DATASHEET

STRM SERIES SECURITY THREAT RESPONSE MANAGERS

Product Overview

The integrated approach of the STRM Series used in conjunction with unparalleled data collection, analysis, correlation and auditing capabilities, enables organizations to quickly and easily implement a corporate-wide security management program that delivers security best practices that include:

Log Management: STRM Series provides scalable log management by enabling distributed log collection across an organization and a centralized view of the information.

Threat Management: STRM Series provides an advanced network security management solution that bridges the gap between network and security operations to deliver real time surveillance and detect complex IT-based threats.

Compliance Management: STRM Series brings to enterprises, institutions and agencies the accountability, transparency and measurability that are critical factors to the success of any IT security program required to meet regulatory mandates.

Product Description

Juniper Networks® STRM Series Security Threat Response Managers combines, analyzes and manages an incomparable set of surveillance data—network behavior, security events, vulnerability profiles and threat information—that empowers companies to efficiently manage business operations on their networks from a single console. With pre-installed software, a hardened operating system and a Web-based setup, the STRM Series lets you get your network security up and running quickly and easily. The bottom line of the STRM Series is simple deployment, fast implementation and improved security, at a low total cost of ownership.

STRM500

Juniper Networks STRM500 Security Threat Response Manager combines all the features and functionality in a single, secure hardware offering. It provides an all-in-one security solution that plugs right into a network, making it fast and easy to deploy. With its intuitive Web-based user interface, configuration is so simple that you can get a STRM500 up and monitoring the network in minutes. STRM500 is optimized hardware that does not require expensive external storage, third-party databases or ongoing database administration. The STRM500 is ideal for deployments in small, medium and large enterprises or departments that do not foresee the need to upgrade to higher events per second or flows/min capacities. STRM500 can also be deployed as dedicated QFlow collectors for collection of network flows to provide Layer 7 analysis.

STRM2500

Juniper Networks STRM2500 Security Threat Response Manager is an enterprise-class appliance that provides a scalable network security management solution for medium-sized companies up to large, globally-deployed organizations. The STRM2500 is the ideal solution for growing companies that will need additional flow and event monitoring capacity in the future. It is also the base platform for large companies that may be geographically dispersed and looking for an enterprise-class scalable solution. The STRM2500 includes on-board event collection, correlation and extensive reporting capabilities.

STRM5000

Juniper Networks STRM5000 Security Threat Response Manager is an enterprise and carrier-class appliance which provides a scalable network security management solution for medium-sized companies up to large, globally-deployed organizations. STRM5000 is the ideal solution for growing companies that anticipate the need for additional flow and event monitoring capacity in the future. It is also the base platform for large companies that are geographically dispersed and looking for a distributed enterprise/carrier-class scalable solution. The STRM5000 utilizes on-board event/flow collection and correlation capabilities, and is expandable with additional STRM5000 appliances acting as event and flow collectors.

