JSA SERIES SECURE ANALYTICS

Product Overview

The integrated approach of JSA Series Secure Analytics, 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. These include superior log analytics with distributed log collection and centralized viewing; threat analytics that deliver real-time surveillance and detection information; and compliance management capabilities—all viewed and managed from a single console.

Product Description

Juniper Networks® JSA Series Secure Analytics combine, analyze, and manage an unparalleled set of surveillance data—network behavior, security events, vulnerability profiles, and threat information—to empower companies to efficiently manage business operations on their networks from a single console.

- **Log Analytics:** JSA Series provides scalable log analytics by enabling distributed log collection across an organization, and a centralized view of the information.
- **Threat Analytics:** JSA 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:** JSA 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.

With preinstalled software, a hardened operating system, and a web-based setup process, the JSA Series lets you get your network security up and running quickly and easily. The bottom line of the JSA Series is simple deployment, fast implementation, and improved security, at a low total cost of ownership.

Architecture and Key Components

JSA3500 Secure Analytics

Juniper Networks JSA3500 Secure Analytics is an enterprise-class appliance that provides a scalable network security management solution for medium-sized companies up to large global organizations. It is also the base platform for an enterprise-class scalable solution. The JSA3500 includes onboard event collection, correlation and extensive reporting capabilities, and is expandable with additional JSA Series appliances acting as event and flow collectors or a combination of both on a single appliance.

JSA3500 can be deployed as an all-in-one appliance or in a distributed setup as a dedicated event, flow, or combination processor. It can also be deployed as a store-and-forward event collector.

JSA5500 Secure Analytics

Juniper Networks JSA5500 Secure Analytics is an enterprise and carrier-class appliance that provides a scalable network security management solution for medium-sized companies up to large global organizations.

JSA5500 can be deployed as an all-in-one appliance or in a distributed setup as a console or dedicated event or flow processor. It can also be deployed as a store-and-forward event collector.

JSA7500 Secure Analytics

Juniper Networks JSA7500 Secure Analytics is an enterprise and carrier-class appliance which provides a scalable network security management solution for large global organizations. JSA7500 can be deployed as a console or distributed event or flow processor. It can also be deployed as a store-and-forward event collector.

JSA Virtual Appliance

Juniper Networks JSA Virtual Appliance (JSA VM) Secure Analytics is a virtualized platform that provides Secure Analytics functionality. JSA Virtual Appliance can be deployed as an all-in-one or in a distributed setup as a console, event or flow processor. It can also be deployed as a store and forward event collector.

JSA VM is designed to run with VMWare ESX 5.0 and ESX 5.1, and requires a configuration with a minimum of two CPUs (1 socket x 2 cores or 2 sockets x 1 core) and 8GB of RAM. It processes a maximum of 1,000 events per second and 50k flows per minute.

Features and Benefits

Table 1. JSA Series Secure Analytics Features and Benefits

Features	Feature Description	Benefits
All-in-one appliances	Event collection, flow collection event processing, flow processing, correlation, analysis, and reporting are all embedded within JSA Series Secure Analytics.	· All core functions are available within the system and it is easy for users to deploy and manage in minutes. · JSA Series architecture provides a streamlined solution for secure and efficient log analytics.
Distributed support	JSA Series has the ability to scale to large distributed deployments that can support up to 5 million events per second.	· Users have the flexibility to scale to large deployments as their business grows. · JSA Series can be easily deployed in large distributed environments.
HDD implementation	JSA Series utilizes SAS HDD in RAID 1 and RAID 10 setups.	· SAS HDD is designed for 24x7 operations. · RAID 1/10 implementation provides best possible performance and redundancy.
Easy and quick install	JSA Series comes with an easy, out-of-the-box setup wizard.	· Users can install and manage JSA Series appliances in a couple of steps.
Automatic updates	Secure Analytics automatically downloads and deploys reputation feeds, parser updates, and patches.	· Users don't need to worry about maintaining appliance and OS updates and patches.
High availability (HA)	Users can deploy all JSA Series appliances in HA mode	· Users can deploy JSA Series with full active/passive redundancy. This supports all deployment scenarios, all-in-one and distributed.
Built-in compliance reports	Out-of-the-box compliance reports are included with the JSA Series.	· JSA Series provides 500+ 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	· JSA Series 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)	· JSA Series supports multiple regulations and security best practices. · Includes compliance-driven report templates to meet specific regulatory reporting and auditing requirements.
Management-level reports on overall security state	The JSA Series reports interface allows you to create, distribute, and manage reports that are generated in PDF, HTML, RTF, XML, or 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.
One stop support	Juniper Networks Technical Assistance Center (JTAC) supports all aspects of the JSA Series.	· Users don't need to go to several places to get support, even for multivendor issues.

