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.
- **Vulnerability Management:** Deployed as a standalone solution or working in conjunction with Threat Analytics, JSA Series can function as a full-featured vulnerability scanner.
- **Risk Management:** JSA Series helps security professionals stay ahead of advanced threats by proactively quantifying risks from vulnerabilities, configuration errors and anomalous network activity, preventing attacks that target high value assets and data.

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

JSA Secure Analytics Appliances

The Juniper Networks Secure Analytics appliances provide a scalable solution for security event management. The JSA3800 and JSA5800 are enterprise-class solutions that can be deployed as an all-in-one solution with integrated event collection, correlation and extensive reporting, or as a dedicated event and/or flow collector. The JSA7500 is a carrier-grade solution and is NEBS certified.

JSA Virtual Appliance

Juniper Networks JSA Virtual Appliance (JSA VM) Secure Analytics is a virtualized platform that provides Secure Analytics functionality. 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 20,000 events per second or 600,000 flows per minute, with 16 cores and 24 GB of RAM.

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.

Vulnerability Management

As a member of the JSA Series Secure Analytics network security management solution, Juniper Secure Analytics Vulnerability Manager helps organizations minimize the chances of a network security breach by proactively finding security weaknesses and mitigating potential risks. Using Juniper Secure Analytics Vulnerability Manager, organizations can perform rapid network scans, discover and highlight high-risk vulnerabilities from an integrated dashboard, and automate regulatory compliance through powerful collection, correlation and reporting tools.

Table 4: Vulnerability Management Features and Benefits

Features	Feature Description	Benefits
Vulnerability overview	Juniper Secure Analytics Vulnerability Manager maintains a current view of all discovered vulnerabilities, including details such as when they were found, when they were last seen, what scan jobs reported them, and to whom the vulnerability was assigned for remediation or mitigation.	Provides the insight needed to make informed decisions.
Vulnerability dashboard	The vulnerability dashboard provides a single, integrated view into multiple vulnerability assessment feeds and threat intelligence sources, allowing security teams to quickly identify exposures that pose the greatest risks.	Makes it easy to identify and prioritize vulnerabilities.
Rapid network scans	Scans can be scheduled or performed dynamically to identify and locate security weaknesses to minimize risks.	Allows network vulnerabilities to be quickly found, analyzed and remediated.
Automated regulatory compliance	Conducts regular network scans and maintains detailed audit trails to facilitate compliance with federal or industry regulations.	Makes compliance easy and automatic.

Risk Management

Juniper Secure Analytics Risk Manager is an integral component of a complete security intelligence solution, helping security professionals detect and mitigate advanced threats. The ability to proactively quantify risk from vulnerabilities, configuration errors, anomalous network activity, and other outside threats can help organizations prevent exploits that target high-value assets and data.

Table 5. Risk Management Features and Benefits

Features	Feature Description	Benefits
Risk Manager Topology Viewer	Enables users to see network devices and their respective relationships, including subnets and links.	Helps visualize current and potential network traffic patterns with a network topology model, based on security device configurations.
Device configuration management	Automates the collection, monitoring, and auditing of device configurations across an organization's switches, routers, firewalls, and intrusion detection system/intrusion prevention system (IDS/IPS) devices.	Provides centralized network security device management, reducing configuration errors and simplifying firewall performance monitoring.
Advanced investigative network topology, traffic and forensics tools	Two network visualization security tools provide unique, risk-focused, graphical representations of the network, providing network and security teams with critical vulnerability information before, during, and after an exploit.	Quantifies and prioritizes risks with a policy engine that correlates network topology, asset vulnerabilities, and actual network traffic, enabling risk-based remediation and facilitating compliance.