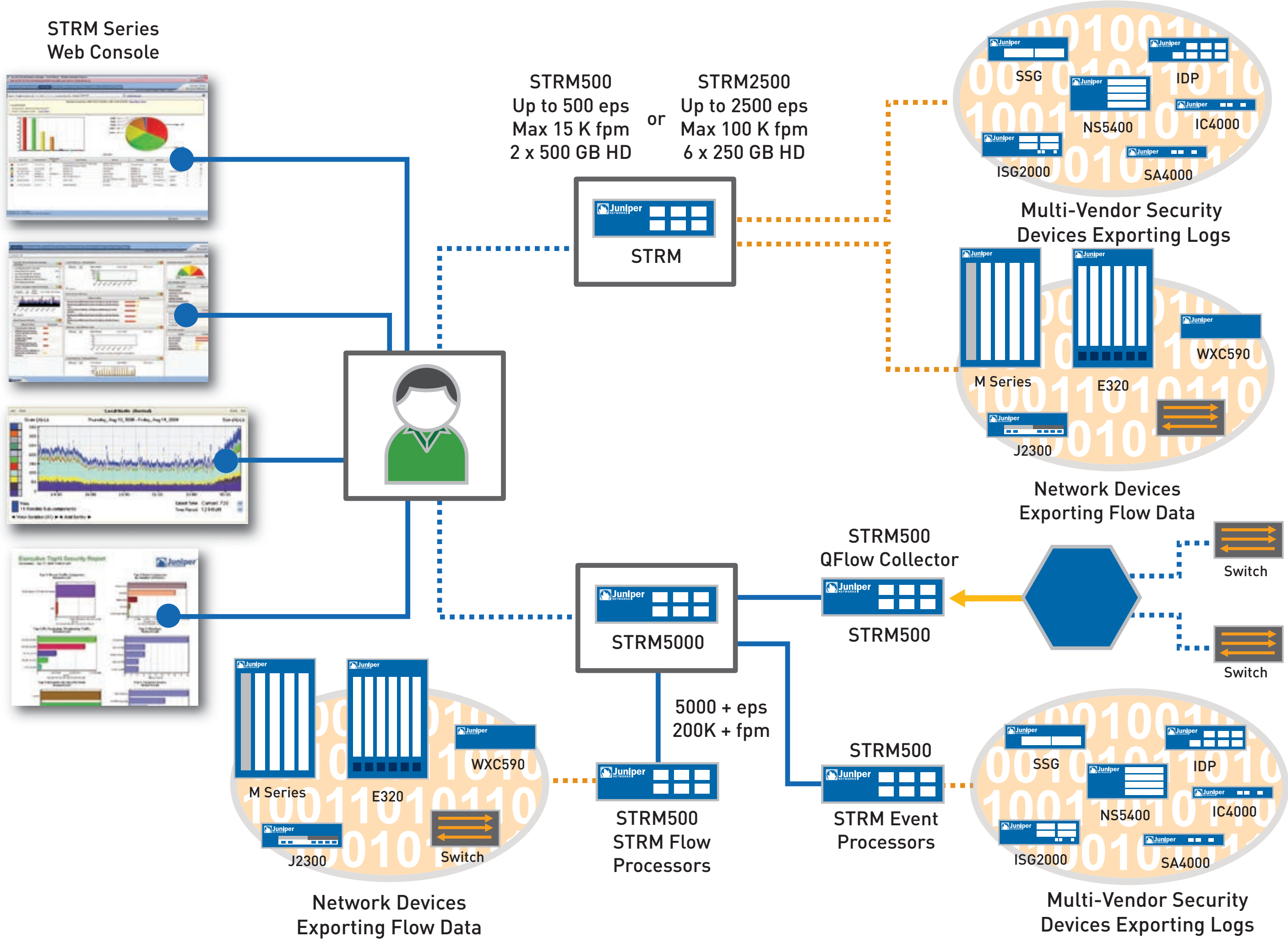

Figure 1: Depicts two scenarios with STRM500 and STRM2500 in a typical deployment, and an STRM5000 deployed in a distributed environment with the STRM500 configured as a QFlow Collector

Features and Benefits

FEATURES	FEATURE DESCRIPTION	BENEFITS
Embedded QFlow	Allows users to tap into Layer 7 traffic by using existing ports or extended 4-port module (optional).	Provides visibility into the security controls, the business applications, and the assets that are being protected.
Distributed support	Ability to scale to large distributed deployments from 500 to 10,000+ events from 15 K to 400 K flows per minute.	Users have the flexibility to scale to large deployments as their business grows. STRM Series can be easily deployed in large distributed environments.
Hardened OS	Juniper's security team monitors and maintains the STRM Series that is optimized for performance and security.	Users don't need to worry about security vulnerabilities, support or patch management for the OS.
Redundant Arrays of Inexpensive Disks (RAID) implementation	STRM Series utilizes embedded RAID (1-5) implementation.	RAID implementation provides High Availability (HA) and redundancy.