Log Analytics

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

Table 2. Log Analytics Features and Benefits

Features	Feature Description	Benefits
Comprehensive log management	JSA Series delivers scalable and secure log analytics 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	JSA Series comes with 1,300+ canned reports. Report Wizard allows users to customize and schedule daily, weekly, and monthly reports that can 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	JSA Series provides a comprehensive log management and reporting solution with a distributed log analytics only solution to collect, archive, customize, and analyze network security event logs.	Allows users to start with a log management and reporting only option and then upgrade to full blown JSA Series functionality as their business need grows— without upgrading their existing hardware.
Log retention and storage	JSA Series database can easily archive logs and integrate into an existing storage infrastructure for long-term log retention and hassle-free storage.	Enables organizations to archive event and flow logs for whatever time period is specified by a specific regulation.
Tamperproof 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	JSA 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 IT forensics.
Data warehousing	JSA Series includes a 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).	Enables full audit of all original events and flow content without modification.

Threat Analytics

JSA Series Secure Analytics' 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 JSA Series was developed to provide an integrated approach to threat analytics that combines the use of traditionally siloed 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 network devices and provides an 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 JSA Series, resulting in automated intelligence that quickly detects, notifies, and responds to threats missed by other security solutions with isolated visibility.

Table 3. Threat Analytics Features and Benefits

Features	Feature Description	Benefits
Out-of-the-box correlation rules	JSA Series correlation rules allow users to detect specific or sequential event flows 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 JSA Series rule wizard to generate automated alerts 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 JSA 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	JSA 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 • This enables the mapping of unknown device events to known JSA Series events in order to be categorized and correlated appropriately.
Historical profiling	JSA Series collects and stores entire event data for later use, enabling extensive use of historical profiling for improved accuracy.	• Allows users to view historical data at any given point as well as views into incident management and the tracking of events.
JSA Series magistrate	JSA 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. • Enables users to see what events have the most impact on their business and respond quickly to threats.
Offense manager API	JSA Series provides a set of open APIs to modify and configure incident management parameters like "create, close, and open."	• Allows users to integrate third-party customer care applications like Remedy and other ticketing solutions.
Flow support	Flow support includes NetFlow, J-Flow, sFlow, and IPFIX	• Enables collection, visibility, and reporting of network traffic. • Includes Network Behavior Anomaly Detection (NBAD) to detect rough servers, and APTs based on network activity.

	All-in-One	Console	Event Processor	Flow Processor	Combo (EP/FP)	Event Collector Store and Forward
JSA3500	✓		✓	✓	✓	✓
JSA5500	✓	✓	✓	✓		✓
JSA7500		✓	✓	✓		✓
JSA VM	✓	✓	✓	✓		✓

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 the following 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

Licensing

Secure Analytics is available in two different licensing options:

• Log Analytics: Enables event searching, custom dashboards, and scheduled reporting

• Threat Analytics: All log analytics features + flow support, advanced correlation, and vulnerability assessment Integration

JSA3500

JSA5500

JSA7500

	JSA3500	JSA5500	JSA7500
Dimensions and Power			
Dimensions (W x H x D)	450 x 438.4 x 88 mm (17.72 x 17.26 x 3.5 in	597.5 x 438.4 x 88 mm (23.52 x 17.26 x 3.5 in)	597.5 x 438.4 x 88 mm (23.52 x 17.26 x 3.5 in)
Weight	28 lb	41 lb 5 oz	63 lb
Rack mountable	2 U	2 U	2 U

