic correlation of antivirus data with other logs and network information for accurate detection and prioritization of threats.
- Reporting and real time viewing of antivirus logs.



Requirement 6: Develop and maintain security systems and applications.

STRM Series:

- Integration with vulnerability management and assessment tools used for creation of asset/host profiles.
- Asset profiles are centrally stored within the STRM Series and used for detection of new hosts on the network, new services running on a host or network, and accurate prioritization of threats based on vulnerability information.
- STRM Series uses real time passive profiling to augment vulnerability data, which is typically not kept up to date, by using network communications to profile which services are running on hosts and keep asset profiles up to date.
- Implement strong access controls.

Requirement 7: Restrict access to cardholder data by business need-to-know.

STRM Series:

- Complete auditing and alerting for access, configuration changes, data changes to systems and databases with cardholder data.
- Detection of multiple logins that are followed by a failed login from suspicious or unknown hosts.
- Default, out of the box authentication log correlation rules allow for easy identification of regulatory compliance servers and quick configuration of internal policies.

STRM Series Example: Access and Authentication Rule for Regulatory Compliance

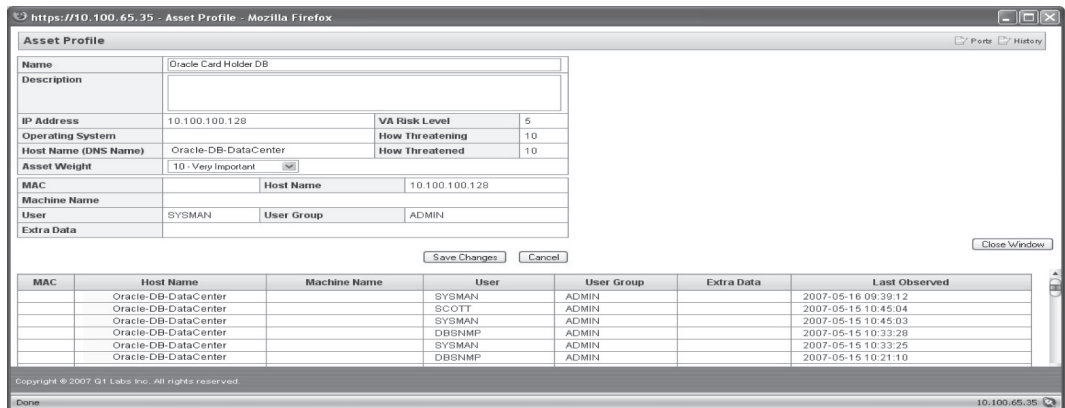
<p>Apply this rule <u>Default-Rule-Compliance: Excessive Failed Logins to Cor</u> on events which are detected by the system</p> <ul style="list-style-type: none"> • and when we see an event match any of the following <u>Default-BB-ComplianceDefinition: GLBA Servers</u>, <u>Default-BB-ComplianceDefinition: HIPAA Servers</u>, <u>Default-BB-ComplianceDefinition: SOX Servers</u>, <u>Default-BB-ComplianceDefinition: PCI Servers</u> • and when we see any of these <u>Default-BB-CategoryDefinition: Authentication Failures</u> with the same <u>destination IP</u> more than <u>10</u> times, across <u>more than 0</u> destination IP(s) within <u>10</u> minutes
<p>Notes (Enter your notes about this rule)</p> <p>Reports excessive authentication failures to a compliance server within 10 minutes.</p>

Requirement 8: Assign a user ID to each person with computer access.

STRM Series:

- The STRM Series leverages existing user identity information within log data from authentication devices, VPN devices and databases, in order to keep a history and audit of user identity assignments to IP addresses, as well as keep a history of access to databases (for example, users logging into Oracle databases).
- Violations and threats against PCI policies are tagged with user identity of IP when a PCI violation is detected.
- Detection of un-encrypted user names and passwords being used to login to cardholder systems.

STRM Series Example: Asset Profile User History and Oracle Server Database Access Audit



Regularly Monitor and Test Network

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

STRM Series:

- Out-of-the-box customizable access and authentication rules allow for easy detection of threatening or invalid access attempts.
- Deep forensic inspection analyzes all log data and network communications to monitor and audit all activity around an access offense.
- File integrity monitoring and notification through log analysis.
- Backup and archive of access audit trails.

