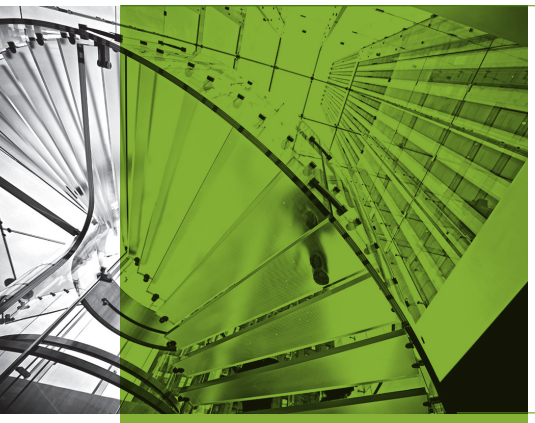

# UNMATCHED SECURITY INTELLIGENCE DETECTS AND BLOCKS ADVANCED THREATS FASTER

*JSA Series Secure Analytics accelerates detection time and reduces risk*

***Challenge***

*Security teams are challenged to analyze and interpret billions of events, correlate the data, and determine the next steps required to mitigate threats, making it nearly impossible to identify which critical events need to be handled first.*

***Solution***

*Juniper Secure Analytics (JSA) helps businesses reduce attack noise, detect and identify threats faster, and quickly respond to these incidents, reducing the risks associated with cyberattacks.*

***Benefits***

- *Reduce noise and block threats based on offenses and alerts*
- *Recognize and remediate sophisticated attacks as early as possible*
- *Reduce risk of human error and time to implement solutions*
- *Reduce the expertise needed to detect and manage threats and vulnerabilities*
- *Use one set of log collectors for management and advanced forensics*

*Today's networks are borderless. Attackers are finding increasingly creative ways to infiltrate networks, and the widespread architectures employed by many organizations make it difficult to acquire actionable cyberthreat intelligence, detect malicious activity, and enforce effective security policies against these sophisticated cyberattacks. While defending against advanced threats is critical for organizations, there is a need for automated solutions that go beyond simple log management and security information and event management (SIEM)—solutions that will allow enterprises to detect and analyze really hard problems in their environment to reduce the threat surface and risks associated with cyberattacks.*

## The Challenge

Selecting a platform upon which to build a security operation is one of the most important strategic decisions a business can make. The foundation of a comprehensive security intelligence solution that investigates, uncovers, and remediates advanced cybersecurity threats has changed over the years. While organizations need deep and real-time visibility into their entire environment to detect today's most virulent cybersecurity attacks, they also need the ability to rapidly take remedial action to eliminate discovered threats across the network.

Organizations realize that network complexity, a lack of real-time security intelligence, and minimal or no integration with security solutions render traditional SIEM offerings ineffective, putting then at tremendous risk. There is an immediate need for more modern, more powerful solutions with fully integrated security intelligence platforms that can effectively analyze large data sets to enable real-time detection and rapid remediation of cyberattacks across the entire enterprise.

## The Juniper Networks Secure Analytics Solution

Juniper Networks® JSA Series Secure Analytics Appliances are a tightly integrated solution that allows businesses to transform raw security data into meaningful insights that can be used to protect the organization from advanced threats and cyberattacks. JSA Series Secure Analytics Appliances help you quickly identify vulnerabilities, perform forensic analysis, automate compliance, and block threats.

The ability to quickly identify potential threats, however, poses its own set of challenges. Enterprise companies are finding that too much security intelligence makes it difficult to separate the signal from the noise and identify true incidents

quickly. Enterprises are also struggling with too many disjointed products from different vendors in their environment, making it difficult to monitor their security posture.

Juniper offers a sophisticated, industry-leading multivendor security solution featuring advanced threat, user behavior, risk, and vulnerability analytics; extensive threat detection capabilities for network and flow anomalies; and the ability to correlate events to reduce false positives and highlight real threats through extensive reporting. JSA Series Secure Analytics provides context and insights across the entire security event timeline, from detection and protection through remediation, applying advanced analytics to identify and prioritize those threats that pose the greatest risk to your business and require immediate attention.

Delivering multiple security capabilities through a purpose-built, extensible platform, the Secure Analytics portfolio offers real-time correlation and anomaly detection across a distributed and scalable repository of security information, enabling more accurate security monitoring and greater visibility for any organization, small or large.

JSA Series Secure Analytics, working in conjunction with other Juniper technologies such as Juniper Sky™ Advanced Threat Prevention malware detection, Juniper Networks SRX Series Services Gateways, automated operations enabled by Juniper Policy Enforcer, and intent-driven policy definition, delivers a complete end-to-end security solution for any multivendor environment. Tightly integrated with partner ecosystems in the cloud access security broker (CASB), the solution delivers endpoint security and network access control (NAC) for highly disparate networks.