A/C power supply	90 to 264 V, 47-63 Hz, 2-6 A, 250 watt AC power module. Dual redundant option.
	• Efficiency 80Plus certified
	• Peak inrush current is:
	  - 40 A maximum at 115 VAC and 25 C
	  - 80 A maximum at 240 VAC and 25
		90 to 264 V, 47-63 Hz, 6-10 A hot swap dual redundant 560 watt AC power module, 560 watt DC power module, -45 to -60 V DC power supply (optional)
		• Peak inrush: <60 A
		• Power module maximum efficiency:
		  - 80Plus 560 W AC
		  - 80Plus 560 W DC
			90 to 264 V, 47-63 Hz, 6-10 A hot swap dual redundant 750 watt AC power module, 750 watt DC power module, -45 to -60 V DC power supply (optional)
			• Peak inrush: <60 A
			• Power module maximum efficiency:
			  - 80Plus 560 W AC
			  - 80Plus 560 W DC

D/C power supply	• 560 W DC power module • -45 to -60 V DC power supply	• 560 W DC power module • -45 to -60 V DC power supply	• 750 W DC power module • -45 to -60 V DC power supply
Chassis material	18 gauge cold rolled steel	18 gauge cold rolled steel	18 gauge cold rolled steel
Fans	Air intake from front and side of unit; exhausts to rear of unit 2 x 80 mm hot swap redundant fans (2nd optional)	Air intake from front and side of unit; exhausts to rear of unit 3 x 80 mm hot swap redundant fans (2nd optional)	Air intake from front and exhausts to rear of unit 6 x 80 mm redundant hot swap fans
Traffic ports	4 x RJ45 10/100/1000 2 x IOC slots full height	4 x RJ45 10/100/1000 2 x IOC slots full height	4 x RJ45 10/100/1000 2 x IOC slots 2/3 height
Console port	1 x RJ45 serial console	1 x RJ45 serial console	1 x RJ45 serial console
Environment			
Operating temperature	41º to 104º F (5º to 40º C)	41º to 104º F (5º to 40º C)	Normal: 41º to 104º F (5º to 40º C), Short-term: 23º to 131º F (-5º to 55º C)
Storage temperature	-40º to 158º F (-40º to 70º C)	-40º to 158º F (-40º to 70º C)	-40º to 158º F (-40º to 70º 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

Specifications (continued)

	JSA3500	JSA5500	JSA7500
Compliance and Safety			
Safety certifications	CSA 60950-1 (2003) Safety of Information Technology Equipment • UL 60950-1 (2003) • EN 60950-1 (2001) • IEC 60950-1 (2001) • EN 60825-1 +A1+A2 (1994) Safety of Laser Products - Part 1: Equipment Classification • EN 60825-2 (2000) Safety of Laser Safety of Optical Fiber Comm. Systems	CSA 60950-1 (2003) Safety of Information Technology Equipment • UL 60950-1 (2003) • EN 60950-1 (2001) • IEC 60950-1 (2001) • EN 60825-1 +A1+A2 (1994) Safety of Laser Products - Part 1: Equipment Classification • EN 60825-2 (2000) Safety of Laser Safety of Optical Fiber Comm. Systems	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
NEBS	No	No	NEBS Level 3/Verizon NEBS certified by METLABS
Hardware Specifications			
HDD	6 x 1 TB SAS 7,200 rpm RAID 10	8 x 1 TB SAS 7,200 rpm RAID 10	28 x 900 GB 10,000 rpm SAS RAID 10
Memory	32 GB	96 GB	128 GB
Maximum events per second (AIO)	5,000	10,000	N/A
Maximum events per second (distributed collector)	5,000	20,000	30,000
Flows per minute	100,000	600,000	1.2 million
CPU	1 x Quad-Core	2 x Octo-Core	2 x Octo-Core
Memory	32 GB RAM	96 GB RAM	Memory: 128 GB RAM
Storage	6 x 1 TB HDD, RAID 10	8 x 1 TB HDD, RAID 10	28 x 900 GB HDD, RAID 10
IOC slots	2 x full height	2 x full height	2 x 2/3 height
PSU	560W AC (Dual optional), (DC optional) Note: Mixing AC and DC supplies is NOT recommended nor supported	560W AC (Dual included), (DC optional) Note: Mixing AC and DC supplies is NOT recommended nor supported	750W DC (Dual included), (AC optional) Note: Mixing AC and DC supplies is NOT recommended nor supported

JSA VM Specifications

	JSA VM All-in-One	JSA VM Distributed
Maximum EPS	1,000	1,000
Flows per minute	50,000	50,000

Juniper Networks Service and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing cost and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit **www.juniper.net/us/en/products-services**.