Features and Benefits (continued)

FEATURES	FEATURE DESCRIPTION	BENEFITS
All-in-one appliances	Event collection, flow collection event processing, flow processing, correlation, analysis and reporting are all embedded within the Juniper Networks STRM Series Security Threat Response Managers.	All core functions are available within the system and it is easy for users to deploy and manage in minutes. STRM Series architecture provides a streamlined solution for secure and efficient log management from a common interface.
Easy and quick install	Easy out-of-the-box setup wizard.	Users can install and manage STRM Series appliances in a couple of steps.
Centralized updates	One place to get all updates.	Users don't need to worry about maintaining appliance and OS updates and patches.
One stop support	Juniper Networks Technical Assistance Center (JTAC) supports all aspects of the STRM Series and multi-vendor support.	Users don't need to go to several places to get support even for multi-vendor issues.

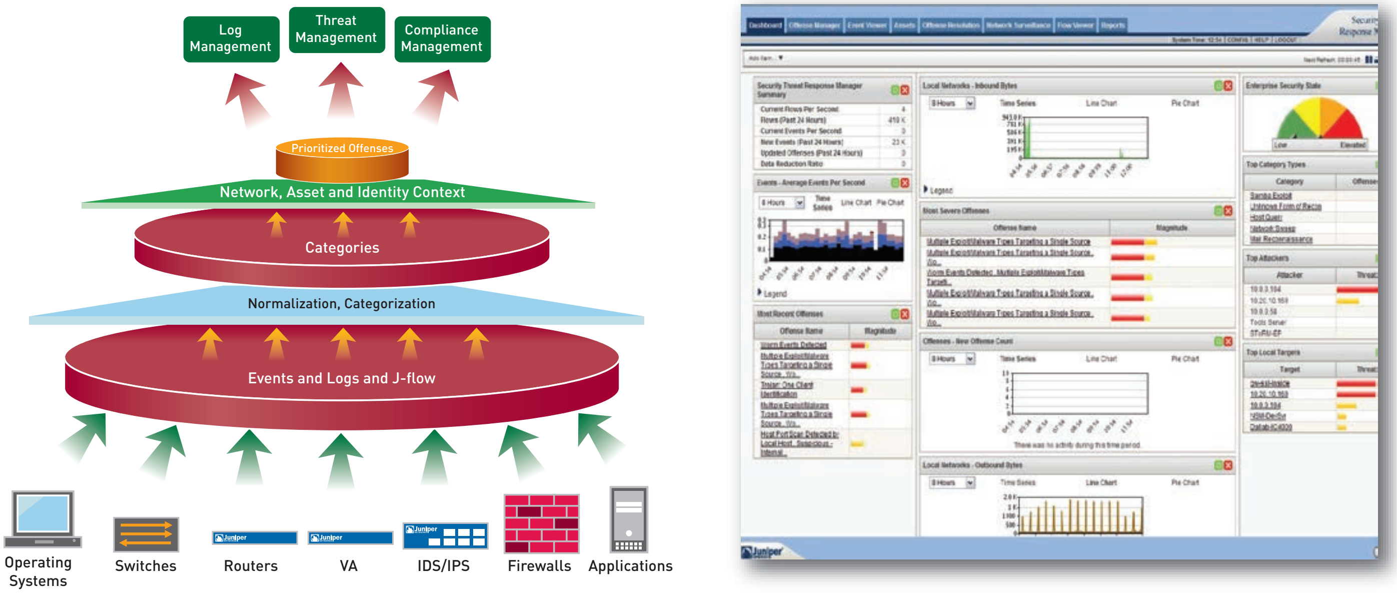

Figure 2: STRM Series architecture and dashboard

Log Management and Reporting

STRM Series provides a comprehensive log management framework that includes scalable and secure log management capabilities integrated with real time event correlation, policy monitoring, threat detection and compliance reporting.