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

JSA3800

JSA5800

JSA7500

	JSA3800	JSA5800	JSA7500
Dimensions and Power			
Dimensions (W x H x D)	17.2 x 1.7 x 23.5 in (43.7 x 4.3 x 56.7 cm)	17.2 x 3.5 x 24.8 in (43.7 x 8.9 x 63 cm)	17.2 x 3.5 x 23.5 in (43.7 x 8.9 x 56.7 cm)
Weight	28 lb (12.7 kg)	42 lb (19 kg)	63 lb (28.6 kg)
Rack mountable	1U (rails and screws included)	2U (rails and screws included)	2U (rails and screws included)
AC power supply	Standard: 650W high-efficiency AC-DC Redundant power: Support hot-swap AC Input: - 100-127 V, 7.8 Amp; - 200-240 V, 3.8 Amp, 60/50 Hz	Standard: 920W high-efficiency (94%+) AC-DC redundant power; support hot-swap AC Input: - 100-240 V, 50-60 Hz, 11-4.4 Amp	Optional: 750W high-efficiency AC-DC hot swap dual redundant power module AC input: 100-240 V, 50-60 Hz, 10-6 Amp DC output: 3 Amp @ +5V standby; 62.5 Amp @ +12V
DC power supply	Optional: 650W high-efficiency redundant DC to DC power supply Support hot-swap. DC Input: -44Vdc to -72Vdc, 20A (max)	Optional: 850W/1010W high-efficiency redundant DC to DC power supply Support hot-swap. DC Input: 850W: -35Vdc to -42Vdc, 30-25A	Standard: 750 W DC power module DC input: 45 to -60 Vdc, 40A (max) DC output: 3 Amp @ +5V standby; 62.5 Amp @ +12V
Fans	4 x 5.6 cm counter-rotating PWM fans	3 x 8 cm 9.5K RPM, 4-pin PWM fans	Air intake from front and exhausts to rear of unit; 6 x 80 mm redundant hot swap fans
Traffic ports	2x SFP+ 10GbE 4x RJ-45 GbE	2x SFP+ 10GbE 4x RJ-45 GbE	4 x RJ-45 10/100/1000 2 x IOC slots 2/3 height
Console port	1 x RJ-45 DB9 serial console	1 x RJ-45 DB9 serial console	1 x RJ-45 serial console
Environment			
Operating temperature	50º to 104º F (10º to 40º C)	50º to 104º F (10º 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)	6,500 ft maximum	6,500 ft maximum	10,000 ft maximum
Altitude (storage)	35,000 ft maximum	35,000 ft maximum	40,000 ft maximum
Compliance and Safety			
Safety certifications	CSA 60950-1 Safety of Information Technology Equipment • UL 60950-1 • EN 60950-1 • IEC 60950-1	CSA 60950-1 Safety of Information Technology Equipment • UL 60950-1 • EN 60950-1 • IEC 60950-1	CAN/CSA-C22.2 • No. 60950-1-03 • UL60950-1:2003 • EN60950-1:2001+A11 • IEC 60950-1:2001
Emissions certifications	• 47CFR Part 15, (FCC) Class A • ICES-003 Class A • EN 55022 Class A • CISPR 22 Class A • EN 55024 • CISPR 24 • EN 300 386 • VCCI Class A • AS/NZA CISPR22 Class A • KN22 Class A • CNS13438 Class A • EN 61000-3-2 • EN 61000-3-3	• 47CFR Part 15, (FCC) Class A • ICES-003 Class A • EN 55022 Class A • CISPR 22 Class A • EN 55024 • CISPR 24 • EN 300 386 • VCCI Class A • AS/NZA CISPR22 Class A • KN22 Class A • CNS13438 Class A • EN 61000-3-2 • EN 61000-3-3	• 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
RoHS	Yes	Yes	Yes

	JSA3800	JSA5800	JSA7500
Hardware Specifications			
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 Six-Core	2 x Ten-Cores	2 x Octo-Core
Memory	64 GB RAM	128 GB RAM	128 GB RAM
Storage	6 x 900GB 2.5" 10K SAS, RAID 10	8 x 900GB 2.5" 10K SAS, RAID 10	28 x 900 GB HDD, RAID 10
IOC slots	None	None	2 x 2/3 height
PSU	650W AC (dual included), (DC optional) Note: Mixing AC and DC supplies is NOT recommended nor supported	920W 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	5,000	20,000
Flows per minute	200,000	600,000

Juniper Networks Services 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 costs 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

Product Number	Description
Log Management	
All in One (AIO) Deployment	
JSA-LMAIO	AIO for hardware
VJSA-LMAIO	AIO for virtual appliance
Distributed Deployment	
JSA-LMCON	Console for hardware
VJSA-LMCON	Console for virtual appliance
JSA-LMEP	Event Processor (EP) for hardware
VJSA-LMEP	Event Processor (EP for virtual appliance
Threat Management (Full SIEM Capability)	
All in One (AIO) Deployment	
JSA-TMAIO	AIO for hardware
VJSA-TMAIO	AIO for virtual appliance
Distributed Deployment	
JSA-TMCON	Console for hardware
VJSA-TMCON	Console for virtual appliance
JSA-TMEP	Event Processor (EP) for hardware
VJSA-TMEP	Event Processor (EP for virtual appliance
JSA-TMFP	Flow Processor (FP) for hardware
VJSA-TMFP	Flow Processor (FP) for virtual appliance

Product Number	Description
Vulnerability Manager	
JSA-VM	Standalone deployment hardware
VJSA-VM	Standalone deployment virtual appliance
JSA-ADVM	Add-on deployment hardware
VJSA-ADVM	Add-on deployment virtual appliance

About Juniper Networks

Juniper Networks challenges the status quo with products, solutions and services that transform the economics of networking. Our team co-innovates with customers and partners to deliver automated, scalable and secure networks with agility, performance and value. Additional information can be found at Juniper Networks or connect with Juniper on Twitter and Facebook.

Corporate and Sales Headquarters
Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, CA 94089 USA
Phone: 888.JUNIPER (888.586.4737)
or +1.408.745.2000
Fax: +1.408.745.2100
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.0.207.125.700
Fax: +31.0.207.125.701

1000476-009-EN May 2017