JSA Series Secure Analytics can be deployed as a standalone solution for customers who are solely interested in a Security Intelligence Analytics (SIA) solution, or it can be deployed as part of the ecosystem for existing or new customers interested in Juniper's comprehensive, end-to-end security solution.

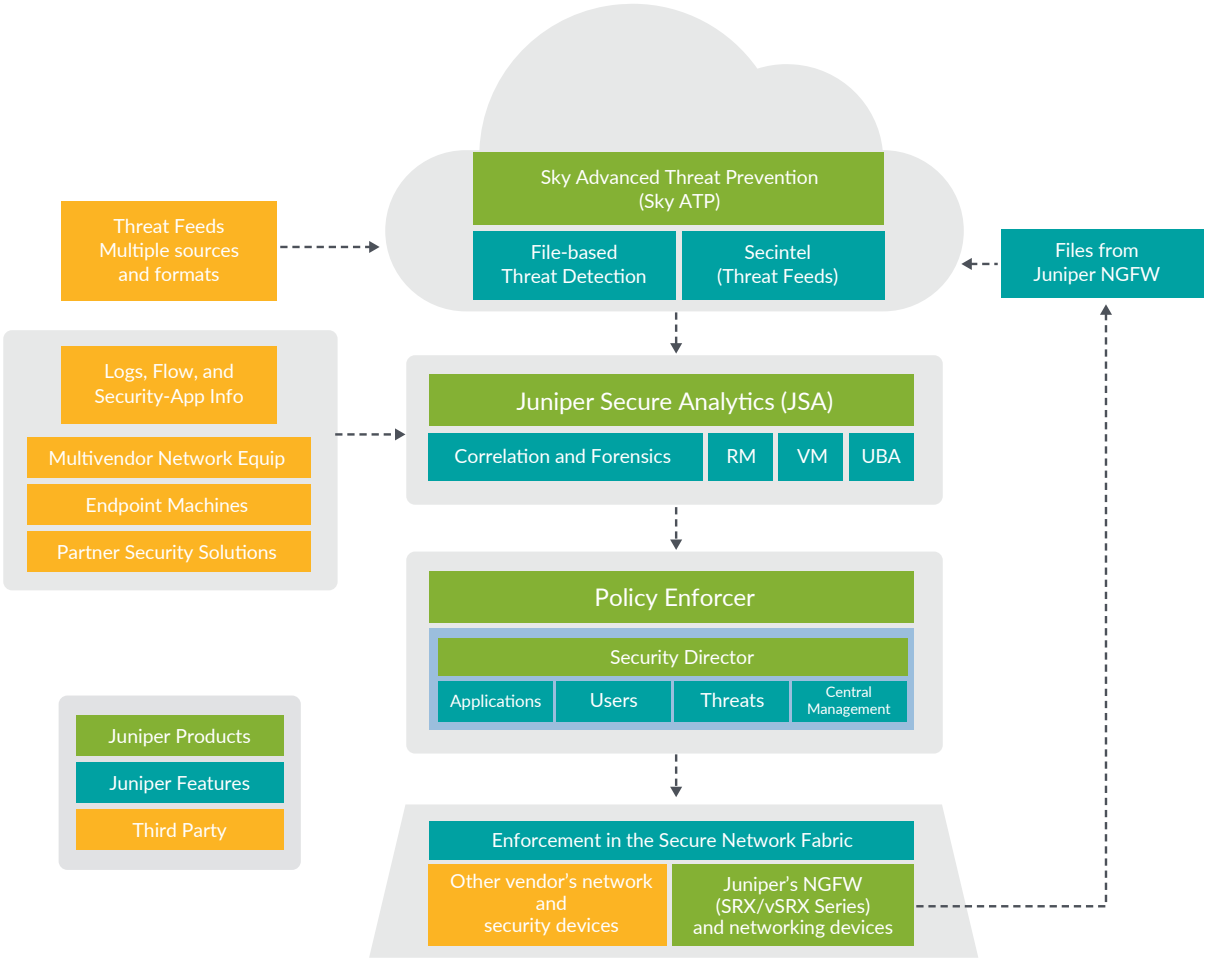


*Figure 1: JSA Series Secure Analytics Appliances and Juniper security solutions (Juniper Sky ATP, Junos Space Security Director, Policy Enforcer, and SRX Series next-generation firewalls)*