FEATURES	FEATURE DESCRIPTION	BENEFITS
Comprehensive log management	Scalable and secure log management with storage capabilities from GB to TB of data storage.	Provides long term collection, archival, search and reporting of event logs, flow logs and application data that enables logging taxonomy from a centralized view.
Comprehensive reporting	STRM Series comes with 220+ canned reports. Report Wizard allows users to customize and schedule daily, weekly and monthly reports. These reports could be exported in PDF, HTML, RTF, Word, Excel and XML formats.	Provides users not only the convenience of canned reports but also the flexibility to create and customize their own reports according to their business needs.
Log management and reporting only option	Provides a comprehensive log management and reporting solution for organizations that are looking to implement a distributed log management only solution to collect, archive and analyze network and security event logs.	Allows users to start with log management and reporting only option and then upgrade to full blown STRM Series functionality as their business need grows without upgrading their existing hardware.

Log Management and Reporting (continued)

FEATURES	FEATURE DESCRIPTION	BENEFITS
Log retention and storage	STRM Series can easily archive logs and integrate into an existing storage infrastructure for long-term log retention and hands of storage.	The STRM Series database enables organizations to archive event and flow logs for however long is specified by a specific regulation.
Tamper proof data	• Event and flow logs are protected by SHA-x (1-256) hashing for tamper proof log archives. • Support of extensive log file integrity checks including National Institute of Standards and Technology (NIST) log management standards.	Provides secure storage based on industry regulations.
Real-time event viewing	STRM Series allows users to monitor and investigate events in real-time or perform advanced searches. The event viewer indicates what events are being correlated to offenses and which are not.	• Users have the ability to quickly and effectively view and filter real-time events. • Provides a flexible query engine that includes advanced aggregating capability and valuable and actionable IT forensics.
Data warehousing	Purpose-built data warehouse for high speed insertion and retrieval of data archive of all security logs, event logs and network activity logs (flow logs).	Full audit of all original events and flow content without modification.

Threat Management

Juniper Networks STRM Series Security Threat Response Managers' network security management solution takes an innovative approach to managing computer-based threats in the enterprise. Recognizing that discrete analysis of security events is not enough to properly detect threats, the STRM Series was developed to provide an integrated approach to threat management that combines the use of traditionally silo'd information to more effectively detect and manage today's complex threats. Specific information that is collected includes:

Network Events:

Events generated from networked resources including switches, routers, servers and desktops.

Security Logs:

Includes log data generated from security devices like firewalls, VPNs, intrusion detection/prevention, antivirus, identity management and vulnerability scanners.

Host and Application Logs:

Includes log data from industry leading host operating systems (Microsoft Windows, UNIX and Linux) and from critical business applications (authentication, database, mail and Web).

Network and Application Flow Logs:

Includes flow data generated by networking devices from vendors and provides the ability to build a context of network and protocol activity.

User and Asset Identity Information:

Includes information from commonly used directories including active directory and Lightweight Directory Access Protocol (LDAP). By incorporating patent pending "offense" management technology, this integrated information is normalized and correlated by the STRM Series, resulting in automated intelligence that quickly detects, notifies and responds to threats missed by other security solutions with isolated visibility.

FEATURES	FEATURE DESCRIPTION	BENEFITS
Out-of-the-box correlation rules	STRM Series correlation rules allow users to detect specific or sequential events or offenses. A rule consists of tests and functions that perform a response when events match.	Provides hundreds of out-of-the-box correlation rules that provide immediate value. Users can create their own rules by using the STRM Series rule wizard to generate automated alerts to security response teams and enable real time policy enforcement.
Offense management	The offense manager allows you to investigate offenses, behaviors, anomalies, targets and attackers on your network. The STRM Series can correlate events and network activity with targets located across multiple networks in the same offense and ultimately the same network incident.	This allows users to effectively investigate each offense in their network. Users can navigate the common interface to investigate the event details to determine the unique events that caused the offense.
QID mappings	STRM Series associates or maps a normalized or raw event to a high-level and low-level category.	Allows users to see real-time events mapped to appropriate categories, which allows the STRM Series to map unknown device events to known STRM Series events in order to be categorized and correlated appropriately.
Historical profiling	Extensive use of historical profiling for improved accuracy of results. STRM Series collects and stores entire event data for later use.	Allows users to view historical data at any given point as well as views into incident management and the tracking of events.
STRM Series magistrate	STRM Series magistrate component prioritizes the offenses and assigns a magnitude value based on several factors that include the number of events, severity, relevance and credibility.	• Allows users to see prioritized security events rather than looking through thousands of log events. • Allows users to see what events have the most impact on their business and respond quickly to threats.