Ordering Information

Model Number	Description
JSA3500	
Hardware Base Unit	
JSA3500-BSE	Juniper Secure Analytics HW Appliance - Mid End
Hardware Spares	
UNIV-10GE-2SFPP	Network Adapter for dualrate SFP+ 1/1H
UNIV-SFPP-DUAL-SR	Dual Rate SFP+ Optics for 10GBASE-SR/1000BASE-SX
UNIV-SFPP-DUAL-LR	Dual Rate SFP+ Optics for 10GBASE-LR/1000BASE-LX
UNIV-MR2U-B-FAN-G	Replacement Fan for JSA3500
UNIV-2U-UNIMNT-G	Universal Rack Mount for JSA3500/5500
SAS1TBHDD7K	Hard Disk Drive (HDD) 1TB 7.2Krpm SAS
UNIV-PS-250W-AC	Power supply Unit (PSU) 250W AC
UNIV-PS-560W-DC	Power supply Unit (PSU) 560W DC
JSA3500	
Licenses	
All-In-One Threat Analytics	
J3500-T-A-1250E	Juniper Threat Analytics in an All-in-One architecture. License to upgrade additional EPS=1250 only . Requires J3500-T-A-1E25KF
J3500-T-A-1E25KF	Juniper Threat Analytics in an All-in-One architecture. License to Add EPS=1250, Flows=25K Qflows/SFlows (50K J/NetFlows); Devices=750
J3500-T-A-25KF	Juniper Threat Analytics in an All-in-One architecture. License to upgrade additional Flows=25K Qflows/SFlows (50K J/NetFlows) only Requires J3500-T-A-1E25KF
J3500-T-HA	Juniper Log Analytics All-In-One HA license for JSA1500
All-In-One Log Analytics	
T4trrrJ3500-L-A-1250E	Juniper Log Analytics in an All-in-One architecture. License to Add EPS=1250; Devices=750
J3500-L-HA	Juniper Log Analytics All-in-One HA license for JSA3500
Distributed Threat Analytics	
J3500-T-A-EP-1250E	Juniper Threat Analytics in a Distributed architecture. License to add EPS=1250 to distributed JSA3500 Event Processor
J3500-T-A-EPFP-COM	Juniper Threat Analytics in a Distributed architecture. License to Add JSA3500 as a combined Event and Flow Processor up to EPS=1250, Flows=25K Qflows/SFlows (50K J/NetFlows)
J3500-T-A-FP-25KF	Juniper Threat Analytics in a Distributed architecture. License to Add JSA3500 as Flow Processor up to Flows=25K Qflows/SFlows (50K J/NetFlows)
J3500-T-COM-HA	Juniper Threat Analytics EF/FP Combo HA license for JSA3500
J3500-T-EP-HA	Juniper Threat Analytics Event Processor HA license for JSA3500
J3500-T-FP-HA	Juniper Threat Analytics Flow Processor HA license for JSA3500

