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 provide 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—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.
- **Security Director:** The Junos Space Security Director application includes a "Block" button that, when clicked, automatically creates and deploys a firewall rule in the optimal location within your rules base to remediate detected offenses.

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 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 JSA7800 is an enterprise-class solution deployed as an all-in-one solution with integrated event collection, correlation and extensive reporting, or as a dedicated event and/or flow collector.

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, making it 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 can 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.
Security Director integration	Juniper Secure Analytics integrates with Junos Space Security Director to block malicious IP addresses in an attack with a single mouse click.	• Increases speed at which malware is blocked • Reduces the expertise needed to harness the power of IBM Qradar and Juniper Secure Analytics products
HDD implementation	JSA Series utilizes SAS HDD in RAID 1, RAID 6, and RAID 10 setups.	• SAS HDD is designed for 24x7 operations. • RAID 1/10 implementation provides the best 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 to support 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 generated in PDF, HTML, RTF, XML, or XLS formats.	• Users can use the report wizard to create executive and operational level reports that combine 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 the convenience of canned reports and the flexibility to create and customize their 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 them 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.
Tamper-proof data	• Event and flow logs are protected by SHA-x (1-256) hashing for tamper-proof log archives. • Support for extensive log file integrity checks including the 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 correlated to offenses and which are not.	• Users can 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, we developed the JSA Series 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 network and protocol activity context.
- **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 the same network incident.	• 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 • Enables 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 historical profiling for improved accuracy.	• Allows users to view historical data at any given point and provides 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, including 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. Organizations can discover and highlight high-risk vulnerabilities from an integrated dashboard and automate regulatory compliance through powerful collection, correlation and reporting tools.

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 4. 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 every vertical market face a growing set of requirements from IT security regulatory mandates. Recognizing that compliance with a policy or regulation will evolve, 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 protected assets
- 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

JSA7800

	JSA7800
Dimensions and Power	
Dimensions (W x H x D)	17.2 x 3.5 x 24.8 in (43.7 x 8.9 x 63 cm)
Weight	57 lb (25.85 kg)
Rack mountable	2U (rails and screws included)
AC power supply	Standard: 920W high efficiency (94%+) AC-DC redundant power; support hot-swap AC Input: - 100-240 V, 50-60 Hz, 11-4.4A
DC power supply	Optional: 850W/1010W high efficiency redundant DC to DC power supply Support hot-swap 850W: -36Vdc to -42Vdc, 30-25A 1010W: -43 Vdc to -76 Vdc , 30~17
Fans	3 x 8 cm 7K RPM, 4-pin PWM fans
Traffic ports	2 x SFP+ 10GbE 4 x RJ-45 GbE
Console port	1 x RJ-45 DB9 serial console
Environment	
Operating temperature	32° to 104° F (0° to 40° C)
Storage temperature	-40° to 158° F (-40° to 70° C)
Relative humidity (operating)	5 to 90 percent noncondensing
Relative humidity (storage)	5 to 95 percent noncondensing
Altitude (operating)	6,500 ft maximum
Altitude (storage)	35,000 ft maximum
Compliance and Safety	
Safety certifications	CSA 60950-1 Safety of Information Technology Equipment • UL 60950-1 • EN 60950-1 • IEC 60950-1
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
Warranty	Hardware one year and software 90 days
NEBS	No
RoHS	Yes

	JSA7800
Hardware Specifications	
Maximum events per second (distributed collector)	40,000
Flows per minute	1.2 million
CPU	2 x Ten-Core
Memory	128 GB RAM
Storage	16 x 2TB, 2.5", SAS RAID 6
IOC slots	None
PSU	920W AC (dual included), (DC optional) Note: Mixing AC and DC supplies 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 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

Please contact your Juniper sales representative for the latest JSA Series ordering information.

About Juniper Networks

Juniper Networks brings simplicity to networking with products, solutions and services that connect the world. Through engineering innovation, we remove the constraints and complexities of networking in the cloud era to solve the toughest challenges our customers and partners face daily. At Juniper Networks, we believe that the network is a resource for sharing knowledge and human advancement that changes the world. We are committed to imagining groundbreaking ways to deliver automated, scalable and secure networks to move at the speed of business

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
www.juniper.net

APAC and EMEA Headquarters
Juniper Networks International B.V.
Boeing Avenue 240
1119 PZ Schiphol-Rijk
Amsterdam, The Netherlands
Phone: +31.207.125.700