Compliance Management

Organizations of all sizes across almost every vertical market face a growing set of requirements from IT security regulatory mandates.

Recognizing that compliance with a policy or regulation will evolve over time, many industry experts recommend a compliance program that can demonstrate and build upon these key factors:

Accountability: Providing surveillance that reports on who did what and when.

Transparency: Providing visibility into the security controls, business applications and assets that are being protected.

Measurability: Metrics and reporting around IT risks within a company.

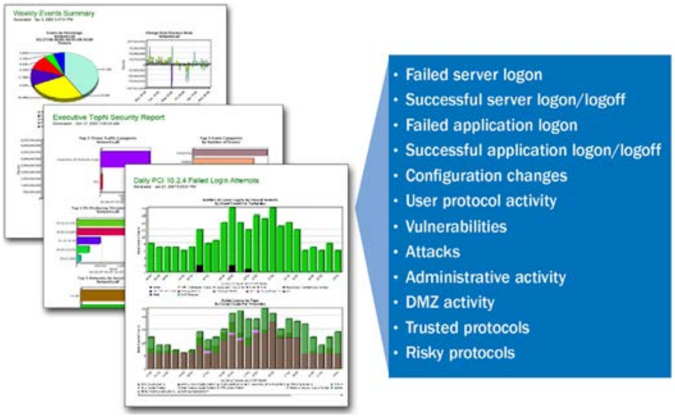
Weekly Events Summary
Executive TopN Security Report
Daily PCI 10.2.4 Failed Login Attempts
• Failed server logon
• Successful server logon/logoff
• Failed application logon
• Successful application logon/logoff
• Configuration changes
• User protocol activity
• Vulnerabilities
• Attacks
• Administrative activity
• DMZ activity
• Trusted protocols
• Risky protocols

Figure 4: Sample STRM Series compliance monitors and reports

FEATURES	FEATURE DESCRIPTION	BENEFITS
Built-in compliance reports	Out-of-the-box compliance reports are included with the STRM Series.	Provides hundreds of out-of-the-box compliance reports.
Reporting and alerting capabilities for control framework	• Control Objectives for Information and related Technology (CobiT) • International Organization for Standardization (ISO) ISO/IEC 27002 (17799) • Common Criteria (CC) (ISO/IEC 15408) NIST special publication 800-53 revision 1 and Federal Information Processing • Standard (FIPS) 200	Enables repeatable compliance monitoring, reporting and auditing processes.
Compliance-focused regulation workflow	• Payment Card Industry Data Security Standard (PCI DSS) • Health Insurance Portability and Accountability Act (HIPAA) • Sarbanes-Oxley Act (SOX) • Graham-Leach-Bliley Act (GLBA) • Federal Information Security Management Act (FISMA)	• Supports multiple regulations and security best practices. • Compliance-driven report templates to meet specific regulatory reporting and auditing requirements.
Management-level reports on overall security state	The STRM Series reports interface allows you to create, distribute and manage reports. These reports can be generated in PDF, HTML, RTF, XML and XLS formats.	Users can use the report wizard to create executive and operational level reports that combine any network traffic and security event data in a single report.