Model Number	Description
Distributed Log Analytics	
J3500-L-A-EP-1250E	Juniper Log Analytics in a Distributed architecture. License to add JSA3500 as Event processor EPS=1250
J3500-L-EP-HA	Juniper Log Analytics Event Processor HA license for JSA3500
Upgrade from Log Analytics to Threat Analytics	
J3500-L-1250E-T	License to upgrade Juniper Log Analytics to Juniper Threat Analytics in an All-in-One setup. Upgrade to EPS =1250, Flows=25K Qflows/SFlows (50K J/NetFlows);Devices=750
J3500-L-EP-1250E-T	License to upgrade distributed Event Processor from Juniper Log Analytics to Juniper Threat Analytics. Upgrade to EPS =1250;Devices=750 for JSA3500
Event Collector - Store-and-Forward	
J3500-EC-SF	Event Collector Store-and-Forward License for JSA3500
Devices	
JSA-ADD-DEV-1	Additional Log Source Provides capacity for 1 additional log source.
JSA-ADD-DEV-50	Additional Log Source Provides capacity for 50 additional log sources.
JSA-ADD-DEV-500	Additional Log Source Provides capacity for 500 additional log sources.
JSA-ADD-DEV-1K	Additional Log Source Provides capacity for 1,000 additional log sources.
JSA-ADD-DEV-5K	Additional Log Source Provides capacity for 5,000 additional log sources.
JSA-ADD-DEV-10K	Additional Log Source Provides capacity for 10,000 additional log sources.
JSA5500	
JSA5500-BSE	Juniper Secure Analytics HW Appliance - High End
Hardware Spares	
UNIV-10GE-2SFPP	Network Adapter for dualrate SFP+ 1/1H
UNIV-SFPP-DUAL-SR	Dual Rate SFP+ Optics for 10GBASE-SR/1000BASE-SX
UNIV-SFPP-DUAL-LR	Dual Rate SFP+ Optics for 10GBASE-LR/1000BASE-LX
UNIV-HE2U-B-FAN-G	Replacement Fan for JSA3500
UNIV-2U-UNIMNT-G	Universal Rack Mount for JSA3500/5500
SAS1TBHDD7K	Hard Disk Drive (HDD) 1TB 7.2Krpm SAS
UNIV-PS-560W-AC	Power supply Unit (PSU) 560W AC
UNIV-PS-560W-DC	Power supply Unit (PSU) 560W DC

Ordering Information (continued)

Model Number	Description
JSA5500 (continued)	

Licenses

All-In-One Threat Analytics

Model Number	Description
J5500-T-A-2kE100KF	Juniper Threat Analytics in an All in One architecture. License to Add EPS=2500, Flows=100K Qflows/SFlows (200K J/NetFlows); Devices=750
J5500-T-A-2500E	Juniper Threat Analytics in an All in One architecture. License to upgrade additional EPS=2500 only. Requires J5500-T-A-2kE100KF
J5500-T-A-100KF	Juniper Threat Analytics in a All in One architecture. License to upgrade additional Flows=100K Qflows/SFlows (200K J/NetFlows) only. Requires J5500-T-A-2kE100KF
J5500-T-HA	Juniper Threat Analytics All-in-One HA license for JSA5500

All-In-One Log Analytics

Model Number	Description
J5500-L-A-2500E	Juniper Log Analytics in a All in One architecture. License to Add EPS=2500; Devices=750
J5500-L-HA	Juniper Log Analytics All-in-one HA license for JSA5500

Distributed Threat Analytics

Model Number	Description
J5500-T-A-CON	Juniper Threat Analytics Console License for JSA5500
J5500-T-A-EP-2500E	Juniper Threat Analytics in a Distributed architecture. License to add EPS=2500 to Distributed Event Processor
J5500-T-A-EP-10KE	Juniper Threat Analytics in a Distributed architecture. License to add EPS=10000 to Distributed Event Processor
J5500-T-A-EP-20KE	Juniper Threat Analytics in a Distributed architecture. License to add EPS=20000 to Distributed Event Processor
J5500-T-A-FP-100KF	Juniper Threat Analytics in a Distributed architecture. License for Flow Processor to add Flows=100K Qflows/SFlows (200K J/NetFlows)
J5500-T-CON-HA	Juniper Threat Analytics Console HA license for JSA5500
J5500-T-EP-HA	Juniper Threat Analytics Event Processor HA license for JSA5500
J5500-T-FP-HA	Juniper Threat Analytics Flow Processor HA license for JSA5500