STRM Series Example: PCI Violation Offense (Oracle DB Compromise)

Offenses are used to detect threats and violations and keep a history of all information (flows and logs) associated with the offense.

Database user associated to the logs that created the offense is clearly displayed, so there is not need for digging through logs.

Highest severity events and log messages are displayed in offense with easy drill down to all logs for a complete audit.

Event Name	Magnitude	Device	Category	Destination	Start Time
EXECUTE PROCEDURE succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
EXECUTE PROCEDURE succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
EXECUTE PROCEDURE succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
EXECUTE PROCEDURE succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
EXECUTE PROCEDURE succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
EXECUTE PROCEDURE succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
EXECUTE PROCEDURE succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
EXECUTE PROCEDURE succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
SELECT succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32
SELECT succeeded	██████████	Auto-discovered OracleDbAudit at qaoracle	System Action Allow	Oracle	05-16 10:09:32

Requirement 11: Regularly test security systems and processes.

STRM Series:

- The STRM Series provides continuous monitoring of security, systems and processes.
- Real time alerting and notification of changes to the network, and threats or violations that impact meeting compliance.
- Up to date vulnerability information through the use of passive profiling of network communications.
- Application layer visibility with a layer 7 analysis of the network.
- Real time views and historical reports of all collected network and log data.

Viewing events from 2007-05-16 09:35:00 to 2007-05-16 11:36:00 (View Real Time Events)

Current Filters:
High Level Category: Authentication (Clear Filter)

Event Name	Device	Event Count	Start Time	Category	Source
Misc Logout	Auto-discovered OracleDbAudit at qaoracle	1	2007-05-16 10:50:20	Misc Logout	Oracle Card Holder DB:0
Misc Login Succeeded	Auto-discovered OracleDbAudit at qaoracle	1	2007-05-16 10:50:17	Misc Login Succeeded	Oracle Card Holder DB:0
Misc Logout	Auto-discovered OracleDbAudit at qaoracle	1	2007-05-16 10:39:21	Misc Logout	Oracle Card Holder DB:0
Misc Login Succeeded	Auto-discovered OracleDbAudit at qaoracle	1	2007-05-16 10:39:15	Misc Login Succeeded	Oracle Card Holder DB:0
Misc Logout	Auto-discovered OracleDbAudit at qaoracle	1	2007-05-16 10:22:51	Misc Logout	Oracle Card Holder DB:0
Misc Login Succeeded	Auto-discovered OracleDbAudit at qaoracle	1	2007-05-16 10:22:48	Misc Login Succeeded	Oracle Card Holder DB:0
Misc Logout	Auto-discovered OracleDbAudit at qaoracle	1	2007-05-16 09:55:30	Misc Logout	Oracle Card Holder DB:0
Misc Login Succeeded	Auto-discovered OracleDbAudit at qaoracle	1	2007-05-16 09:55:27	Misc Login Succeeded	Oracle Card Holder DB:0

Advanced filtering and real time view of aggregated logs and events.

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

STRM Series:

- Continuously analyzes all network and security data for identification of threats and vulnerabilities.
- Automatically learns all assets and hosts on the network and provides user identity profile and running services profile based on passive vulnerability assessment and active vulnerability assessment.
- Default STRM Series built-in policy rules map directly to PCI requirements.
- Easy to use customizable rules engine that allows organizations to build their own compliance intelligence for monitoring and notification of specific violations.
- Offenses provide documented and historical perspective of all analysis and data associated to a PCI-related incident.

Conclusion

The wide ranging security and network requirements of PCI and other regulatory compliance standards requires a network security platform with the intelligence and architecture that supports global organizations with a diverse set of network and security devices. In order to meet these requirements, STRM Series leverages log and network flow data to provide intelligent and highly prioritized information on threats, risks and violations. The STRM Series allows security and network operations teams to gain control of network security and stay on top of the mountains of data they are presented with on a daily basis.

About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or 408.745.2000
Fax: 408.745.2100
www.juniper.net

APAC Headquarters

Juniper Networks (Hong Kong)
26/F, Cityplaza One
1111 King's Road
Taikoo Shing, Hong Kong
Phone: 852.2332.3636
Fax: 852.2574.7803

EMEA Headquarters

Juniper Networks Ireland
Airside Business Park
Swords, County Dublin, Ireland
Phone: 35.31.8903.600
EMEA Sales: 00800.4586.4737
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.