Table 1. Business Value and Benefits of Juniper Secure Analytics Platforms:

| Business Value | Benefits |
|---|---|
| Fastest SIEM in the market | • Uses state-of-the-art machine learning and data mining tools<br>• Offers the best search speed in the industry when correlating petabytes of data across hundreds of nodes<br>• Enables more effective threat management while producing detailed data access and user activity reports |
| Lower OpEx and CapEx | • Eclipses all other SIEM solutions by ingesting different types of data and correlating it across all data sources (flow, log, events, vulnerabilities, and configurations)<br>• Offers integrated view that reduces costs by consolidating several network devices |
| Open, modular, and integrated architecture | • Supports log and flow data storage for troubleshooting, IT security, and search reports<br>• Ingests all different types of data and correlates it across flow, log, events, vulnerabilities, and configuration data sources<br>• Integrates deeply with Juniper Networks Junos® Space Security Director features such as auto create and blocking based on offenses/alerts<br>• Supports policy enforcement and automation, enabling direct policy action on SRX Series firewalls and closing the security detection, analysis, and remediation loop<br>• Provides hundreds of out-of-the-box correlation rules that provide immediate value |
| Automation | • Uploads any type of script to run unique and custom business workflows<br>• Enables automated management of millions of security events, allowing Security Incident Responders to do their jobs<br>• Works with IBM Security App Exchange, enabling customers, business partners, and other developers to build applications that support automation and custom security workflows |
| Compliance | • Delivers compliance and PCI DSS, GDPR, SOX, and CISO business-level reports |
| Real-time visibility | • Provides real-time visibility into the entire IT infrastructure for threat detection, known and unknown malware, forensics, and prioritization |
| Quick and easy deployment | • Uses very simple deployment and configuration to enable well-tuned JSA Series Secure Analytics to be up and running within a few days in medium to large-scale deployments |
| Scalable and flexible architecture | • Available as physical or virtual platforms that operate across on-premises and cloud environments<br>• Supports hundreds of third-party products |
| Deployment and operational costs | • Delivers the only SIEM on the market that allows vendor consolidation, reducing costs by looking at different types of data sources and eliminating the need for several different vendors |
| Noise and alert prioritization | • Designed to focus security analyst investigations on actionable lists of suspected and high probability incidents |
| Detailed data access and user activity reports | • Produces executive-level reports<br>• Provides workflow in work order tickets for admins and approvers<br>• Effectively manages compliance and security audits |
| Multitenancy and single Web console as the master | • Enables managed service providers to provide security intelligence solutions in a cost-effective manner |

## Deployment Models

### Threat Management—Full SIEM

JSA Series Secure Analytics Appliances make full use of security intelligence through deep-dive correlation across events and flow data matched against configured rules, thereby generating an offense. With the full SIEM capabilities and features, offense management allows users to investigate threats, behaviors, anomalies, targets, and attackers on the network. By applying a combination of automated processes and machine learning, the Secure Analytics portfolio provides an intelligent security solution that learns from itself and evolves in real time, reducing the time required to detect and respond to new incidents.

The threat management deployment model offers all log management features, including threat and anomaly detection, offense management (advanced alerting), risk assessment, asset profiling, historical correlation, network flow capture, and analysis.

Table 2: Full SIEM Features

| Features | Details |
|---|---|
| Log analytics | The JSA Series provides scalable log analytics by enabling distributed log collection across an organization, and they provide a centralized view of the information. |
| Threat analytics | The JSA Series provides an advanced network security management solution that bridges the gap between network and security operations, delivering real-time surveillance and detecting complex IT-based threats. |
| Compliance management | The JSA Series delivers the accountability, transparency, and measurability critical to enabling any IT security program to meet regulatory mandates. These appliances perform regular network scans and maintain detailed audit trails to facilitate compliance with federal or industry regulations. |
| Vulnerability management | Deployed as a standalone solution or working in conjunction with full SIEM advanced features like threat analytics, the JSA Series can function as full-featured vulnerability scanners with an embedded scanning engine to provide real-time visibility into network vulnerabilities. |
| Risk management | The JSA Series helps security professionals stay ahead of threats by proactively quantifying risks from vulnerabilities, configuration errors, and anomalous network activity, preventing attacks that target high-value assets and data. |

### Log Management—Policy Centric

JSA Series Secure Analytics Appliances, both physical and virtual, deliver scalable and secure log analytics with storage capabilities ranging from gigabits to terabits of data. These log collecting and reporting capabilities, which allow users to collect and mine system events, provide a custom dashboard, reporting that includes limited compliance reporting, vulnerability scanning through the addition of vulnerability management licenses, alerting, and basic correlation.

## Solution Components

### Juniper Secure Analytics

JSA Series Secure Analytics Appliances combine, analyze, and manage an unparalleled set of surveillance data—network behavior, security events, vulnerability profiles, and threat information—to empower companies to automate the analysis of large data sets and efficiently manage business operations on their networks from a single console. JSA Series platforms, which can be key components of the Juniper Networks SDSN platform, are also integrated with Juniper Networks Junos Space Security Director central management software, providing real-time threat intelligence for quick threat remediation and direct policy enforcement across the network.

To learn more about the Security Analytics portfolio, please visit www.juniper.net/us/en/products-services/security/secure-analytics.