Distributed Log Analytics

Model Number	Description
J5500-L-A-CON	Juniper Log Analytics Console License for JSA5500
J5500-L-A-EP-2500E	Juniper Log Analytics in a Distributed architecture. License to add EPS=2500 to Distributed Event processor
J5500-L-A-EP-10KE	Juniper Log Analytics in a Distributed architecture. License to add EPS=10000 to Distributed Event processor
J5500-L-A-EP-20KE	Juniper Log Analytics in a Distributed architecture. License to add EPS=20000 to Distributed Event processor
J5500-L-CON-HA	Juniper Log Analytics Console HA License for JSA5500
J5500-L-EP-HA	Juniper Log Analytics Event Processor HA license for JSA5500

Upgrade from Log Analytics to Threat Analytics

Model Number	Description
J5500-L-2500E-T	License to upgrade Juniper Log Analytics to Juniper Threat Analytics in an All-in-One architecture Upgrade to EPS =2500, Flows=25K Qflows/SFlows (50K J/NetFlows);Devices=750
J5500-L-CON-T	License to Upgrade Console from Juniper Log Analytics to Juniper Threat Analytics Console
J5500-L-EP-2500E-T	License to upgrade Distributed Event Processor with 2500 EPS from Juniper Log Analytics to Juniper Threat Analytics
J5500-L-EP-10K-T	License to upgrade Distributed Event Processor with 10k EPS from Juniper Log Analytics to Juniper Threat Analytics
J5500-L-EP-20K-T	License to upgrade Distributed Event Processor with 20k EPS from Juniper Log Analytics to Juniper Threat Analytics

Event Collector - Store-and-Forward

Model Number	Description
J5500-EC-SF	Event Collector Store-and-Forward License for JSA5500

Devices

Model Number	Description
JSA-ADD-DEV-1	Additional Log Source Provides capacity for 1 additional log source.
JSA-ADD-DEV-50	Additional Log Source Provides capacity for 50 additional log sources.
JSA-ADD-DEV-500	Additional Log Source Provides capacity for 500 additional log sources.
JSA-ADD-DEV-1K	Additional Log Source Provides capacity for 1,000 additional log sources.
JSA-ADD-DEV-5K	Additional Log Source Provides capacity for 5,000 additional log sources.
JSA-ADD-DEV-10K	Additional Log Source Provides capacity for 10,000 additional log sources.

JSA7500

Model Number	Description
JSA7500-BSE	Juniper Secure Analytics HW Appliance - Very High End.

Hardware Spares

Model Number	Description
UNIV-10GE-2SFPP-H	Network Adapter with support for dualrate SFP+ optics. 2/3 Height for JSA7500.
UNIV-SFPP-DUAL-SR	Dual Rate SFP+ Optics for 10GBASE-SR/1000BASE-SX
UNIV-SFPP-DUAL-LR	Dual Rate SFP+ Optics for 10GBASE-LR/1000BASE-LX
UNIV-FAN-NEBS	Replacement Fan for JSA7500-NEBS-BSE
UNIV-AIRFILT-NEBS	Air filter for JSA7500-NEBS-BSE
SAS900HDD10K	Hard Disk Drive (HDD) 900GB 10Krpm SAS
UNIV-PS-750W-AC	Power supply AC for JSA7500
UNIV-PS-750W-DC	Power supply DC for JSA7500

Ordering Information (continued)

JSA7500 (continued)

Licenses

Distributed Threat Analytics

Model Number	Description
J7500-T-A-CON	Juniper Threat Analytics Console License for JSA7500
J7500-T-A-EP-2500E	Juniper Threat Analytics in a Distributed architecture. License to add EPS=2500 to Distributed Event Processor
J7500-T-A-EP-10KE	Juniper Threat Analytics in a Distributed architecture. License to add EPS=10000 to Distributed Event Processor
J7500-T-A-EP-20KE	Juniper Threat Analytics in a Distributed architecture. License to add EPS=20000 to Distributed Event Processor
J7500-T-A-FP-100KF	Juniper Threat Analytics in a Distributed architecture. License for Flow Processor to add Flows=100K Qflows/SFlows (200K J/NetFlows)
J7500-T-CON-HA	Juniper Threat Analytics Console HA license for JSA7500
J7500-T-EP-HA	Juniper Threat Analytics Event Processor HA license for JSA7500
J7500-T-FP-HA	Juniper Threat Analytics Flow Processor HA license for JSA7500