Specifications

	STRM500	STRM2500	STRM5000
Dimensions and Power			
Dimensions (W x H x D)	17.72 x 3.5 in x 17.26 (45 x 8.8 x 43.84 cm)	23.52 x 3.5 x 17.26 in (59.75 x 8.8 x 43.84 cm)	23.52 x 3.5 x 17.26 in (59.75 x 8.8 x 43.84 cm)
Weight	26 lb 2 oz	39 lb 5 oz	43 lb 10 oz
Rack mountable	2U	2U	2U
A/C power supply	90 V to 264 V hot swap dual redundant 400 watt AC power module	90 V to 264 V hot swap dual redundant 700 watt AC power module	90 to 264 V hot swap dual redundant 700 watt AC power module
D/C power supply	90 V to 264 V hot swap dual redundant 710 watt DC power module with optional 48 V DC power supply	90 V to 264 V hot swap dual redundant 710 watt DC power module with optional 48 V DC power supply	90 to 264 V hot swap dual redundant 710 watt DC power module with optional 48 V DC power supply
Simultaneous AC and DC modules support	Yes	Yes	Yes
Chassis material	18 gauge cold rolled steel	18 gauge cold rolled steel	18 gauge cold rolled steel
Fans	2 x 80 mm hot swap redundant fans (2nd optional)	3 x 80 mm hot swap redundant fans (2nd optional)	3 x 80 mm hot swap redundant fans (2nd optional)
Traffic ports	2x RJ45 10/100/1000	2x RJ45 10/100/1000	2x RJ45 10/100/1000
Console port	1x RJ45 serial console	1x RJ45 serial console	1x RJ45 serial console
Environment			
Operating temperature	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)	41° to 104° F (5° to 40° C)
Storage temperature	-40° to 158° F (-40° to 70° C)	-40° to 158° F (-40° to 70° C)	-40° to 158° F (-40° to 70° C)
Relative humidity (operating)	8 to 90 percent noncondensing	8 to 90 percent noncondensing	8 to 90 percent noncondensing
Relative humidity (storage)	5 to 95 percent noncondensing	5 to 95 percent noncondensing	5 to 95 percent noncondensing
Altitude (operating)	10,000 ft maximum	10,000 ft maximum	10,000 ft maximum
Altitude (storage)	40,000 ft maximum	40,000 ft maximum	40,000 ft maximum
Compliance and Safety			
Safety certifications	CAN/CSA-C22.2 No. 60950-1-03 UL60950-1:2003 EN60950-1:2001+A11 IEC 60950-1:2001	CAN/CSA-C22.2 No. 60950-1-03 UL60950-1:2003 EN60950-1:2001+A11 IEC 60950-1:2001	CAN/CSA-C22.2 No. 60950-1-03 UL60950-1:2003 EN60950-1:2001+A11 IEC 60950-1:2001
Emissions certifications	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A, EN 55022 Class A, EN 55024 Immunity, EN 61000-3-2, VCCI Class A	FCC Class A EN 55022 Class A EN 55024 Immunity EN 61000-3-2 VCCI Class A
Warranty	Hardware one year and software 90 days	Hardware one year and software 90 days	Hardware one year and software 90 days
Hardware Specifications			
HDD	2 x 500 GB RAID 1	6 x 250 GB RAID 5	6 x 500 GB RAID 10
Memory	8 GB	8 GB	8 GB
Events per second	Up to 500	Up to 2500	Up to 10,000
Flows per minute	Max 15 K	Max 100 K	Max 400 K

Performance-Enabling Services and Support

Juniper Networks is the leader in performance-enabling services and support, which are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to bring revenue-generating capabilities online faster so you can realize bigger productivity gains, faster rollouts of new business models and ventures, and greater market reach, while generating higher levels of customer satisfaction. At the same time, Juniper Networks ensures operational excellence by optimizing your network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/products-services.**