### Junos Space Security Director—Consistent Security Policy and Management Tools

With Juniper's scalable and intuitive Junos Space Security Director software, enterprises can make informed security decisions and achieve end-to-end visibility across applications, users, and threats in their physical and virtual cloud data centers. With easy-to-use actionable intelligence powered by JSA Series Secure Analytics, a holistic network view, and a rich security feature set, Security Director lets enterprises immediately take remedial actions and block high-risk applications and threats with a single click. User visibility and user-level application and threat visibility features allow administrators to create policies that improve user productivity, bandwidth usage, and session consumption for one or more data centers. By offering single-pane-of-glass management and an easy-to-use intelligent security rule creation wizard and auto-rule placement, Security Director lets you create less complex security policies faster.

To learn more about Security Director, please visit www.juniper.net/us/en/products-services/security/security-director.

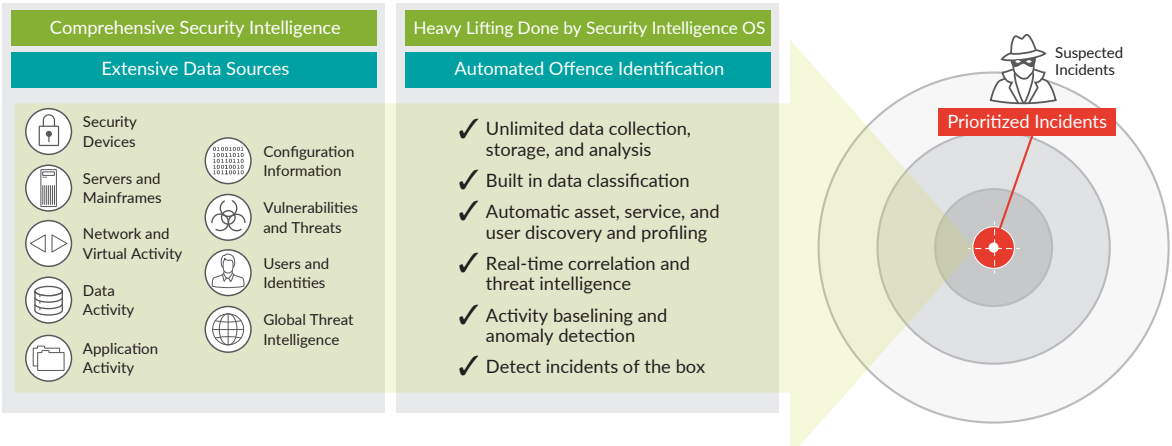


*Figure 2: JSA Series Secure Analytics in a nutshell: automated offense identification*

### Sky Advanced Threat Prevention—Advanced Malware Protection from the Cloud

A cloud-based service that is integrated with Junos Space Security Director and SRX Series firewalls, Sky Advanced Threat Prevention delivers a dynamic anti-malware solution that adapts to an ever-changing threat landscape.

An advanced, cloud-based anti-malware service, Sky ATP uses dynamic analysis (sandboxing) to defend against sophisticated "zero-day" attacks, providing built-in machine learning to improve verdict accuracy. Sky ATP feeds over Stix and Taxii can also be consumed by JSA as additional sources of threat feeds.

To learn more about Sky ATP, please visit www.juniper.net/us/en/products-services/security/sky-advanced-threat-prevention.

### Dynamic Policy Control, Detection, and Enforcement

Juniper Connected Security delivers next-generation protection that leverages the entire network, not just perimeter firewalls, as a threat detection and security enforcement domain. The Policy Enforcer component of Junos Space Security Director provides the ability to orchestrate policies created by the Sky ATP cloud-based malware detection solution and distributes them to Juniper Networks EX Series Ethernet Switches and QFX Series switches, as well as to Juniper virtual and physical SRX Series firewalls deployed in private and public cloud data centers.

To learn more about the Software-Defined Secure Network, please visit www.juniper.net/us/en/solutions/software-defined-secure-networks.

## Summary—Moving Beyond SIEM: An Integrated and Scalable Security Intelligence Platform

Effective security intelligence helps organizations make smarter decisions and reduce the risks associated with cyberthreats by processing more information more effectively across the entire network environment. Juniper's JSA Series Secure Analytics makes applying security easier and more effective by automating analysis across all available data and quickly delivering actionable security intelligence that allows organizations to make better security decisions against sophisticated attacks. Deep integration between the JSA Series platforms and Security Director allows organizations to reduce the risk of human error and improve their security posture without requiring any additional operational or personnel costs, including the need to purchase, maintain, and integrate multiple point products.

### Next Steps

For more information about Juniper Networks security solutions, please visit www.juniper.net/us/en/products-services/security or contact your Juniper Networks representative.

## 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
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

Juniper Networks | Engineering Simplicity