Distributed Log Analytics

Model Number	Description
J7500-L-A-CON	Juniper Log Analytics Console License for JSA7500
J7500-L-A-EP-2500E	Juniper Log Analytics in a Distributed architecture. License to add EPS=2500 to Distributed Event processor
J7500-L-A-EP-10KE	Juniper Log Analytics in a Distributed architecture. License to add EPS=10000 to Distributed Event processor
J7500-L-A-EP-20KE	Juniper Log Analytics in a Distributed architecture. License to add EPS=20000 to Distributed Event processor
J7500-L-CON-HA	Juniper Log Analytics Console HA License for JSA7500
J7500-L-EP-HA	Juniper Log Analytics Event Processor HA license for JSA7500

Upgrade from Log Analytics to Threat Analytics

Model Number	Description
J7500-L-CON-T	License to Upgrade Console from Juniper Log Analytics to Juniper Threat Analytics Console
J7500-L-EP-2500E-T	License to upgrade Distributed Event Processor with 2500 EPS from Juniper Log Analytics to Juniper Threat Analytics
J7500-L-EP-10K-T	License to upgrade Distributed Event Processor with 10k EPS from Juniper Log Analytics to Juniper Threat Analytics

Event Collector - Store-and-Forward

Model Number	Description
J7500-EC-SF	Event Collector Store-and-Forward License for JSA7500

Devices

Model Number	Description
JSA-ADD-DEV-1	Additional Log Source Provides capacity for 1 additional log source.
JSA-ADD-DEV-50	Additional Log Source Provides capacity for 50 additional log sources.
JSA-ADD-DEV-500	Additional Log Source Provides capacity for 500 additional log sources.
JSA-ADD-DEV-1K	Additional Log Source Provides capacity for 1,000 additional log sources.
JSA-ADD-DEV-5K	Additional Log Source Provides capacity for 5,000 additional log sources.
JSA-ADD-DEV-10K	Additional Log Source Provides capacity for 10,000 additional log sources.

Virtual Appliance All-In-One

Model Number	Description
JV-T-100E-10KF-B	JSA Virtual Machine Threat Analytics Base license. All in One Architecture. License for 100EPS and 10KF
JV-T-20KF	JSA Virtual Machine Threat Analytics in All in One Architecture. License for adding 20KF (max two to reach platform max=50KF)
JV-T-300E	JSA Virtual Machine Threat Analytics in All in One Architecture. License for adding 300EPS (max three to reach platform max=1000 EPS)

Virtual Appliance All-In-One Log Analytics

Model Number	Description
JV-L-100E-B	JSA Virtual Machine Log Analytics Base license. All in One Architecture. License for 100EPS.
JV-L-300E	JSA Virtual Machine Log Analytics in All in One Architecture. License for adding 300EPS (max three to reach platform max=1000 EPS)

Virtual Appliance Distributed Threat Analytics

Model Number	Description
JV-T-CON-B	JSA Virtual Machine Threat Analytics Base license for Console in Distributed deployment.
JV-T-EP-100E-B	JSA Virtual Machine Threat Analytics Base license for Distributed EP Deployment. License for 100EPS
JV-T-FP-10KF-B	JSA Virtual Machine Threat Analytics Base license for Distributed FP Deployment. License for 10KF
JV-T-EP-300E	JSA Virtual Machine Threat Analytics license for Distributed EP Deployment. License for adding 300EPS (max three to reach platform max=1000EPS)
JV-T-FP-20KF	JSA Virtual Machine Threat Analytics license for Distributed FP Deployment. License for adding 20KF (max two to reach platform max=50KF)

Virtual Appliance Distributed Log Analytics

Model Number	Description
JV-L-CON-B	JSA Virtual Machine Log Analytics Base license for Console in Distributed Log Management deployment.
JV-L-EP-100E-B	JSA Virtual Machine Log Analytics Base license for Distributed EP Deployment. License for 100EPS
JV-L-EP-300E	JSA Virtual Machine Log Analytics license for Distributed EP Deployment. License for adding 300EPS (max three to reach platform max=1000EPS)

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at **www.juniper.net.**

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