Ordering Information

MODEL NUMBER	DESCRIPTION
STRM500	
STRM500-A-BSE	STRM500 base HW appliance only
STRM500-ADD-250EPS-15KF	License to add up to 250 EPS and 15 K flows
STRM500-UPG-500EPS-15KF	License to upgrade up to 500 EPS with 15 K flows
Log Management Option	
STRM500-LM-ADD-500EPS	License to add up to 500 EPS for Log Management only
Upgrade Log Management to Full STRM	
STRM500-LM-500EPS-TO-TM	License to upgrade to full STRM up to 500 EPS with 15 K flows
QFlow Collector	
UNIV-1GE-4ETH	4 Port 10/100/1000 MB Ethernet card
STRM500-QFC-ADD-50MB	STRM Series Q-Flow Collector for aggregate speed up to 50 MB
STRM500-QFC-UPG-200MB	STRM Series Q-Flow Collector for aggregate speed up to 200 MB
STRM2500	
STRM2500-A-BSE	STRM2500 base HW appliance only
STRM2500-ADD-1KEPS-50KF	License to add up to 1000 EPS and 50 K flows
STRM2500-UPG-2500EPS-50KF	License to upgrade up to 2500 EPS with 50 K flows
STRM2500-UP-2500EPS-100KF	License to upgrade up to 2500 EPS and 100 K flows
Log Management	
STRM2500-LM-ADD-1KEPS	License to add up to 1000 EPS for Log Management only
STRM2500-LM-UPG-2500EPS	License to upgrade up to 2500 EPS for Log Management only
Upgrade Log Management to Full STRM	
STRM2500-LM-1KEPS-TO-TM	License to upgrade to full STRM up to 1000 EPS with 50 K flows
STRM2500-LM-2500E-TO-TM	License to upgrade to full STRM up to 2500 EPS with 50 K flows
STRM5000	
STRM5000-A-BSE	STRM5000 base HW appliance
STRM5K-ADD-5KE-200KF	License to add up to 5000 EPS and 200 K flows
Event Processor (Distributed)	
STRM5K-ADD-EP-5KEPS	License to add STRM5000 as Event Processor up to 5000 EPS
STRM5K-UPG-EP-10KEPS	License to upgrade STRM5000 Event Processor up to 10,000 EPS
STRM5000 (continued)	
Flow Processor (Distributed)	
STRM5K-ADD-FP-200KF	License to configure STRM5000 as Flow Processor up to 200 K flows/min
STRM5K-UPG-FP-400KF	License to upgrade Flow Processor up to 400 K flows/min
STRM Console (Distributed)	
STRM5K-ADD-CON	License to configure STRM5000 as Console
Log Management	
STRM5K-LM-ADD-5KEPS	STRM Series Log Management only, license to add STRM Series Log Management only up to 5000 EPS
Log Management (Distributed)	
STRM5K-LM-ADD-EP-5KE	STRM Series Log Management only, license to add STRM5000 Log Management as Event Processor up to 5000 EPS
STRM5K-LM-UP-EP-10KE	STRM Series Log Management only, license to upgrade STRM5000 Log Management as Event Processor up to 10,000 EPS
STRM5K-LM-ADD-CON	STRM Series Log Management only, license to add STRM5000 Log Management Console for Distributed Architecture
Upgrade Log Management to Full STRM	
STRM5K-LM-5KE-TO-TM	License to upgrade STRM Series Log Management to full STRM with Threat Management Upgrade to 5000 EPS and 100 K flows
STRM5K-LM-EP-5KE-TO-TM	License to upgrade STRM Series Log Management Event Processor to full STRM Event Processor with Threat Management for 5000 EPS
STRM5K-LM-CON-TO-TM	License to upgrade STRM5000 Log Management Console to full STRM5000 Console with Threat Management for Distributed Architecture
Universal	
UNIV-500G-HDD	Hard drive for STRM500 and STRM5000
UNIV-250G -HDD	Hard drive for STRM2500
UNIV-MR2U-FAN	Fan for STRM500
UNIV-HE2U-FAN	Fan for STRM2500 and STRM5000
UNIV-PS-400W-AC	STRM500 AC power supply
UNIV-PS-700W-AC	STRM2500 and STRM5000 AC power supply
UNIV-PS-710W-DC	DC power supply for STRM500, STRM2500, and STRM5000
UNIV-MR2U-RAILKIT	Mounting rail kit for STRM500
UNIV-HE2U-RAILKIT	Mounting rail kit for STRM2500 and STRM5000

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

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
Fax: 35.31.8903.601

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

1000217-001-EN Feb 2009

♻ Printed on recycled paper.